EU study on the

Legal analysis of a
Single Market for the Information Society

New rules for a new age?

1. Executive summary

November 2009
Chapter 1
Executive summary

1. Introduction to the study

This report presents the findings of a study commissioned by the European Commission's Information Society and Media Directorate-General. The study aims to review the relevant EU legal rules for the information society (excluding the telecom legal framework, consumer acquis and VAT rules) in order to identify gaps and inconsistencies, determine the practical impact of these rules and assess their future readiness. The study not only investigates these issues, but also comes up with recommendations on how the rules should be changed in order to encourage cross-border trade, promote new technologies and promote on-line business.

The study was undertaken by Prof. dr. Patrick Van Eecke and Maarten Truyens, lawyers associated with DLA Piper UK LLP. Other members of the study's core team include João Luís Traça (law firm Miranda, Correia, Amendoeira & Associados) and Mina Zoulovits (Philothéides, Rogas & Partners). The fourth member of the core team is Daniel Nepelski (DIW Berlin), who established the link between the legal aspects of this study and the economic aspects of the economic study that was undertaken in parallel by DIW Berlin. The core team was complemented by an advisory board of three high-profile international legal experts and visionaries: Prof. Lawrence Lessig (Universities of Stanford and Harvard, United States), Dr. Makoto Ibusuki (Seijo University, Tokyo), and Prof. dr. Ian Walden (Queen Mary, University of London). They provided the core team with legal expertise, especially from outside the EU, and delivered visionary advice on the future of legal rules in information technology.

This study was commissioned by the European Commission's Information Society and Media Directorate-General, in response to the invitation to tender OJ 2007/S 202 244659 of 19/10/2007. The study does not, however, express the Commission's official views. The views expressed and all recommendations made are those of the authors.
2. Trends and challenges

The EU regulatory framework for the information society was created in a piecemeal fashion over a period of several years (mainly 2000-2005), resulting in a set of European Directives that each cover one or more different areas of the information society.

![Figure 1: technological versus legislative activities in the field of information technology](image)

Many of these Directives have proven to be beneficial to fostering the information society. For example, the **eCommerce Directive** has allowed Internet access and hosting providers to develop their business through a protective liability regime, and has facilitated the uptake of all online services through the freedom of establishment, the freedom of online service delivery and so-called "home country control". The **eSignatures Directive** has introduced the legal possibility to use various kinds of electronic signatures. Meanwhile, the **Data Protection Directive** has made service providers aware of the necessity to handle citizens' personal data with care.

However, since its adoption, the EU regulatory framework has been confronted with a myriad of new technological developments. The rapid spread of broadband and wireless access has resulted in an almost permanent connectivity, resulting in the **omnipresence of the Internet**, as well as an increasing dependency on it. The Internet has created new – and more complex – types of interaction that overhauled the traditional webshop-to-consumer relations. The advent of **Web 2.0** services, which are characterised by massive user participation, has led to the development of enormous **online communities**, and has boosted the power of the individual by allowing individuals to reach the entire online community — resulting in influential individual blogs as well as the broadcasting of real-time messages. Online communities have also fostered the creation of new business models that rely on the aggregated personal information and the "**wisdom of the crowds**" to offer personalised services. For such services, **personal data** has become increasingly important, and is even considered the "**new currency of the digital world**". Taking into account the current development of ambient intelligence and smart objects (including technologies such as RFID), this trend can only be expected to accelerate even further.
An equally interesting development is the ever-increasing **focus on digital content**. New online services – such as online collaboration tools and online video sites – capitalise on the ease with which content in digital form can be created and distributed. New **distribution models**, which use either traditional "client-server" models or collaborative peer-to-peer technologies, facilitate the easy exchange of both copyright-protected and "open content" information. It is becoming increasingly clear that copyright laws do not seem to appropriately reflect the day-to-day reality on the Internet, where users copy photos, music and texts without permission — often even being unaware of the fact that they breach the law. These users are caught in a fundamental **"copyright paradox"**: never before have copyrighted works been so important, yet never before have users disrespected copyright in this amount. Aware of this paradox, rightholders start lawsuits, hesitate to sell digital works online, or sell digital works that are overly protected and consequently do not allow users to enjoy their legal exceptions.

The different ways to deal with copyright and privacy can particularly be observed for those who grew up in the digital environment (the so-called **"digital natives"**), for whom the distinction between the online and the offline environment is increasingly blurred, and who uphold a different legal paradigm for issues such as privacy and copyright. While the discrepancy between their values and the values of "digital immigrants" may not be threatening at first sight, one should realise that **today's digital natives** will soon become political decision makers, for whom the established (offline) values feel progressively unnatural.

Due to all these new developments, even those Directives that were pivotal for the uptake of the information society, now present lacunae, interpretation difficulties and outdated parts. These issues have been further exacerbated by the **legal duality**, which is the assumption that the online environment must be regulated differently than the offline environment. This legal duality is increasingly conflicting with the growing convergence and blurred distinction between the online and the offline environment.

Another disturbing factor is the significant **formalism** of several Directives, which is reminiscent of the legislator's lack of trust in the digital environment. For example, the eCommerce Directive requires online service providers to announce in advance whether or not the concluded contract will be filed by the service provider, and explain which technical steps can be taken to identify and correct input errors during the ordering process. No such formalities apply in the offline world, where most contracts can be concluded by sheer party consent.

### 3. Concise evaluation of each Directive

- **The eCommerce Directive** (2000/31/EC) has introduced the important principles of freedom of establishment, freedom of service provision, acceptance of electronic contracting and protection of online intermediaries. In return, it requires online service providers to comply with several transparency obligations.

However, these **transparency obligations** have become a stumbling block for new technologies and business models, because they mainly lead to increased compliance cost and offer few real consumer protection. These transparency obligations require further refinement, and may even have become superfluous.

Court cases have shown that the eCommerce Directive's **special liability regime** for online intermediaries is too focused on Web 1.0 services, leaving an entire list of new service models – particularly the most promising Web 2.0 and cloud computing services – unprotected. In addition, no online intermediary is protected against injunctions, which may lead to costly lawsuits, public exposure and technical implementation costs. Furthermore, no harmonised notice-and-takedown procedure exists,
resulting in legal uncertainty for online intermediaries and practical difficulties for rightholders to take down illegal material.

- The Data Protection Directive (95/46/EC) has made the EU the worldwide leader in data protection, and the EU should persist in this guiding role. However, despite the fact that the Data Protection Directive’s core values have survived the test of time, its actual interpretation and formalities have become increasingly excessive, leading to burdensome and sometimes questionable obligations for data controllers, which may create unnecessary competitive disadvantage for European companies. The interpretation of the Data Protection Directive should therefore return to its core values. Moreover, the Directive should leave the assumption that data processing is restricted to a few centralised entities. Instead, it should take into account the decentralised, global and online processing of personal data in today’s information society.

- The ePrivacy Directive (2002/58/EC) has shown to be a valuable asset in the protection of privacy in the online context, although its scope is fairly limited (mainly telecoms confidentiality and protection against unsolicited messages / spam). The ePrivacy Directive sufficiently covers the most prominent type of spam, although the rules are somewhat complex and do not cover all other types of unsolicited messages (e.g., instant messaging spam and spam through Bluetooth devices). However, because any further strengthening of the anti-spam rules risks to affect the wrong parties (bona fide companies) while leaving the real spam culprits untouched, the enforcement of the current anti-spam rules should be the priority in the short term.

- Although the Copyright Directive (2001/29/EC) takes into account some features of digital and online content, its core is not yet sufficiently adapted to the digital reality. The principles of copyright are still too much engrained in the offline world of analogue works, mainly defining copyright from the viewpoint of exclusive author rights. It is questionable whether this can be sustained in the future. The current legal framework has created a strong protection for rightholders, although this has not prevented the massive infringement of copyright in the online environment. In practice, the current rules impede the distribution of protected works and confront users – both consumers and businesses – with a list of ambiguities and exceptions that do not take into account the daily reality. A fundamental reform of copyright legislation has therefore become necessary.

- Because the EU telecoms framework was under review throughout the course of the study, only the important topic of net neutrality was investigated (i.e., the question of whether telecom operators must take a neutral position towards the data that passes through their networks). Although the new telecom rules enhance the protection against net neutrality infringements by imposing additional transparency obligations, they cannot be used to generally counter net neutrality infringements. In fact, effective overall net neutrality rules do not exist at all, although some competition and data protection rules could be used to deal with specific issues. In light of the rise of net neutrality infringements in Europe and abroad, a clear policy position and/or legal intervention is becoming necessary.

- As recognised by the European Commission, the previous eMoney Directive (2000/28/EC) has failed to reach the full potential of the electronic money market. The new eMoney Directive (2009/110/EC – adopted in October 2009) has solved several ambiguities created by the previous Directive, but has not resolved several other ambiguities, and has introduced a few ambiguities of its own. As a result, the legal treatment of electronic money services – particularly platform payment and mobile payment systems – is still not entirely clear, although precisely these types of services seem to be the future of online payments.

Another important issue is that the new eMoney Directive has failed to fundamentally change the waiver regime (according to which electronic money service providers can be exempted from specific
obligations), which still does not apply on a European level. The improvements brought by the new eMoney Directive may therefore not be sufficient to trigger an uptake of electronic money.

- **The eSignatures Directive** (1999/93/EC) has achieved its objective of EU-wide legal recognition of electronic signatures. However, it has not succeeded in getting companies and consumers to actually use electronic signatures on a large scale in a day-to-day context. Since electronic signatures could be key to solving several problems of the information society (including spam and identity theft) their use should be further encouraged. Furthermore, initiatives to remove technical hurdles, such as a lack of interoperability, should be stimulated.

- Electronic invoicing has also suffered from insufficient market adoption, mostly due to the burdensome legal requirements set forth by the current eInvoicing Directive (2006/112/EC), which suffers from a lack of harmonisation, a lack of legal clarity, and unnecessary discrimination between electronic and paper invoices. However, the proposal for a new eInvoicing Directive (COM(2009) 21 final) addresses these issues by providing for an equal treatment of paper and electronic invoices.

The figure below provides an overview of the number of legal issues associated with each Directive, as well as the extent to which each Directive can be considered technology-neutral.

![Figure 2: technological neutrality and number of legal issues of each Directive](image)

### 4. Practical impact of the current legal framework

The legal issues that were identified for each Directive, are not isolated theoretical issues. The text below provides some illustrations of why changes to the legal framework have become necessary.

- **Cloud computing** promises to fundamentally change the nature of IT services, by offering decentralised, global processing and storage possibilities. In true cloud computing service models, data is simultaneously stored on – and processed by – servers located across the globe, which collaborate in real-time to process data.

However, the most essential aspects of cloud computing fundamentally clash with the Data Protection Directive’s strict rules on transferring personal data outside the EU. Cloud computing service providers subject to the EU data protection rules may also suffer competitive disadvantages due to the “transfer
paradox", because personal data which would be collected outside the EU, and would then be transferred to the EU for further processing, can – in principle – not be transferred back to the original third country (because the Data Protection Directive considers such country to offer no adequate protection).

The decentralised nature of cloud computing also implies significantly diminished control of the data controller over the data being processed. Although delegation of processing is not new, it is the significant degree with which control is delegated, the potentially vast amount of third parties involved, and the highly distributed model which may cause collisions with the EU data protection requirements with respect to the selection and control of data processors.

The online profiling of individuals has become an essential aspect of many Web 2.0 services and business models. However, the possibility to perform profiling activities is legally unclear. While it is not contested that some profiling data qualifies without any doubt as "personal data" (because it can be directly linked to natural persons), it is questionable whether this is also the case for data that cannot be linked to a natural person (so-called "abstract profiles"). In case abstract profiling would also be subject to the Data Protection Directive, the legal framework may become inhibitive for the further advancement of such services and business models, even though the privacy risk in processing abstract profiles is relatively low.

Social communities such as Facebook, Netlog, Hyves and Myspace have become very popular, particularly among digital natives. However, the EU data protection principles are often difficult to reconcile with the functioning of such communities — which encourage users to expose an exponential amount of (sensitive) personal data about themselves and others. Millions of their users qualify as "data controllers", hence are responsible for the lawful processing of personal data. This sheer number of data controllers seems to collide with the EU legislation's once valid assumption that personal data would be processed only by a few isolated, centralised entities.

The role of online intermediaries (auction platforms, social networks, video sharing websites, cloud computing platforms, ...) has become increasingly important in the online environment, as they host the infrastructure and the software through which information is processed and on which online communities are built. Their legal position remains difficult, however. As from the moment an online intermediary gains sufficient popularity, its business model will be scrutinised, particularly from a copyright point of view. Although the eCommerce Directive intended to protect such online intermediaries against liability claims caused by the illegal content of their users, case law illustrates that the eCommerce Directive does not protect many Web 2.0 services against such liability claims. Moreover, the eCommerce Directive does not protect them from injunctions from, particularly, copyright holders. Accordingly, legal compliance and legal defence costs are becoming increasingly burdensome for key players, which may hinder the further development of online platforms.

Although the eCommerce Directive has introduced the freedom of establishment and the freedom of online service delivery, many online businesses still suffer from important compliance costs due to a lack of harmonised rules, as well as diverging interpretations of harmonised rules. For example, it is not clear to which extent online service providers have to comply with local rules of other Member States, due to the ambiguities in the scope of the "coordinated field" (country-of-origin compliance) of the eCommerce Directive. When sending email advertisements, it is not clear whether reliance on national anti-spam rules is sufficient, or whether compliance with the national rules of each recipient is required. Lawyers have to be involved to screen the website of service providers to verify whether all transparency and electronic contracting formalities of the eCommerce Directive have been met. Similar involvement of lawyers is also required in the field of data protection, to draft privacy policies (almost no templates exist) and to submit data protection notifications. Meanwhile, the care for real data protection issues is lacking,
due to a lack of standards and the ambiguity and divergence of the interpretation of the current data protection rules.

■ Due to the diverging national implementations of the Copyright Directive and the exclusive rights of authors, the online distribution of copyrighted materials is still stagnating and focused on the national territory. The current legal framework hardly gives authors and collecting societies any incentive to conclude licensing agreements on a pan-European level, resulting in costly licensing procedures and limited availability of online material. This limited availability of lawful online content is, in turn, also cited as one of the reasons for the massive infringement of copyright by consumers (although there are also many other contributing factors). To counter these infringements, rightholders apply strong technical protection measures to their content, which risk to undermine consumer rights, making the limited lawful content that is available even less attractive. These issues are part of a difficult debate, but illustrate in any case that a fundamental revision of the current state of online copyright is becoming necessary.

■ The current legal framework has also been ineffective to boost consumer trust in the online environment. For example, it has not yet provided efficient solutions for cross-border online disputes. Although online dispute resolution (ODR) is promising to be a cost-efficient alternative to costly and time-consuming court proceedings, its success has so far been limited to specific areas (particularly domain names and auctioning), for which the dispute resolution procedure and the actual enforcement are integrated in the platform on which the dispute arises. However, online service providers currently receive insufficient incentives to integrate ODR in their platforms.

Another area where consumer trust is lacking, is the use of electronic payments. Although there is a clear need for fast and cheap electronic payment instruments, the majority of electronic transactions is still paid with traditional credit/debit cards. However, many customers refuse to use their credit/debit card online because of security considerations. Meanwhile, the use of real "electronic money" is still very limited, despite the existence of a legal framework for e-money since 2001.

Finally, the growing number of cybercrime threats also undermines consumer trust. While the European legislation with regard to cybercrime is sufficiently advanced and future-proof, effective enforcement seems to be lacking. The same is true for spam, which also causes consumer concerns. Although a sufficient legal framework exists to fight spam, the actual enforcement of these rules is lagging behind.

5. Conclusion

The study shows that most of the EU Directives that together make up the legal framework for the information society have been beneficial to fostering the uptake of online services and encouraging users to participate in the information society. However, almost a decade after their adoption, these Directives appear dented by the increased complexity of the online environment and the introduction of new trends and technologies. While the legal issues of some Directives can be resolved through a small incremental update, other Directives need a more fundamental revision. Their version 2.0 will ensure that the EU legal framework will be prepared for a true Single European Information Space.
EU study on the

Legal analysis of a
Single Market for the Information Society

New rules for a new age?

2. Recommendations

November 2009
# Table of contents

<table>
<thead>
<tr>
<th>Chapter 2</th>
<th>Recommendations</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>General</td>
<td>2</td>
</tr>
<tr>
<td>2.</td>
<td>Scope of the Directives</td>
<td>4</td>
</tr>
<tr>
<td>3.</td>
<td>Applicable law</td>
<td>5</td>
</tr>
<tr>
<td>4.</td>
<td>Privacy and data protection</td>
<td>5</td>
</tr>
<tr>
<td>5.</td>
<td>Digital content and copyright</td>
<td>9</td>
</tr>
<tr>
<td>6.</td>
<td>Liability of online intermediaries</td>
<td>11</td>
</tr>
<tr>
<td>7.</td>
<td>E-payments</td>
<td>12</td>
</tr>
<tr>
<td>8.</td>
<td>Electronic contracting</td>
<td>13</td>
</tr>
<tr>
<td>9.</td>
<td>Net neutrality</td>
<td>14</td>
</tr>
<tr>
<td>10.</td>
<td>Spam</td>
<td>16</td>
</tr>
<tr>
<td>11.</td>
<td>Cybercrime</td>
<td>17</td>
</tr>
<tr>
<td>12.</td>
<td>Dispute resolution</td>
<td>18</td>
</tr>
<tr>
<td>13.</td>
<td>Self-regulation</td>
<td>19</td>
</tr>
</tbody>
</table>

This study was commissioned by the European Commission’s Information Society and Media Directorate-General, in response to the invitation to tender OJ 2007/S 202 244659 of 19/10/2007. The study does not, however, express the Commission’s official views. The views expressed and all recommendations made are those of the authors.
Chapter 2
Recommendations

This document presents a list of one hundred recommendations to prepare the current EU legal framework for the information society for a true Single European Information Space. Each recommendation should be read together with the detailed explanations set out in Chapters 3 to 13 of the report.

Short, mid and long term recommendations – A distinction is made between recommendations that can be implemented on the short term (2010-2015), the mid-term (2015-2020) and the long term (2020 and beyond). These time frames correspond to the relative political and legal difficulty to implement these recommendations, as well as the urgency involved. Hence, the threshold for implementing recommendations for the short term is relatively low, or the urgency involved is rather high. Conversely, recommendations for the mid-term require important legal modifications, may receive more resistance, and/or concern problems that will not become a pressing issue in the next few years. Recommendations for the long term are of a more visionary nature, are not limited to mere evolutionary changes, and encompass thoughts from a fresh angle.

High, medium and low importance recommendations – The column at the right refers to the relative importance of each recommendation (high importance, medium importance or low importance). "High importance" means that the implementation of the recommendation is considered critical, while "low importance" means that the recommendation is considered a "nice-to-have". Medium importance recommendations are not considered critical, although their implementation is nevertheless important.

1. General

Short term

1. Remove legal obstacles that are reminiscent of the legislator's "cold feet" for enacting laws for the online environment.

The current online rules contain many formalities and legal hurdles, which were meant to foster trust and increase consumer protection (e.g., strict security requirements for e-invoices, more than thirty different requirements for qualified e-signatures, mandatory notification for processing personal data; etc.). The time has come to abolish them and to opt for more flexible legislation with no unnecessary compliance overhead.

2. Ensure technological neutrality of all laws, and envisage introducing a mandatory legislative "neutrality test".

The experience with the eCommerce Directive, the eInvoicing Directive, the eSignatures Directive and the Copyright Directive has learned that the online environment evolves too quickly for legislators to catch up. Laws that are drafted with particular technologies in mind may therefore present a legal hurdle for new technologies.
3. **Start awareness campaigns to increase consumer trust and reduce online naivety.**

Despite the Internet's pervasiveness, many users still exhibit a certain level of "online naivety" (e.g., by assuming absolute online anonymity or by not realising that mouse clicks can result in binding obligations). Awareness creation is crucial to foster trust and ensure that, over time, online habits are created that can be used to develop an online "bonus pater familias" standard. Possible campaign topics could include how service providers make use of personal data, the importance of secure software, the advantages of e-signatures, the preservation of digital evidence, etc.

4. **Boost self-regulation and standardisation initiatives.**

Self-regulation has been part of the Internet since its early conception, and is also promoted by many EU legal instruments. This support for self-regulation is strongly recommendable, and should in fact be further strengthened wherever possible, in all topics investigated by this study. Relevant areas for self-regulation and standardisation include data protection (e.g., content of privacy policies and best practices for security), advertising (e.g., behavioural advertising), copyright (e.g., interoperability of DRM) and dispute resolution (e.g., adoption of minimum quality criteria for online dispute resolution).

**Mid-term**

5. ** Adopt converged legal rules.**

Due to the increasing convergence of the online and the offline environment, it is no longer appropriate to maintain separate laws for both environments. Such duality undermines the core value of the predictability of the legal rules, and also undermines the trust in these rules. However, in the short term, such converged rules will be difficult to reach in many areas, because society has not yet fully absorbed the particularities of the online environment. Hybrid rules may therefore still be justified in the short term.

6. **Enter into international data protection, copyright and spam treaties.**

It is an illusion to believe that the EU can enforce its legislation around the globe. Instead, for some of the most important issues, it should be considered to (have Member States) conclude international treaties, to provide appropriate legal answers to the new reality and ensure that at least the core European values are preserved. Although the EU could be required to water-down some of its rules, a watered down protection outside the EU will almost always be a better policy option than having no protection at all.

**Long term**

7. **Make access providers responsible for the provision of "clean Internet".**

The rise of cloud computing and web services illustrates that the Internet is evolving towards utility-based information technology. Similar to the obligation of water suppliers to provide germ-free water and the obligation of electricity suppliers to provide a stable electricity current, access providers should be made responsible for providing a spam-free, malware-free and secured Internet connection. Access providers should, however, only be made responsible for security-related issues, and must not be required to "police" the Internet or to remove illegal content (similar to how electricity providers are not responsible for the illegal use of electricity by their customers).
2. **Scope of the Directives**

**Short term**

8. **Encourage an interpretation of "information society services" that also includes online activities that are substantially provided for free.**

The current definition – as used in the eCommerce Directive – excludes online services that are not "normally provided for remuneration" from the freedom of establishment, the freedom of service provision and the special liability protection and the transparency obligations. This could impact many Web 2.0 services that are substantially offered for free to most users, which is predicted to become one of the key future business models.

9. **Publish a comprehensive register that includes all national rules that are notified by Member States as derogations from the freedom of service principle. Clarify that national rules that have not been notified do not apply to service providers established in other Member States.**

Due to the ambiguous scope of the "coordinated field" of the eCommerce Directive (which defines the scope of the freedom of establishment and the freedom of online service provision) it is not clear to which extent local national rules would apply to online service providers established in other Member States.

10. **Confirm that the coordinated field of the eCommerce Directive covers any rule that can affect online service providers, with the exception of rules that indiscriminately apply both online and offline.**

   It is currently ambiguous whether the coordinated field covers only what is explicitly regulated by the eCommerce Directive itself (transparency obligations, anti-spam rules, contracting processes, etc.), or whether it also covers rules outside the Directive.

**Mid-term**

11. **Envisage maximum harmonisation when drafting new Directives that impact the information society.**

   While the use of uniform and clear criteria for determining the applicable law is recommended (as explained in recommendation 15 below), a certain level of complexity will remain, due to the inherently borderless nature of the information society. Maximum harmonisation can significantly help to reduce the importance of the question which national law applies.

12. **Reconsider the exclusion of online gambling.**

   The eCommerce Directive excludes gambling activities, which has resulted in a legal "grey area" because it is not clear to which extent national rules can prohibit online gambling. While there used to be indications to the contrary, the Court of Justice has not yet prohibited such national gambling rules. Taking into account the importance of consumer protection in this area, it seems appropriate to include online gambling in the scope of the coordinated field of the eCommerce Directive and/or to create a harmonised regulatory framework for the online gambling market. Similarly, the eCommerce Directive's exclusion of the activities of notaries and lawyers should also be reconsidered.
3. **Applicable law**

**Mid-term**

13. Amend the current EU legal instruments on jurisdiction (Brussels I) and applicable law (Rome I - II) to include criteria that are suitable for today's complex information society services.

These legal instruments currently mainly rely on geographical criteria (such as the place of delivery or the country where the damage occurs), which are unsuitable for information society services for which the geographical location is irrelevant or difficult to determine.

14. Include rules on the applicable law for defamation and data protection issues in the Rome II Regulation.

During the drafting process of the Rome II Regulation, privacy and data protection violations (as well as defamation cases) were deliberately excluded from the scope of the Regulation. This causes legal uncertainty as regards the national law that applies to such cases.

15. Adopt uniform and clear criteria for the applicable law across all legal instruments relevant for the information society, preferably using the country of establishment / residence as the connecting factor.

The Directives currently differ in the criteria they use to define which national law applies. For example, the eCommerce Directive uses the country of origin; the Data Protection Directive uses the country where an establishment processes personal data; the consumer acquis Directives use the Member State of the consumer; etc.

4. **Privacy and data protection**

**Short term**

16. Start a fundamental debate on privacy and data protection.

Privacy and data protection are increasingly threatened by the cross-border nature of the Internet and the new paradigms upheld by digital natives and Web 2.0 service providers. While privacy and data protection are fundamental human values that deserve the Data Protection Directive's current level of protection, a fundamental debate – which goes well beyond the mere legal issues – is required to define the balance of all rights and interests involved.


While some commentators argue that "privacy is dead" and that the current rules should be abolished, the core values of the Data Protection Directive are too valuable, and must not be touched during any review of the Directive. Nevertheless, the administrative overhead and extensive scope interpretation should be scaled down.

18. Realign the interpretation of "personal data" with the (online) reality.

The current interpretation takes an almost "absolute" approach, so that any data which can somehow, by someone, be linked to a natural person (even if only indirectly), will become subject to the Data Protection Directive. This results in an almost unlimited, needlessly wide interpretation.
19. Change the "household exception" and clarify the distinction between private and public use in view of the online environment.

Personal data that is processed in the course of a purely personal or household activity, is completely exempted from all obligations of the Data Protection Directive (article 3.2). However, taking into account that individuals can collect gigabytes of (often highly sensitive) personal data for purely personal / household reasons, the assumption no longer holds true that such activities do not present data protection issues. It should therefore be considered to subject such activities to at least the most important data protection obligations.

20. Change the definition of "data controller" into a definition that is predictable, flexible and apt for the online context, and minimises situations with concurrent data controllers for the same type of processing.

Under the current definition of "data controller", it is often not clear whether a person or company actually qualifies as a data controller, because the distinction between data controllers and "data processors" is no longer apt to deal with today's more complex situations — particularly when there are several parties involved with partially overlapping responsibilities. This results in legal uncertainty and in situations where multiple parties are simultaneously considered data controllers.

21. Encourage the Member States to widen the competence of national data protection authorities and bring their staffing and budget to a level which enables them to effectively conduct their enforcement tasks.

In several Member States, the enforcement of data protection legislation is less effective due to the national data protection authority's lack of resources, lack of personnel, lack of effective powers, and their focus on a wide range of tasks. (This under-resourced enforcement effort of supervisory authorities was already reported by the Commission in its first report on the Data Protection Directive.)

22. Optimise and streamline the binding corporate rules (BCR) procedure, in particular with regard to the mutual recognition procedure.

The BCR procedure is a useful tool for protecting the privacy of data subjects, while facilitating international global transfers of personal data to corporate groups in countries without sufficient data protection legislation. Although the advantages of this procedure are clear, it is currently subject to a lengthy and complex approval process: companies must obtain the approval of the data protection authority of each Member State from which they intend to transfer data. Also due to disagreements among data protection authorities, very few BCR applications have been approved so far.

23. Adopt voluntary standards in the field of data protection.

Taking into account that the lack of standards supporting data protection legislation creates considerable uncertainty for both data controllers and data subjects, the adoption of data protection standards should be encouraged in the short term. Example areas include standards for security measures, content and structure of privacy policies, storage terms, and data export formats.

24. Introduce an information security breach notification duty for all data controllers.

Such notification duty would oblige data controllers to inform data subjects when their personal data would be stolen, lost or exposed. The new ePrivacy Directive limits such notification duty to telecom operators and Internet access providers.
25. Encourage online service providers to draft multi-layered privacy policies.

Although privacy policies are the de facto standard to meet the Data Protection Directive's transparency requirements and obtain a lawful ground for processing, many privacy policies fail to meet their goals, because they are considered a pure formality, and because they are too long, too "legalese" and too vague. Multi-layered policies would resolve this issue by presenting both a concise summary (to encourage consultation by everyone), as well as a detailed statement.

26. Abolish the notification duty for data controllers.

Many Member States require data controllers to submit a data protection notification to the national data protection authority. These notifications contribute little to the transparency towards data subjects, but cause a clear administrative burden for data controllers and data protection authorities. Abolishing the notification duty would free up time for data controllers to focus on real data protection compliance, instead of mere formal compliance.

27. Introduce an explicit prohibition on unsolicited data aggregation, similar to the existing prohibition on spam.

Considering the often surreptitious nature of unsolicited data aggregation activities, as well as their privacy-threatening features, strong action should be taken against these services. While it could be argued that such services are already prohibited under the general data protection rules, an explicit prohibition could nevertheless be advisable.

28. Encourage stakeholders to invest in educating citizens about the privacy impact of their behaviour in an online context.

Data subjects — particularly consumers — should be made aware of the privacy impact of their behaviour in an online context, for example with respect to the non-volatile nature of data posted on the Internet, the electronic footprints that are left behind on the Internet, the use of privacy enhancing technologies, the hidden business model of "free" services, etc.

29. Restrict the application of the EU data protection rules to online services that actively target EU citizens.

Through an overly extensive interpretation of the concept of "equipment", foreign online service providers currently become subject to the EU data protection rules when they use "cookies" on their website (which is the case with the majority of websites). The application of the EU rules should instead be limited to services that actively target EU citizens.

30. Consider the creation of "safe harbor" schemes with third countries, similar to the US safe harbor list.

In order to facilitate data transfers between the EU and the US, the US Department of Commerce has developed a "safe harbor" framework in consultation with the European Commission. It may be useful to encourage governments of other countries to also set up similar systems. Foreign companies would then be able to exchange personal data with EU companies without having to conclude model clauses agreements or fulfilling other administrative formalities.
**Mid-term**


   The "New Approach" entails a set of rules and principles governing the EU standardisation process in the domains of health, safety and security. The re-qualification of the Data Protection Directive as a "New Approach" Directive would formalise the requirement to lay down the practical and technical implementation of the Directive's essential principles in standards. As a consequence, the legal uncertainty concerning compliance with the Directive would be reduced, because compliance with the standards will automatically result in compliance with the Data Protection Directive.

32. **Change the definition of "sensitive data" into either a purpose-based approach or a contextualised approach.**

   The Data Protection Directive significantly restricts the processing of sensitive data (i.e., data relating to race, political opinions, religious / philosophical beliefs, or trade-union membership). The question arises whether this definition takes sufficient account of the implied sensitive nature of data (e.g., culinary preferences such as kosher or halal can reveal religious beliefs). Also, many types of data which most citizens would consider as "sensitive" (such as financial or biometric data) do not qualify as "sensitive data". In a purpose-based approach, personal data is qualified as sensitive when the processing is intended to reveal sensitive information. A contextualised approach to sensitive data means that personal data becomes sensitive according to its context.

33. **Introduce a "right to be forgotten".**

   This would give every citizen the right to ask a data controller to remove personal data as from a specified period of time (for example, five years), even when the data was initially collected with the consent of the data subject. Such "right to be forgotten" would be particularly useful for community sites, where data subjects may regret in the future of having uploaded pictures and blogs today.

34. **Introduce a "right to data portability", which allows citizens to request a copy of the personal data held by the data controller.**

   Article 12 of the Data Protection Directive already grants data subjects the right to access their personal data, and to request communication of the personal data that is being processed. However, this article does not require data controllers to send actual copies of the data: it suffices to communicate the data "in an intelligible form". A "right to data portability" would allow data subjects to request a copy of their personal data in a usable, standardised format to enable (for example) the migration to another online service provider.

35. **Initiate discussions on an international data protection treaty with a group of countries as large as possible.**

   Considering the inherent cross-border nature of the Internet, it is an illusion to believe that the EU can enforce its legislation around the globe. There seems to be a worldwide consensus as regards the fact that an international data protection instrument is required to ensure privacy protection, while at the same time allowing cross-border data flows. There also seems to be a certain level of consensus regarding the basic principles.
36. Consider using a "black list" instead of a "white list" of third countries to which personal data can (not) be transferred.

Unless particular precautions are complied with, the Data Protection Directive does not allow to transfer personal data to countries outside the EU that do offer an inadequate level of protection. The current "white list" of approved countries is overly restrictive in practice, so that a black list may be more suitable. As another alternative to the current binary distinction between countries which do and countries which do not provide this adequate protection, intermediary ("grey") categories of countries could be introduced, depending on the type of processing and countries involved.

37. Accept the processing of personal data for reasons of compliance with a third country's legal obligations as a lawful ground for processing.

Article 7 of the Data Protection Directive provides for a limited set of legal grounds for processing personal data. In addition to the consent of the data subject, the "legal obligation" constitutes an important ground for the lawful processing of personal data. However, obligations imposed by foreign laws do not qualify as a "legal obligation" for lawful processing. This creates considerable uncertainty for data controllers, since situations arise (e.g., US whistleblowing laws) where they are simultaneously subject to a foreign obligation to disclose personal data and an EU prohibition to disclose this data.

5. Digital content and copyright

Short term

38. Accelerate the debate on copyright, in order to develop legal solutions for the highly complex opposition between the interests of users and the interests of rights holders.

Even though various improvements to the copyright legal framework can significantly contribute to restoring the currently skewed balance, a fundamental copyright debate is necessary, because ad hoc measures and stopgaps do not fundamentally resolve the issues at stake. The Commission has already started this debate through initiatives such as the October 2009 reflection paper.

39. Encourage the adoption of multi-territorial licensing in order to increase legal certainty of commercial users and foster the development of online services.

This could, for example, be achieved through predetermined contractual terms, which lead to less time and money spent during the preparatory stage of a transaction. Inspiration can also be found in the licensing model chosen for the satellite broadcasting sector (as set forth by the Satellite and Cable Directive) with respect to the rights of communication to the public and making available to the public.

40. Encourage the adoption of balanced codes of conduct and/or contractual clauses.

Codes of conduct can address issues such as transparency and fairness of contractual terms, and can act as an incentive for all stakeholders to voluntarily comply with contractual terms regarding digital content. Moreover, they can increase trust between the sector-specific digital content players and bring together all stakeholders to discuss the most crucial issues and problems related to the protection of digital content.

41. Consider the introduction of a mediation system to resolve deadlocks and conflicts between rightholders and users of digital content.

Inspiration can be found in article 11 of the Satellite and Cable Directive, which introduces the establishment of a mediation system when no agreement is reached on the cable retransmission of a broadcast.
42. Clarify the Audiovisual Media Services (AVMS) Directive as to how its obligations apply to community platforms and user generated content.

The AVMS Directive only applies to service providers that exercise "editorial responsibility" over audiovisual content, which is defined as "the exercise of effective control both over the selection of the programmes and over their organisation". It is not clear to which extent a video platform with user generated content falls within the scope of this definition, so that it may be difficult to argue that such platforms exercise "editorial control" over the millions of videos uploaded to its platform.

43. Encourage the creation of balanced policies and business models.

A balance would, in particular, need to be found between dealing with piracy through a combination of education and user awareness, sufficient availability of legal content and the application of reasonable DRM measures.

44. Encourage the adoption of open standards for technological protection measures (TPMs), so that stakeholders can create compatible equipment and services.

Due to the ease with which digital works can be copied, rightholders rely on TPMs (such as Digital Rights Management) to prevent and restrict acts such unauthorised copying. Besides the issue that TPMs can conflict with a user's privacy and private use rights, an important drawback is the lack of compatibility between TPMs, which tends to lock users into the software, hardware or services of particular vendors.

45. Introduce a legal obligation to clearly mark goods protected by TPMs.

Consumers must be informed in advance about all TPMs that are applied to content to be purchased by them. One way is to introduce an obligation (preferably through self-regulation) to clearly mark the use of TPMs on the packaging of goods, or on the web pages where goods are purchased.

Mid-term

46. Revise and harmonise the list of exceptions and limitations set forth by the Copyright Directive.

The Copyright Directive contains a long list of possible exceptions and limitations to the exclusive rights of authors. This list is not harmonised, so that Member States can decide if and how to implement the exceptions and limitations. Furthermore, the list exhibits many ambiguities and leaves ample discretionary room to Member States. Consequently, the exceptions and limitations have become a cluttered chaos on the Member State level.

47. Reflect new consumer requirements in the list of exceptions and limitations.

In addition to a general revision of the list of exceptions and limitations, it could be envisaged (i) to extend the scope of the private use exception, to also cover internet publishing activities undertaken by consumers; (ii) to introduce a right of “format shifting” (i.e., converting content from one medium to another); and (iii) to introduce an exception for “creative transformative or derivative works” for user generated content.

48. Adopt new statutory provisions that allow consumers to undertake some minimum actions on digital content.

Examples include the right to technical neutrality and interoperability of content and devices; the right to receive information regarding the technological protection measures used; the right to fair contract terms; the right of privacy protection; etc.
49. Extend collective agreements between collecting societies and distributors.

Similar to the current licensing issues in the online distribution of works, the sector of satellite and cable broadcasting encounters situations where rightholders that are not represented by a collecting society could individually enforce their rights, creating interruptions in retransmitted programs. The Satellite and Cable Directive resolved this issue by extending the collective agreements between collecting societies and broadcasting organisations to other rightholders that are not represented by a collective society. A similar reasoning can be used to facilitate the online distribution of works.

50. Enhance the European copyright legal framework to better tackle commercial-level copyright infringements.

Criteria must be developed to distinguish between consumer-level and commercial-scale copyright infringements. Under the current legal framework, it is still too difficult and costly for rightholders to counter commercial-scale infringements. Member States should increase cross-border cooperation and strengthen their criminal and civil sanctions. In addition, data protection legislation could be modified in such a way that alleged data protection infringements can no longer be invoked as a mere procedural defense against commercial-scale copyright infringements.

51. Introduce an exception for the use of orphan works for which a diligent, good faith search for the rightholder has been conducted.

An orphan works is a copyrighted work for which the rightholder cannot be identified. Millions of such works can currently not be reproduced or disseminated, because such would require the consent of the rightholders. To resolve this issue, sector-specific, mutually recognised criteria should be introduced for diligent searches for rightholders. An exception should provide that orphan works can be used when these criteria are met.

52. Adopt rules that prohibit TPMs from depriving users of lawful uses of works.

TPMs may deprive users from lawful uses permitted under the exceptions and limitations set forth by the Copyright Directive (such as the private use exception or the education exceptions), effectively limiting various personal and transformative uses. Many current TPMs are therefore unfit to accommodate the myriad of possible transformative uses that copyright exceptions may allow.

53. Provide guidance with regard to the proposed role of courts in the interpretation of the "three step test".

The "three step test" is included in several international treaties, and imposes constraints on the possible limitations and exceptions to exclusive rights. However, its interpretation has been the object of discussions, because the test suffers from a lack of direction as to where the line between grants and reservations of copyright should be drawn.

6. Liability of online intermediaries

Short term

54. Introduce a harmonised and balanced notice-and-takedown procedure.

Unlike the United States and Japan, there is no harmonised EU notice-and-takedown procedure, leading to difficulties for rightholders to have infringing material taken down, as well as legal uncertainty for online intermediaries. A clear procedure must be adopted which balances the rights of the users, rightholders and intermediaries, inter alia by allowing users the possibility to oppose to the takedown before it is effectuated.
55. Develop standards that build upon the statutory notice-and-takedown procedure. Standards could be adopted for online platforms that attract large amounts of illegal material, which would specify how rightholders can cooperate with intermediaries to make the notice-and-takedown procedure as efficient as possible for all parties involved. Such standards could also specify how selected rightholders can get privileged access to the platform and to dedicated tools to search for infringements, while respecting the privacy of users and confidentiality of the affected material.

**Mid-term**

56. Harmonise the possibility to impose injunctions on online intermediaries. Although the eCommerce Directive protects some online intermediaries against liability caused by their users, intermediaries are not protected against injunctions (i.e., requests to take down material and prevent further infringements), which can lead to costly lawsuits, public exposure and technical implementation costs. Member States currently vary significantly in the conditions and the types of measures that can be imposed on intermediaries, causing legal uncertainty. In addition to harmonisation, it could be envisaged to only allow third party content injunctions as a last resort or in urgent circumstances, and to remunerate intermediaries for all costs incurred.

57. Enlarge and clarify the scope of the special liability regime. The current special liability regime set forth by the eCommerce Directive is too focused on three types of services (mere conduit, caching and hosting), and is too dependent on particular technologies. As a result, many new (Web 2.0 and cloud computing) services are not protected against third party liability. The special liability regime should therefore be revised to protect all online third party information processors against liability claims, excluding service providers that induce their users to infringe third party rights.

58. Avoid that service providers that exercise good-faith control over third party content loose the protection of the special liability regime. The eCommerce Directive does not grant liability protection when an online intermediary exercises control over the infringing material. Already, case law has emerged that exposes intermediaries who exercise good-faith control over third party content hosted by them (e.g., by cleaning up offending user comments on a blog; by removing spam messages from a forum; by monitoring offensive language in a chat room; etc.).

7. **E-payments**

**Short term**

59. Clarify the scope of the new exceptions of the new eMoney Directive, to resolve the legal uncertainty faced by many emerging online payment services. The new eMoney Directive has resolved several issues found in the previous eMoney Directive, *inter alia* by introducing two important exceptions: (i) the e-money rules do not apply to payment services in a "limited network" of service providers; and (ii) the e-money rules do not apply to service providers that do not solely act as intermediaries between the customer and the supplier of the goods / services. Although a cautionary approach applies due to the Directive's very recent adoption, the scope of these two exceptions may not be sufficiently clear in practice.
60. Stimulate the development of online escrow services.
Online financial escrow services enhance consumer trust, as they ensure a correct transaction between buyer and seller through a trusted third party. The development of such services should be stimulated to increase their use and acceptance, and lower the transaction costs involved. As such services are particularly relevant for important financial transactions, it is recommended to generally subject them to control and supervision.

61. Consider creating a voluntary accreditation system for e-money issuers.
While a strict regulation of all e-payment service providers would cripple the uptake of e-payment services, it could nevertheless be useful to introduce a voluntary accreditation system for e-money issuers (similar to the accreditation system for electronic signatures), in order to enhance consumer trust.

Mid-term

62. Exempt e-payment service providers from the e-payment rules when the maximum value stored in each individual account does not exceed 150 EUR.
The previous eMoney Directive illustrated that burdensome rules on the provision of e-money services significantly hamper the uptake of e-money services. Considering the relatively low societal risk of services limited to 150 EUR per user, it could be envisaged to exempt such services from the e-money rules to foster the uptake of e-money.

63. Introduce mutual recognition for e-money license waivers.
While the eMoney Directive allows national authorities to waive e-money obligations, such waivers only apply on a national basis, effectively restricting the associated service to the national territory. Mutually recognised waivers would resolve this issue.

8. Electronic contracting

Short term

64. Encourage the adoption of the proposal (COM(2009) 21 final) to change the current e-invoicing rules.
The current rules impose a significant number of security requirements for electronic invoices, while no such requirements apply to paper invoices. These rules are one of the reasons why the uptake of electronic invoicing has been hampered in practice. The new proposal aims to eliminate the barriers to e-invoicing by removing all differences between electronic invoices and traditional paper invoices. Taking into account the many issues that plague the current e-invoicing legal framework, the adoption of the Commission’s new proposal is recommendable.

65. Change the transparency obligations of the eCommerce Directive in order to make them compatible with current business models.
The European Court of Justice recently ruled that article 5.1.c of the eCommerce Directive – which requires online service providers to make available their contact details – must be interpreted in such way that, in practice, all online service providers must publish a telephone number on their website. This requirement will present difficulties for service providers that have a (low-cost) business model that does not allow for a permanently accessible telephone line.
66. **Adopt concise, sector-specific, templates of terms and conditions.**

Such templates can be used to counter the trend of using overly long terms and conditions. Preferably, the use of such templates would also be integrated in trustmarks.

**Mid-term**

67. **Adopt harmonised rules on e-archiving and digital evidence.**

No harmonised rules currently exist with respect to electronic archiving and digital evidence. These rules constitute the "missing link" in the spectrum of legal instruments relating to e-contracts, because all other steps found in a typical contractual process are already covered by other Directives (from the ordering process to the signature of the order and the invoicing process).

68. **Review article 9 (scope exceptions of the eCommerce Directive) to reflect the increased maturity of electronic commerce.**

Article 9 requires Member States to provide equivalence for e-documents in all contractual matters, but excludes several contract types for which online contracting was not considered appropriate (such as real estate transactions and family law contracts). Until these exceptions are removed, the eCommerce Directive will keep conveying the message that e-contracting is only suitable for "minor" transactions.

69. **Abolish articles 10 (information obligations) and 11 (ordering process obligations) of the eCommerce Directive.**

Article 10 describes the requirements to be met before the conclusion of the contract (primarily information duties), while article 11 describes the requirements for online ordering procedures. Although these requirements were answers to valid concerns at the time the Directive was drafted, they have now either become too evident, have become a stumbling block for new technologies and business models, and mainly lead to increased compliance costs. Moreover, they overly protect consumers and discriminate against the offline contracting process.

9. **Net Neutrality**

**Short term**

70. **Adopt a set of clear net neutrality principles.**

Several net neutrality interferences have already surfaced in Europe, and the number of (known) interferences is rising. However, there exist only few and fragmented rules to deal with neutrality interferences. In order to preserve the core value of network accessibility, a clear set of principles for preserving net neutrality should therefore be adopted, for example as part of a "charter of Internet rights". These principles would specify that access providers must allow users to send and receive all lawful content, freely use services and run applications of their choice, and connect and use the hardware and software of their choice. These principles would preferably be complemented by self-regulatory initiatives on a technical level.
71. Achieve compliance with these net neutrality principles by adopting a "comply or explain" approach, if necessary followed by light touch regulation. A "comply or explain" approach should be adopted in the very short term, which would allow access providers a limited time frame (e.g. one year) to comply with the net neutrality principles, and (as the case may be) to state their reasons for not complying with certain of these rules. Such an approach would not only create a framework for access providers to adhere to, but would also provide national regulatory authorities with information on types of net neutrality interferences that take place. If the "comply or explain" approach does not yield the envisioned effects in the short term, light touch regulation should be adopted.

72. Adopt strong regulation when net neutrality interferences would persist despite light touch regulation. Adopting strong regulation would be the regulatory third step (after the "comply or explain" approach and the light touch regulation) to counter net neutrality interferences.

73. Extend or clarify the powers of national telecom authorities. These authorities should have sufficient monitoring capabilities to observe the behaviour of access providers. It could also be envisaged to provide them with additional tools to gather information relating to net neutrality infringements on an ad hoc basis. Interventions should be possible irrespective of the presence of significant market power, so that interventions can occur on a case-by case basis.

74. Define and impose minimum service levels on access providers, to allow intervention when an access provider degrades the quality of service to unacceptably low levels. The current legal framework does not allow to intervene when an access provider degrades the quality of service to unacceptably low levels. To remedy this situation ex ante, minimum service levels need to be defined and imposed upon access providers. Such minimum service levels need to distinguish between various transmission technologies (wired, wireless, cellular network, …), and need to be updated in order to take into account evolutions in Internet usage.

75. Impose clear obligations on access providers to inform users about any applicable restrictions before selling an Internet access subscription. (Note that the new Universal Services Directive already contains several steps in this direction.) Preferably, the information provided by access providers should be provided on the basis of a standardised template, and published online to allow consumers easy access to the information.

**Mid-term**

76. Adopt the principle that access to the Internet is a human right. Recent initiatives underscore the social importance of Internet access. In Finland, a new law (coming into effect in July 2010) gives citizens a legal right to broadband Internet access; in November 2009, the European Parliament stressed the importance of human rights (particularly privacy) in relation to internet access; in France, the Constitutional Council ruled that Internet access is such an important component of the freedom of expression, that it cannot be cut off by administrative bodies.
77. **Adopt clear and uniform rules on the possibility for authorities to block content.**

Member States across the EU increasingly request online content to be blocked. While the scope of these requests has so far been limited to content of which the undesirability is uncontested, some Member States want to extend the blocking to other content (such as gambling websites and violent video games). Such blocking could create obstacles for the Internal Market.

78. **Consider adopting a "Data Blocking Directive".**

Such a Directive would be adopted for reasons similar to the adoption of the Data Retention Directive (the legal and technical differences between national provisions concerning the retention of data present Internal Market obstacles). The Data Blocking Directive should find a balance between the position of the various Member States and could, for example, specify which data can be blocked, and how the blocking should be performed in practice.

10. **Spam**

*Short term*

79. **Do not focus on legislative intervention in the short term.**

The majority of spam relates to traditional email spam, for which there are already sufficient (although somewhat complex) rules. The enforcement instead of the extension of these rules should be the priority. Any further strengthening of the legal framework risks impacting the wrong parties, because the compliance cost for bona fide companies would be increased, while the real spam culprits would only be marginally affected.

80. **Encourage Member States and industry stakeholders to adopt technical measures to fight spam more effectively.**

Examples of technical measures include technologies such as the Sender Policy Framework and Sender-ID (which allow to detect whether the sender of an e-mail is authorized to use a given domain name), or DomainKeys Identified Mail and Message Enhancements for Transmission Authorization (which allow to authenticate the sender). Besides factors such as cost and effectiveness, these technical measures should take into account the amount of user control and respect for data protection and privacy.

81. **Investigate which anti-spam measures can be taken at the international level.**

As long as the national laws of the EU Member States are not geared to one another and to the laws of third countries, the cross-border nature of spam will render legal action against spammers difficult and burdensome. Besides harmonisation within the EU, anti-spam alignment with third countries should also be investigated. Ideally, such investigation would result in a treaty aimed at harmonising anti-spam rules.

82. **Educate consumers on how to deal with spam, and inform businesses on how to communicate with their customers through electronic messages.**

Consumers should be made aware of the threats posed by spam, and be informed on how to deal with unsolicited e-mails, why they should not respond to spam, what software to use to limit spam, where complaints can be filed, etc.

83. **Encourage the adoption of codes of conduct and other industry driven initiatives to deal with spam.**

There is a widespread consensus (backed by the OECD and the Commission) that industry-driven initiatives and codes of conduct can play an important role in anti-spam regulation. Existing codes of conduct include the 2004 "Technology and Policy Proposal" of the Anti-Spam Technical Alliance and the SPOTSPAM project proposed by ECO.
84. **Encourage the measurement of spam.**

Few data exists about the enforcement of anti-spam measures and the impact of the legal framework on spammers. The measurement of spam should be encouraged to provide authorities with accurate and up-to-date information on the source, target, content and volume of spam in their territory, as well as the enforcement actions of national authorities.

85. **Allow national authorities to impose administrative sanctions for spammers.**

Since the traditional criminal and civil courts are often inefficient for dealing with infringements of anti-spam regulation, national enforcement authorities should be able to impose administrative sanctions on spammers, particularly in clear-cut cases. (Some Member States already foresee in the possibility of administrative sanctions.)

86. **Exempt spam messages from data retention obligations.**

The Data Retention Directive requires Internet access providers to store traffic data regarding email messages during a period between 6 and 24 months. Although the majority of emails sent nowadays qualify as spam, the Data Retention Directive does not differentiate between spam and other emails, and requires all emails sent over the network to be stored. Adopting an exemption for spam would significantly reduce the costs associated with storing the data.

**Mid-term**

87. **Simplify and clarify the current anti-spam rules, and extend them to include new forms of spam.**

There is a certain level of uncertainty about the meaning of certain basic concepts in the current rules (such as the terms "subscriber", "sale" and "consent"). Moreover, the current anti-spam rules do not cover all messages that would be considered as unsolicited by the average citizen (e.g., spam on Usenet, search engine spam, blog spam, Bluetooth spam, website popups, etc.). While simplification and clarification should not be a priority in the short term, they can be envisaged for the mid-term.

88. **Convert the rules on spam to a maximum harmonisation legal framework.**

Only the most important rules with regard to spam are harmonised, leaving much discretionary power to the Member States (mainly with regard to the application of the rules to legal persons acting as a recipient, and to other sending mechanisms than the ones mentioned by the ePrivacy Directive). These implementation differences are burdensome for businesses inside and outside the EU.

**II. Cybercrime**

**Short term**

89. **Encourage public-private sector cooperation initiatives in order to allow common action against cybercrime.**

A framework should be developed to support the exchange of information and expertise between public bodies and the industry. Also, the development of technological measures to fight cybercrime (such as filters and accreditation mechanisms) should be stimulated to boost consumer confidence in the information society.
90. Create efficient structures for cross-border cooperation between competent authorities.

The efficiency of the existing substantive legal framework is hampered by a lack of effective enforcement. Efficient structures for cross-border cooperation between the competent authorities need to be created, which foresee in a clear distribution of responsibilities and provide a framework for the exchange of information and cross-border enforcement. Strengthening and reconsidering the role of ENISA (the European Network and Information Security Agency) could also be a solution in this regard.

91. Encourage the twelve Member States that have not yet ratified the Cybercrime Convention to do so as quickly as possible.

The Cybercrime Convention covers almost all forms of cybercrime, so that the need for additional legislative intervention is limited. Steps should be taken to encourage the twelve Member States that have not yet ratified the Convention to do so as quickly as possible. In addition, to avoid allowing criminals a large number of safe havens, the Commission should encourage third countries to accede to the Convention and its additional protocol.

92. Encourage Member States that have not already done so to implement the Framework Decision on Attacks Against Information Systems.

The Framework Decision on Attacks Against Information Systems is of significant importance for the harmonisation of cybercrime regulation in Europe. Member States that have not already done so, should implement the Framework Decision in their national legislation. In addition, all Member States must be encouraged to take into account the remarks of the Commission with regard to a harmonised implementation of the Framework Decision.

12. Dispute resolution

Short term

93. Adopt standards for self-regulated dispute resolution procedures, which set forth minimum procedural guarantees.

One of the most important advantages of online dispute resolution (ODR) is its speed and cost-efficiency, which is reached by using simplified procedures and less formalism. However, care must be taken to ensure that ODR procedures do not jeopardise due process.

94. Adopt voluntary accreditation schemes for ODR service providers.

Such accreditation schemes would be similar to the accreditation scheme for e-signatures (introduced by the eSignatures Directive). By encouraging ODR providers to respect certain minimum values (such as impartiality, transparency and fairness), they would mitigate the due process and other concerns regarding ODR.
Allow alternative dispute resolution (ADR) / ODR procedures towards consumers when the ADR / ODR service provider meets certain minimum quality criteria.

The use of arbitration in consumer contracts is widely restricted in Europe by the Directive on unfair terms in consumer contracts and the Recommendation on Certain Aspects of Mediation. Traditional courts therefore still need to be invoked despite an arbitration clause, which significantly limits the uptake of ADR / ODR. ADR / ODR should be allowed towards consumers, under the strict condition that the procedure meets minimum quality criteria, and that consumers always retain the right to resort to the court. This would be especially useful for dealing with small claims.

Oblige online payment providers to integrate dispute resolution procedures in their online payment flow.

ODR has already provided to be successful in areas such as domain name disputes and auctioning, due to the integration of the ODR in the platform on which the dispute arises. The most important ODR drawback is indeed that it requires the parties to consent to the procedure, which is particularly problematic when an online service provider does not have sufficient incentives to consent to ODR towards a consumer.

Introduce EU-level e-courts dedicated to resolving common online disputes.

Such e-courts would be specialised in online matters, but would in other aspects function like a traditional court. The whole process should be completely digital, and the hearing can be carried out in a more flexible way, e.g. through telephone, audio, video, or e-mail conference. There exist examples that are already operational and resemble these e-courts, such as the .EU arbitration panel in Prague (Czech Republic) and the WIPO panels for UDRP procedures, which have proven to be able to efficiently handle cases from very different jurisdictions.

Consider to which extent self-regulatory initiatives can be linked to standardisation efforts, and stimulate the convergence between self-regulation and standards.

As technical standards can be considered as a type of self-regulation, it can be useful to stimulate a convergence between self-regulation and standards, and to investigate to which extent self-regulatory initiatives can be linked to standardisation efforts. Such link could, for example, be to have the output of self-regulatory initiatives adopted as formal standards through the new standardisation procedures that are currently being developed by the European Commission. A second possibility would be to mirror some of the new governance structures in self-regulatory initiatives.

Encourage the incorporation of trustmarks and codes of conducts in software.

This would allow users to configure their web browsers for trustmark compliance settings, which would convey warnings when a service is not in line with these predefined settings. Provided the software offers an attractive and user-friendly interface, there is a realistic possibility that users and developers will use these features.
100. Adopt self-regulation "templates" that reflect best practices and sound governance principles (transparency, accountability and involvement of all stakeholders).

Templates offer practical help to convince parties to initiate self-regulation. Similar templates have already been successful in other domains (see, for example, the European model EDI agreement drafted in the framework of the TEDIS programme).
EU study on the

Legal analysis of a
Single Market for the Information Society

New rules for a new age?

3. General overview

November 2009
# Table of contents

## Chapter 3. Overview

1. Setting the scene ................................................................. 3
2. Introduction to the study ...................................................... 5
   2.1. Aim .................................................................................... 5
   2.2. Team .................................................................................. 5
   2.3. Approach .......................................................................... 5
   2.4. Topics and legal instruments out of scope ................. 6
3. Key trends that affect the legal framework ....................... 7
   3.1. Omnipresence of the Internet .............................................. 7
   3.2. New ways of doing business ............................................. 8
   3.3. Focus on digital content .................................................. 9
   3.4. Community building ...................................................... 10
   3.5. Individual-to-community (I2C) ........................................... 12
   3.6. Smart objects and ambient intelligence ......................... 13
   3.7. A data-driven world ......................................................... 14
   3.8. Convergence ................................................................. 15
   3.9. Digital natives ............................................................... 16
   3.10. Rise of cybercrime threats ............................................. 17
4. Challenges faced by the legal framework ......................... 18
   4.1. Legal duality ................................................................. 18
   4.2. "Cold feet" ...................................................................... 19
   4.3. Online naivety .............................................................. 19
   4.4. Privacy leakage ............................................................ 20
   4.5. Public support for established rules ............................... 21
   4.6. Local versus global ....................................................... 22
   4.7. Weak enforceability ....................................................... 22
   4.8. Endangered intermediaries ............................................. 23
   4.9. Network accessibility and free speech ............................ 23
   4.10. Democratic deficit of online communities .................... 24
5. Findings per topic ............................................................... 25
   5.1. The future of privacy and data protection ................. 25
   5.2. Digital content and copyright ..................................... 26
   5.3. Liability of online intermediaries ................................ 26
   5.4. E-payment ................................................................. 27
   5.5. Electronic contracting .................................................. 28
   5.6. Net neutrality ............................................................. 28
   5.7. Spam ............................................................................ 29
   5.8. Cybercrime .............................................................. 29
   5.9. Dispute resolution ........................................................ 30
   5.10. Self-regulation ............................................................ 31
6. General recommendations .................................................. 31
   6.1. Introduction: respecting core values .............................. 31
   6.2. Adopt hybrid rules in the short term, but converged rules in the mid-term ....... 34
   6.3. Remove unnecessary obstacles ..................................... 35
   6.4. Ensure technological neutrality ................................. 36
   6.5. Create citizen awareness ............................................. 37
   6.6. Boost self regulation and standardisation ................. 38
   6.7. Clarify and enlarge the scope of the eCommerce Directive ... 38
   6.8. Enter into international treaties ....................................... 40
6.9. Make access providers responsible for the provision of "clean Internet" ......................... 40
6.10. Start a fundamental discussion on data protection and copyright .............................. 41
7. Open issues .................................................................................................................. 43

This study was commissioned by the European Commission’s Information Society and Media Directorate-General, in response to the invitation to tender OJ 2007/S 202 244659 of 19/10/2007. The study does not, however, express the Commission’s official views. The views expressed and all recommendations made are those of the authors.
Chapter 3
Overview

1. Setting the scene

Since its public adoption in the early nineties, the Internet has profoundly changed society and important aspects of our lifestyle, such as the way we communicate, interact, collaborate, shop and work. Its tremendous success has boosted the distribution, creation and use of information on such an extraordinary scale, transforming society into the so-called "information society" or "network society"— a society whose social structure is made of networks powered by microelectronics-based information and communication technologies\(^1\).

Aware of the importance of these evolutions, the EU undertook several legislative efforts to address the challenges posed by the information society. For example, in 1995, the Data Protection Directive was enacted to protect the personal data of individuals by determining when the processing of such data is lawful. The Electronic Signatures Directive of 1999 created a legal basis for electronic signatures, facilitating reliable electronic contracting. As another example, the Electronic Commerce Directive enacted in 2000, constituted the basic legal framework for electronic commerce in the Internal Market. In 2002, the ePrivacy Directive was adopted to complement the Data Protection Directive. These and other directives together constitute the "acquis communautaire" for the information society.

As illustrated below, the regulatory framework for the information society was created in a piecemeal fashion over a period of several years (mainly 2000-2005), with European directives that each cover one or more different areas of the information society. The bulk of the EU legislative efforts are concentrated in the period 1999 - 2003, before the emergence of today's "Web 2.0".

These legislative efforts have only been partially successful. Over the years, it has become clear that some of the legal instruments adopted between 1995 and 2005 did not respond to all questions and

problems faced by today’s information society. While the current Directives affect most important issues, there are several areas (gaps) that are currently not covered by EU legislation, even while the EU is in the best position to regulate these areas. Moreover, there are several examples of frictions and overlaps between Directives.

These issues have exacerbated when new technologies and trends emerged for which the existing legal rules were not designed. Furthermore, the national case law for some EU legal instruments is too disparate across Member States. The current legal framework could therefore be described as a patchwork, where some rules are missing, other rules are overrepresented and some rules overlap. However, these issues are not uniformly distributed across all Directives, as illustrated below.

---

2 See, for example, the Commission Staff Working Document on the Review of the E-Money Directive (2000/46/EC), page 15: “The Commission services are of the view that the evidence gathered during the course of the review process establishes that, six years after its adoption and some four years since its implementation in the Member States, there is a case for a fundamental overhaul of the Directive.”; the proposal for a new VAT Directive (COM (2009) 21 final, p. 9: “Allowed by the various options available to them, Member States have implemented the rules on e-invoicing in a divergent way. This has created a disharmonised set of e-invoicing rules that have been difficult for businesses to comply with, especially when sending cross border e-invoices.”

3 For example, clear rules dedicated to preserving “net neutrality” on the Internet; creating uniform rules that determine the applicable law and court for the online environment.

4 For example, the very high level of protection offered by the Data Protection Directive, as compared to the privacy-threatening effects of digital rights management (DRM, as legally protected by the Copyright Directive) and the long retention periods of the Data Retention Directive.

5 For example, the legal provisions relating to spam are currently distributed between four distinct legal instruments; the legal provisions on transparency towards consumers are also distributed among the eCommerce Directive, the Unfair Commercial Practices Directive and the Distance Selling Directive.

6 Examples: spam using Bluetooth, instant messaging tools or social community websites; dealing with liability of peer-to-peer service providers; dealing with the liability of “freemium” services; introducing a “right to be forgotten” on the Internet.

7 For example, the special liability regime found in the E-commerce Directive has triggered diametrically opposing decisions from courts across the EU.

8 Note: the circles with dotted lines represent currently pending proposals. The size of the circle suggests the relative importance of the legal instrument in the entire legal framework for the online environment.
2. **Introduction to the study**

2.1. **Aim**

This study aims to review the legal rules for the information society, both on the EU-level and the national level, in order to investigate the gaps and inconsistencies, determine their practical impact and assess their future readiness. The study not only investigates these issues, but also comes up with recommendations on how these rules should be changed in order to encourage cross-border trade, promote new technologies and promote on-line business. In other words, the study tries to prepare the current legal framework for a true Single European Information Space, aimed at an open and competitive digital economy, where ICT is emphasised as a driver of inclusion and quality of life.

2.2. **Team**

This study was undertaken by Prof. dr. Patrick Van Eecke and Maarten Truyens, lawyers associated with DLA Piper UK LLP. Other members of the study's core team include João Luís Traça (law firm Miranda, Correia, Amendoia & Associados) and Mina Zoulovits (Philotheidis, Rogas & Partners). The fourth member of the core team is Daniel Nepelski (DIW Berlin), who established the link between the legal aspects of this study and the economic aspects of the economic study that was undertaken in parallel by DIW Berlin.

The core team was complemented by an advisory board of three high-profile international legal experts and visionaries: Prof. Lawrence Lessig (Universities of Stanford and Harvard, United States), Dr. Makoto Ibusuki (Seijo University, Tokyo), and Prof. dr. Ian Walden (Queen Mary, University of London). They provided the core team with legal expertise, especially from outside the EU, and delivered visionary advice on the future of legal rules in information technology.

2.3. **Approach**

The approach of the study is multi-layered, combining multiple angles to reach its goal of providing a holistic assessment of the legal framework for the information society.

i. **EU-level and Member State level** – The study investigates the EU-level legal instruments that together make up the "acquis communautaire" for the online environment. It determines to which extent these EU-level legal instruments are still adequate for today's information society, whether they cover all relevant issues, and whether they are internally consistent.

However, the study is not limited to the EU-level legal instruments: for several topics, it also investigates how these instruments are implemented in the Member States. Member States not only implement the EU legal instruments differently in their own legal system; their case law and legal doctrine also show varying approaches. The study investigates some of the issues that arise, and how they can be dealt with at the European level.

ii. **Multiple time horizons** – The study provides recommendations for both the short-term, the mid-term and the long-term time horizons. For the short-term (2010 to 2015), it specifies recommendations that have a relatively low adoption barrier from a political and legal perspective, or for which the issue concerned is considered urgent. Such recommendations aim at removing current stumbling blocks, and do not require a complete overhaul of the acquis communautaire.

However, the study is not limited to such "low hanging fruit" for the short term. It also suggests recommendations for the mid-term (2015 to 2020), which require important legal modifications, or may receive more political resistance.
In addition, together with visionary legal experts from within and outside the EU, the ideal legal landscape for Europe in the long term (2020 and beyond) was envisaged. Such recommendations for the long term are not limited to mere evolutionary changes, and encompass recommendations from a fresh angle, through out-of-the-box thinking. The reader should bear in mind, however, that the barrier towards implementation will be naturally higher than the short-term and mid-term recommendations.

iii. Key topics – In order to come up with relevant short and mid-term recommendations, the study team has investigated in depth ten key topics. Each of these topics – set out in Chapters 4 to 13 – deal with particularly important, problematic or contested issues in the online environment.

iv. Legal instruments – In Chapter 14 (Annex), each of the most important EU legal instrument is separately covered, to identify its gaps, inconsistencies and future readiness, in a discussion of its relevant articles. This annex builds upon the issues identified in Chapters 4 to 13.

v. Theoretical and practical approach – It is the clear aim of the study to go beyond the theoretical level, and also come up with practical recommendations — particularly for the short-term — that have a clearly identified impact on all stakeholders. "Practical" also means that the recommendations have been corroborated by stakeholders through workshops, as well as through various interviews.

vi. Key trends, challenges, values & solutions – The study emanates from the observation that the EU's current legal framework for the information society is increasingly thwarted by trends that are taking place at an unprecedented speed (such as increased end-user participation, permanent connections to the network and new approaches to privacy). These key trends pose numerous challenges for today's society and its legal framework, as further discussed below. Throughout the study, it is investigated how the existing legal rules can be adapted to cope with these new trends and find solutions for today's challenges. In coming up with recommendations, the study takes into account the core European values.

2.4. Topics and legal instruments out of scope

The EU legal framework for the information is quite extensive and directly or indirectly touches upon many different subjects. In the picture below, we illustrate which topics we currently consider most relevant for the information society (located within the concentric green circles), taking into account the key trends and key challenges described in the remainder of this chapter.

Furthermore, three core topics – highlighted in white in the picture above – are not covered by the study, although it is acknowledged that these legal instruments constitute an important part of the information society legal framework:

- The telecom legal framework as such, as this legal framework is being reviewed during the course of the study

The consumer acquis (including in particular the Distance Selling Directive 97/7/EC), as this framework is also being reviewed.

The VAT legal framework for the information society, as this framework was recently revised through Directives 2008/8/EC and 2008/9/EC.

3. Key trends that affect the legal framework

3.1. Omnipresence of the Internet

Background – In the last decade, there has been a gradual replacement of dial-up modems by broadband connections, a technological evolution in which several European countries have proven to be among the frontrunners. In 2008, the milestone of 100 million European broadband subscribers was crossed, bringing the EU Member States one step closer to a true Single European Information Space. The roll-out of VDSL2 networks and fibre-to-the-home promises even higher speeds in the coming years, while the "digital dividend" (the wireless spectrum that has been freed up in the switchover from analogue to digital terrestrial TV) will increase the availability of mobile access. The big success of portable devices such as laptops and (3G or even 4G) smartphones has stimulated nomadic use and has set a trend towards technological convergence.

The rapid spread of broadband and wireless access has resulted in an almost permanent connectivity at home and at work, at speeds that allow bandwidth-demanding and interactive applications. This has resulted in a growing integration of the Internet into our lives, a new breed of services and an ever-increasing dependence on the Internet. The Internet has thus become (part of) the fabric of our lives.

Legal issues – The permanent connectivity and the evolutions in communication technology have created frictions with the existing legal framework, which is for a large part still primarily focused on the offline environment. Although the existing legal instruments (such as the eCommerce Directive and the Data Protection Directive) claim to take a technology-neutral approach, they are clearly targeted at traditional delineated transactions between a limited number of parties (typically a webshop and a customer), involving a limited amount of data being stored in a manageable scenario.

---

10 See http://ec.europa.eu/consumers/rights/cons_acquis_en.htm
11 Denmark and the Netherlands occupy the top positions in broadband penetration, followed by Sweden and Finland. Although the take-up of broadband is unevenly distributed across the EU, the gap has been reduced slightly in 2008. The Commission and many Member States are taking initiatives to further reduce this gap: see Europe's Digital Competitiveness Report, 4 August 2009, available at http://ec.europa.eu/information_society/eeurope/2010/docs/annual_report/2009/sec_2009_1060_vol_1.pdf, p. 9
13 See for example Belgacom (www.belgacom.be/private/en.jsp/dynamic/product.jsp?dcrName=hbs_vdsl_res), UPC (www.upc.nl/internet/fiber_power_120/) and Deutsche Telekom (www.t-home.de/Neuanschluss_DSL). These three providers are amongst those offering high-speed (VDSL or Fibre-based) broadband.
Today’s Web 2.0 services involve data flows transferred across the globe, transferred between “data clouds” by combined web services managed by multiple parties, replacing “one-shot” transactions of the Web 1.0 era with constant transactions via almost permanent data connections. The very purpose of technologies such as cloud computing, software-as-a-service and webservice mash-ups is to outsource and combine data processing and data storage in the most efficient (often decentralised) way, using whichever party or technology is deemed most suitable. These technologies often make it impossible for a data controller to know which parties are involved in the data processing, or where data is stored.

The existing legal instruments do not provide adequate answers to the liability and data protection questions triggered by the omnipresence of the Internet. Questions such as who is owner of the data being processed, and which parties in a chain of processing commands can be held liable, have become increasingly difficult to answer. Even relatively straightforward requirements, such as the information requirements set forth in articles 5 and 10 of the eCommerce Directive, have become difficult to apply, considering that a substantial number of client devices have small screens (PDAs or smartphones) or rely on data streams that only allow a limited number of characters (transactions by SMS).

3.2. **New ways of doing business**

Description – Evolutions in communication technology have already influenced business processes and culture to a great extent. The Internet has enabled companies to communicate and collaborate more efficiently and at a lower cost, largely independent of geographical boundaries. The Internet has also facilitated the birth of a new breed of companies, such as online stores, search engines, social networking sites, hosting providers, online financial services and storage services, some of which have quickly gained a strong foothold in the market.

In addition, the Internet has "upgraded" traditional service models (such as bookstores and music shops) with new digital features, allowing unlimited shelf space and personal shopping recommendations based on statistical information collected from other customers. Companies like eBay have reinvented the traditional auction model, and lifted this concept to a new level. Online trading communities for video games, books, music, movies, and other items have grown beyond the size of their traditional antipodes.

Rapidly diminishing costs of processor power, bandwidth and storage have also led to a new line of business models that essentially offer services free of charge to the majority, or even all of the users (the so-called "freemium" model). This business model was not possible in an offline environment, where shelf space and staff costs were prohibiting factors to really offer services for free. While some offline business models also promised "free" services, almost all of these services were hiding or shifting the costs to other places.

Although in 2007 only 4.2% of the total turnover of enterprises stemmed from e-commerce, the relationship between businesses and consumers has also been affected by the technological changes. Small and medium businesses can use the Internet to communicate with a global audience, a feat

---

17 For example, fast-food drive-in franchisees can outsource the taking of orders to a central location hundreds of kilometres further away, increasing order processing speed, cutting mistakes by half, serving thirty additional cars each hour and increasing customer satisfaction. See T. L. FRIEDMAN, *The World is Flat* (updated edition), 2006, p. 48
19 For example, the site Game Trading Zone has 179,187 confirmed trades since October 20, 1997. Source: http://gametz.com
20 C. ANDERSON, ibid.
21 Eurostat Information society statistics on E-Commerce via Internet, see http://ec.europa.eu/eurostat
previously reserved for multinationals with a worldwide store network. Costs for the distribution of goods and services have diminished, as there is no more need to have physical points of sale in every area of distribution. Some services are distributed in an entirely new way: the emerging22 "software-as-a-service" (SAAS) distribution model, for example, makes software available to customers as a service across the Internet, instead of requiring the customer to install the software on his computer.

Legal issues – Although, as a result of technological evolutions, consumers can easily engage in cross-border shopping, there are legal barriers that hinder the realization of a true internal market and undermine the potential of new savings promised by technological advances, as illustrated by the following examples:

- While e-invoicing promised to greatly decrease costs and increase speed of processing, the e-invoicing process is plagued by practical and legal barriers. Although companies have a great deal of freedom for guaranteeing the origin and integrity of electronic invoices23, the practical implementation of an electronic invoicing system is problematic for companies involved in cross-border transactions, due to additional requirements imposed by some Member States24.

- It is unclear which language requirements apply to web shops: should the entire website be available in the language of a country if a web shop is accessible from that country?

- It is also unclear to which extent aggregated statistical data gathered from the community can be considered personal data. The combination of data collected from web shops, search engines, etc. allows rather complete profiling of consumers. The European data protection advisory body "Working Party 29" has a very strict point of view in this respect and interprets the concept of "personal data" in a very broad way25: even dynamic IP addresses are considered personal data.

3.3. Focus on digital content

Background – The increasing bandwidth and processing power of computers have led to the predominance of digital content. Information in digital form offers many possibilities previously deemed impossible. Users can upload their own blog posts, pictures, videos and music, and view information uploaded by others (often collectively referred to as "user generated content"). New online services, such as digital photo albums, online collaboration tools and online video sites capitalise on the ease with which content in digital form can be exchanged. The combination of the abovementioned increase in connectivity and mobility and these evolutions on the content level, has resulted in "digital convergence": different kinds of content (e-mail, music, television, etc.) are available on different devices (desktop pc, notebook, cell phone, etc.), using different networks (wired, wireless).

The low cost and speed associated with the distribution of digital content have also brought about new distribution models, both using traditional "client - server" models (such as Apple’s iTunes26 or BBC’s

---

22 The market for software as a service is predicted to reach $11.5 Billion in revenue by the end of 2011. Source: Gartner (2007). See www.gartner.com/hyperlink.jsp?id=511899
23 EDI, advanced electronic signatures and any other means accepted by the Member State concerned
24 For example, Germany requires qualified signatures on electronic invoices, while Finland does not require any signature. As a result, it has been reported that it is problematic for a Finnish merchant to issue electronic invoices to its German customers.
26 According to Apple’s CEO Steve Jobs, iTunes had sold 5 billion songs as of June 2008, accounting for more than 70% of worldwide online digital music sales. See www.apple.com/quicktime/qtv/specialevent1008.
iPlayer\textsuperscript{27} and using collaborative peer-to-peer technologies (such as BitTorrent and P2PTV). Some content creators have resorted to Digital Rights Management (DRM) protection schemes, but these techniques have encountered resistance, as they limit the control users have over content they buy.

**Legal issues** – Among the legal issues associated with this trend, are questions regarding the application of existing legal instruments to the new services that have emerged as a result of the success of digital content, online liability for content, piracy, DRM and open source.

Copyright laws do not seem to appropriately reflect the day-to-day reality on the Internet, where users (particularly “digital natives”, i.e. those born after 1980, who grew up in the digital environment) copy photos, music and texts without permission — often unaware of the fact that they breach the law. These users are caught in a fundamental “copyright paradox”: never before have copyrighted works been so important to consumers (and minors in particular), yet never before have users disrespected copyright in this amount. Aware of this paradox, rights holders start lawsuits, hesitate to sell digital works online, or sell digital works that are overly protected and consequently do not allow users to enjoy their legal exceptions.

Another issue associated with digital content, is the possibility of reuse. The widespread online availability of digital content makes it very appealing to create derivative works using this content. However, such reuse is often not allowed, due to the strict exceptions found in the EU Copyright Directive. The “fair use” doctrine in the US is sometimes proclaimed to offer a higher degree of flexibility in comparison with the limitative, non-harmonised set of exceptions in the EU Copyright Directive. This indicates that a new balance may need to be found between protecting the legitimate rights of the content producers and allowing information to be shared without excessive restrictions.

Yet another issue concerns DRM, installed to counter digital piracy. Although DRM is often deemed indispensable in a digital environment due to the possibility of easy and perfect copying of digital works, the use of DRM has led to consumer complaints\textsuperscript{28} and legal issues\textsuperscript{29}. Adverse to the trend towards increased control over digital creations (of which DRM is a manifestation) is the “open source” software movement, as well as the related free licensing schemes (such as Creative Commons) for other types of content. Such licenses encourage, instead of restrict, the reuse of content.

### 3.4. Community building

**Background** – The internet has evolved from a medium allowing limited two-way information provision in the mid nineties to what has been called “Web 2.0”: a mature, distinctive medium characterised by **user participation**, openness, mass collaboration and network effects\textsuperscript{30}. Properly channelled, Web 2.0 means connecting minds and creativity on a scale never before imagined\textsuperscript{31}. In the enterprise environment, it is expected that these collaboration tools will generate an “Enterprise 2.0”\textsuperscript{32}.

\begin{itemize}
    \item \textsuperscript{27} In 2008, the iPlayer accounted for 5% of UK internet traffic. See www.guardian.co.uk/business/2008/apr/30/technology.virginmedia
    \item \textsuperscript{28} www.nytimes.com/2007/05/03/technology/03code.html
    \item \textsuperscript{29} For example, the term “effective” in article 6 of the Copyright Directive concerning technological measures to protect copyright has been the subject of much debate.
    \item \textsuperscript{30} T. O’REILLY, “Web 2.0 Principles and Best Practices”, O’Reilly Radar Report
    \item \textsuperscript{31} V. REDING, SPEECH/08/616, “Digital Europe: the Internet Mega-trends that will Shape Tomorrow’s Europe.”
    \item \textsuperscript{32} Communication on future networks and the internet, COM(2008) 594 final, page 4
\end{itemize}
Social networking sites such as Facebook, Myspace and Netlog have attracted a huge and mainly young audience, and have taken their place among the highest ranking websites in the world\textsuperscript{33}. Users are encouraged to upload pictures, videos or music to complement their virtual identity. Online role playing games and virtual worlds such as World of Warcraft, Eve Online and Second Life allow large scale interaction in a 3D environment, giving rise to virtual online economies. So-called "wiki's" allow end-users to jointly create manuals, encyclopaedias or even novels. Millions of media buffs now use blogs to add their voices to a vociferous stream of dialogue and debate called the "blogosphere"\textsuperscript{34}.

Community building even occurs in more subtle ways, for example with websites that provide recommendations on the basis of the direct input or indirect input (surfing, buying or listening behaviour) of millions of users — a entirely new phenomenon which is dubbed "crowdsourcing". Business models built around crowdsourcing and reuse of user-contributed material seem to become central in tomorrow's online business, creating a "hybrid" economy where the efforts of service providers and end-users are intertwined\textsuperscript{35}.

One of the best example is the "long tail" in online retail. Due to the fact that online web shops are not bound by real-world limitations, they can have unlimited "shelf space" for their products, so that they can offer an almost unlimited product assortment to their customers. Online retailers that indeed offer a very wide selection of products, have observed that — contrary to their expectations — a very large percentage of their sales is generated by products that are not "mainstream" or "popular" (the so-called "tail" of products). Even more interesting is the observation that even the most specialised niche products are being sold. Although the individual quantities for each such product may be very low, the aggregate sales for all niche products together often amounts to 40% or even 50% of an online retailer's total sales volume.

Contrary to offline shops — which pre-select available content and typically only offer the best-selling products — online shops can therefore significantly contribute to cultural diversity, which is an important value in Europe. However, it is also observed that "long tail" sales only work in practice when sufficient guidance is offered to customers (e.g., Amazon's "other readers have also bought..." statements). Crowdsourcing is essential to this guidance.

The Internet has arguably become the most powerful tool to date for spreading information. The possibility to reach a huge audience at a negligible cost has stimulated businesses, grassroots activists, governments and marketers to use the medium to engage people in their activities. The internet has not only become a powerful tool for spreading information, it has also proved quite effective in supporting collaboration. The open source software model, for example, is a form of distributed, collaborative, asynchronous, partly volunteer, software development\textsuperscript{36}.

Legal issues — Legal systems are typically focused on straightforward one-to-one relationships, for example a commercial transaction between a supplier and a customer, or extra-contractual damage caused by one party to another party. They are not typically designed for dealing efficiently with contractual issues or liability cases caused by several persons at once. Numerous questions can arise in this context, for which no clear answers exist in the current legislation:

- Which contributors can be held liable in case damage is caused to a third party?

\textsuperscript{33} At the time of writing, the Alexa rankings of Facebook, Myspace and Netlog are respectively fifth, seventh and sixty-sixth. See www.alexa.com/site/ds/top_sites.

\textsuperscript{34} D. TAPSCOTT and A.D. WILLIAMS, Wikinomics. How mass collaboration changes everything, 2006, p. 1


\textsuperscript{36} FP. DEEK and J.A.M. McHUGH, Open source. Technology and policy, Cambridge University Press, page 159. The term "open source" is actually more complex, and encompasses several aspects at once. See the open source definition at www.opensource.org/docs/bsd
How should the responsibility between users and service providers be drawn, when the service provider re-uses and re-compiles material uploaded by the users?

Should the anonymity of contributors be preserved in case of illegal content?

Is it fair for terms & conditions to stipulate that the ownership of uploads and creations automatically transfers to the service provider?

Is it fair and democratic that an online community of millions of people is, in many cases, centrally ruled by only a handful of people?

To which extent can semi-anonymous profiling data be used for crowdsourcing purposes?

For example, it is not clear whether "abstract" profiling activities are subject to the Data Protection Directive. If this is the case, then the accompanying data protection rules may become inhibitive due to the many restrictions that apply.

Another example is the Audiovisual Media Services Directive. This Directive only applies to service providers that exercise "editorial responsibility" over audiovisual content. It is not clear to which extent a video platform with user generated content (such as YouTube) falls within the scope of this definition, as it is difficult to argue that such platforms exercise "editorial control" over the millions of videos uploaded to its platform.

Yet another issue is how communities can be made responsible for the data they create. Under the current special liability regime of the eCommerce Directive, hosting providers are not liable for third party content hosted by them (as pointed out in Chapter 6, this protection is not always correctly applied in practice). Accordingly, the platform operator is not responsible for the content created by "the community". However, the question then arises who can be held liable for this content, as it is often difficult to track down individuals within a collectivity of million members.

A fourth issue is the "democratic deficit" legal gap of some online communities (see section 4.10).

The online legal framework should take into account the special concerns generated by online communities. The legal rules should consider these issues, yet should also allow the accompanying business concepts to flourish, by removing unnecessary legal hurdles that deal with these online communities.

3.5. Individual-to-community (I2C)

Background – Almost paradoxically, the Internet has not only facilitated community building, but has also facilitated the power of the individual, who can directly reach the community at large through the Internet (end-to-end).

For example, many individual bloggers have become very influential, sometimes with daily pageviews approaching one million. Similarly, some persons have millions of persons who have subscribed to their micro-blogs (such as Twitter messages), allowing one individual to directly reach millions of readers. Even when such bloggers are employees of a company, the public perception detaches their individual reputation from their companies, focusing the attention on the individual instead of on the company.

Many artists have become famous through the Internet, for example due to their personal videos on YouTube. Other artists have single-handedly launched (or is it confirmed?) new business models on the Internet. New innovative business models allow individuals to directly lend money to other

37 For example, Daily Kos (politics), Jason Calacanis, The Blog Herald, Jason Kottke and Hylton Jolliffe. A famous recent example is the fashion blog of the thirteen year old Tavi Gevinson.

38 For example, Tyra Banks, Marie Digby, Savannah Outen and Esme Denters

39 See, for example, Radiohead, which distributed its album on the Internet for free, asking only voluntary donations in return.
individuals\textsuperscript{40}. Individual messages broadcasted online can make\textsuperscript{41} or break a product\textsuperscript{42}, can make a person world famous in a very positive way, but can sometimes also make a person equally famous in a very negative way\textsuperscript{43}.

This trend is what we would call "individual-to-community" (I2C), a new kind of context that exists parallel to the business-to-business (B2B) and business-to-consumer (B2C) contexts. Due to the world wide exposure made possible through the Internet, individuals have become empowered by the Internet, and are enabled to individualise the Internet to define their own user experience.

\textbf{Legal issues} – Most liability and defamation laws simply do not take into account the worldwide effects of one’s actions. The current legal framework of international private law provides complex referral rules to be applied by the judges of each Member State. It is difficult to determine which laws apply and which courts are competent in such cases, so that these issues alone will often make harmed party refrain from any legal redress.

Furthermore, many legal obligations are primarily targeting professionals, excluding consumers. The question then arises to which extent the current legal rules apply to influential individuals, who may act as a consumer instead of as a professional.

\section*{3.6. Smart objects and ambient intelligence}

\textbf{Background} – Terms such as \textit{"the Internet of things"}, \"ubiquitous computing\", \"ambient intelligence\" and \"smart objects\" are all related to the description of another potentially disruptive technological evolution. They refer to the vision that technology will become invisible, embedded in our natural surroundings, present whenever we need it, enabled by simple and effortless interactions, attuned to all our senses, adaptive to users and context-sensitive, and autonomous\textsuperscript{44}. Examples include personal biometric monitors woven into clothing and refrigerators that are "aware" of their contents, able to both plan a variety of menus from the food actually on hand, and warn users of stale or spoiled food\textsuperscript{45}.

Radio frequency identifier (RFID) tags, chips that can be used for identification and tracking purposes using radio waves, are already being used on a large scale for supply chain management, animal tracking, passport control and other purposes. Worldwide revenue for RFID technology is forecasted to total $1.2 billion in 2008\textsuperscript{46}, and is expected to grow five times by 2018\textsuperscript{47}. E-health applications, such as the monitoring of vital health parameters, are being developed, and are expected to be very successful, considering our aging demographic. The seamless connection of objects through the Internet promises to allow far-reaching control over our environment\textsuperscript{48}.

Another promising area is near-field communications (NFC), which is used for mobile payment and mobile ticketing in public transport.

\textsuperscript{40} See, for example, Zopa.com

\textsuperscript{41} See, for example, Andrew Milligan's "bean bag" (www.sumolounge.com), which became popular only through a blog post.

\textsuperscript{42} See, for example, the "Dell Hell" case of Jeff Jarvis, who single-handedly initiated the reorganisation of Dell computer's customer care service, after blogging about a bad experience (C. ANDERSON, \textit{The long tail}, edition 2009, page 233).

\textsuperscript{43} See, for example, the case of the Finnish shooter "wumpscut86".

\textsuperscript{44} W. WEBER, J. RABAЕ and E. AERTS, "Introduction", in \textit{Ambient Intelligence}, Springer, 2005, page 1


\textsuperscript{47} Communication on future networks and the internet, COM(2008) 594 final, page 5

\textsuperscript{48} See the Commission Recommendation of 12.5.2009 on the implementation of privacy and data protection principles in applications supported by radio-frequency identification - C(2009) 3200 final
Legal issues – The legal issues that will need to be addressed concern primarily the protection of privacy rights and the security of data. The 1995 Data Protection Directive was created on the premise of centralised mainframes, a view that will no longer hold true when millions of independent devices such as RFID chips and smart objects all process data. The question arises whether the strictly confined setup of the Data Protection Directive can be aligned with this new environment.

Some specific questions raised by smart objects, include the issue of who exactly is allowed to exert control over the devices constituting the Internet of things, who will be liable in cases where failure of one of the connected devices causes damage, and how contracts can be established through the mediation of these devices. The industry is aware of the suspicion that some have towards these technologies, and that initiatives have been taken to remedy some of the critic. For example, EPCglobal's second generation standard provides for a kill-switch, which allows users to permanently disable the RFID tag in a product. It remains however yet to be seen if such forms of self regulation can suffice to meet the objections voiced by experts and the public opinion.

Another issue is the security of these millions of devices. The Commission has already recognised that the efforts required to ensure the security and integrity of networks and services must be accelerated to guarantee that Europe can show international leadership on the global stage.

3.7. A data-driven world

Background – Collecting data has become commonplace. Unlike people born into previous generations, those who are born digital will grow up to have a large number of digital files kept about them – whether they like it or not – and these files begin to accumulate right from the moment of birth. On the Internet, cookies gather visitor information and search engines store searches. Website visitors, some quite young, willingly provide personal information to social networking sites and online stores. In finance, databases containing credit card and social security numbers are accumulated by financial institutions. Even in the offline world, navigation technologies allow for indoor and outdoor localization.

The Internet has evolved to a pervasive platform that is used for a variety of purposes, leading to enormous amounts of information being collected in a decentralised fashion, because virtually all of our digital acts can be captured and stored in databases. As our society starts to rely more on the Internet to communicate with and provide services to its customers and citizens, adequate protection mechanisms to safeguard the data in possession of public and private entities needs to be put in place, to safeguard the privacy of individuals.

Legal issues – The boom in the gathering, storage and use of information urges an assessment of the existing instruments regarding privacy and data protection. The current EU data protection legislation assumes that limited amounts of data are stored by a small number of parties, in a centralised and manageable way. Conversely, today's internet features numerous parties collecting personal data in a decentralised way, with reuse of personal data – often for purposes of direct marketing – being the rule.

49 For information on EPCglobal see www.epcglobalinc.org/about.
51 See the "Communication on future networks and the Internet", COM(2008) 594 final, page 10
53 See, for example, the Belysio service, which allows users to constantly convey their geographical location to other users of the service.
instead of the exception. When a person’s privacy rights are violated, it is not even clear which law will apply, as privacy and data protection violations are excluded from the Rome II Regulation.  

Collecting personal data has even become a viable business model on itself, allowing a new generation of Web 2.0 websites to survive without other sources of revenue. Although online services often operate under a veil of lawfulness by requesting the user’s prior consent, the question arises whether this consent can be deemed valid, as privacy policies are often long, non-standardised and simply not understandable for non-lawyers, so that they are almost never read. Even so, while they do not read the privacy policy, many users seem to be concerned about their privacy. Still other users – particularly children and teenagers – seem to adopt a new position towards privacy, deliberately reducing their level of privacy protection, due to the new incentives to reveal information online about oneself.

The discrepancy between the philosophy of the data protection legal framework and the way internet businesses treat personal data, is therefore highly similar to the aforementioned discrepancy between copyright legislation and everyday use of digital content.

3.8. Convergence

Background – The concept of convergence has many applications in the online context. There is convergence of media, such as television shows that refer to websites for more information, newspapers that print user comments submitted online, and cross-media campaigns that simultaneously cover many media. Many new television sets can be connected to the Internet to allow users to watch online video fragments (e.g., on YouTube). Conversely, many movies and television shows are broadcasted in a digital format, or can be ordered on demand through the Internet via set top boxes.

There is also a convergence of the online and the offline context, due to the arrival of new technologies and new devices that are permanently connected to the Internet. For example, new cell phone services (such as Belysio) allow citizens to permanently track the geographic position and whereabouts of their friends and family; new communication technologies allow medical diagnosis and treatment at a distance; the new concept of “augmented reality” literally blends the online and offline context on a digital device by integrating in real-time information about the surrounding real world in the user interface of a device; cycling champions Twitter during their activities and criticise each other through public text messages.
More recent is the observation that increasingly, **online concepts are being "mirrored" in the offline environment**, or that online concepts are used to define and explain offline activities. While the reverse has been true as from the very conception of the Internet, the "online reflection" is a recent trend that may be the best illustration of the state of convergence between the online and offline world.

For example, abbreviated language and "emoticons" typically used in electronic message are trickling into offline texts; companies start to organise offline mass games that resemble typical online games such as World Of Warcraft; television shows allow customers to send messages in real-time to publicly provide comments on the show; the concept of "open source" software has given rise to open source beer recipes; offline products such as cars can now also be ordered with a limitless variety of replaceable exterior parts, effectively mimicking the customisation / personalisation options found on many websites and software packages.

An interesting illustration of this trend is the "offline store" cartoon, available at [executiveeducation.wharton.upenn.edu/ebuzz/0508/images/cartoon2.jpg](http://executiveeducation.wharton.upenn.edu/ebuzz/0508/images/cartoon2.jpg).

**Legal issues** – Existing legislation is for a large part still primarily focused on the offline environment. In most of the cases where the online context has been taken into account, separate legal rules have been adopted for the online world. This legal duality is no longer justified in an era where the online and offline context are increasingly intertwined, particularly for the digital natives.

An interesting example is the 2007 Audiovisual Media Services Directive, which is still primarily focused on traditional concepts in the offline audiovisual environment, although one of its main goals is to be better suited for the online environment. For instance, one of the Directive's crucial criteria is the "editorial responsibility" of a media service provider, which is defined as "the exercise of effective control both over the selection of the programmes and over their organisation". It is not clear to which extent a commercial online video platform such as YouTube falls within the scope of this definition, as it is difficult to argue that YouTube exercises "editorial control" over the millions of videos uploaded to its platform (YouTube only removes illegal content on request). Instead, it could be argued that "the community" exercises this control. However, the Directive does not take into account such decentralised organisations, and only focuses on traditional, centralised control hierarchies.

### 3.9. Digital natives

**Background** – An ever-increasing part of a typical minor’s life is to be situated in the online context. Digital natives stand out as the most regular, intensive users of internet advanced services, who fully exploit the many possibilities offered by the web, and are twice as inclined as other users to pay for services online. As have so nicely described J. PALFREY and U. GASSER: "You see them everywhere. The teenage girl with the iPod, sitting across from you on the subway, frenetically typing messages into her cell phone. The whiz kid summer intern in your office who knows what to do when your e-mail client crashes. The eight-year-old who can beat you at any video game on the market—and types faster than you do, too. (...) All of them are "Digital Natives."

**Legal issues** – Contrary to "digital immigrants", digital natives use other legal paradigms. They no longer seem to make a sharp distinction between the online and the offline context, or the "public" and the "private" context. All these contexts are woven into one context: "their world". Digital natives expose their privacy in ways that are astonishing; they download digital material while only vaguely recognising that this downloading may infringe third party copyright; they have different habits, practices and ethical codes that may be hard to grasp for outsiders.

---

62 See [www.opensourcebeerproject.com](http://www.opensourcebeerproject.com/)


64 Ibid., page 57
While the discrepancy between the current legal framework and the behaviour and value set of digital natives may not be threatening at first sight, one should realise that today's digital natives will have important purchasing power tomorrow, and will soon become political decision makers, for whom the established (offline) values feel progressively unnatural. Hence, given current trends, any distinction between the digital environment and the offline environment will have become largely academic by 2025.\(^{65}\)

### 3.10. Rise of cybercrime threats

The reliance on the Internet opens the door for malicious attacks on networks, websites, services and databases. The profound changes brought about by the digitisation, convergence and continuing globalisation of computer networks have increased the risk that computer networks and electronic information may also be used for committing criminal offences. Indeed, in addition to amateur attackers, professional hackers and organised crime are starting to use highly sophisticated attack tools to access private and otherwise valuable information, or gain control of the computer itself, forming so-called "botnets", that organise attack services for money.\(^{66}\)

As our society will become even more dependent on smart digital systems in our core infrastructures, it can be expected that cybercrime threats will further increase.\(^{67}\)

**Legal issues** – The cybercrime threats undermine the trust of consumers and companies in the online society, hampering the further uptake of electronic commerce. Furthermore, the threat of cybercrime also causes legislators to become (overly) cautious when enacting rules for the online world, which often leads to practical

It is acknowledged by the European Commission\(^{68}\) that the fight against cybercrime is a significant challenge. However, the fight against cybercrime is often obstructed by cross-border legal issues, such as competent jurisdiction, applicable law, cross-border enforcement, and lack of evidence. Traditional cooperation between European member states (e.g., through Europol and Eurojust) has proven to be slow and ineffective when dealing with cybercrime, and new cooperation structures have not yet been sufficiently developed.

Another legal issue is that the threat of cybercrime seems not yet reflected in the "bonus pater familias" model of good online citizenship. Courts do not yet know to which extent they can hold consumers or companies liable for not having taken adequate security measures (such as firewalls and malware protection). The question is to which extent intermediaries (such as access providers) should be held responsible for "clean internet", and to which extent this is also the responsibility of the end-users.

---


\(^{67}\) European Internet Foundation, *The digital world in 2025 - indicators for European Action*, www.eifonline.org/site/download.cfm?SAVE=10859&LG=1, page 28

\(^{68}\) A good example is e-invoicing, which is subject to many stringent security measures. Paper invoices, on the other hand, are not subject to such additional security measures. Similarly, some electronic signatures (the so-called "qualified" electronic signatures) are subject to more than thirty requirements.

4. Challenges faced by the legal framework

Due to the various trends outlined above, and the emergence of new technologies, the legal framework for the online society is exposed to many challenges (as illustrated below). The most important challenges are described in this section 4.

4.1. Legal duality

Most of the laws that were enacted to respond to the legal questions arising in the online environment, demonstrate a tendency to legal duality, i.e. treating the online environment differently than the offline environment.

For some aspects, this duality is obviously justified, because the online and offline context have different characteristics. For example, current electronic signatures operate in an entirely different way than traditional handwritten signatures, and necessarily require the involvement of a third party, so that a special legal framework becomes imperative.

For other aspects, this duality was entirely justified at the moment the online legal rule was adopted, although the question now arises whether this justification is still relevant in all cases. For example, in the online environment, an "opt-in" requirement applies to most unsolicited electronic communications due to overload of e-mail spam. In the offline environment, however, an "opt-out" requirement applies to unsolicited paper communications, so that many people receive significant amounts of paper publicity that gets thrown away immediately. Another example is the "cooling off" period (cancellation right) for distance sales. While this cancellation right was introduced to boost consumer confidence in distance sales, this right may have become too protective for those goods where sensory perceptions are not required for making a correct purchasing decision.

For many other aspects, a separate legal treatment is no longer justified. For example, electronic invoices are subject to a variety of specific rules that intend to secure the electronic invoice, while such

---

70 E.g., buying an external hard drive, a book or a DVD online. In many cases, it may even be easier for a consumer to obtain an informed decision when buying online (where online reviews are online a mouse click away), as compared to buying the same goods offline (in a busy shop, where sales people may not have personal experience with the goods being sold).
rules do not apply to traditional paper invoices. Another example is the transparency obligation of online shops, which – according to the European Court of Justice\textsuperscript{71} – requires the shop operator to provide 24/7 telephone access to its customers.

While legal rules should take into account the distinctive traits of the online environment, the deep-rooted duality may no longer be appropriate in an era of pervasive internet connectivity, inherent convergence, hybrid services and increasing participation of digital natives.

The challenge is therefore to find a reasonable balance between a harmonised set of rules that would simultaneously apply without discrimination to both contexts (online and offline), but would nevertheless deal in an appropriate way with the specificities of each context.

4.2. "Cold feet"

In addition to the legal duality, the current online laws also show significant formalism, which demonstrate that the legislator does not fully trust the digital environment. For example:

- The electronic contracting principles of the eCommerce Directive do not apply to real estate, family law and succession-related contracts, giving the impression that only for "less important" contracts it should be possible to contract online\textsuperscript{72}.

- Online service providers must announce in advance whether or not the concluded contract will be filed by the service provider, and which language(s) will be offered for the conclusion of the contract. Furthermore, they must take an additional step to explicitly confirm each online order. No such formalities apply in the offline world, where most contracts can be concluded by sheer consent of the parties.

- Stringent security measures are imposed on electronic invoices. Conversely, no security measures apply to traditional, paper invoices.

- The eCommerce Directive establishes the "country of origin" principle, to avoid that online service providers would be faced with certain technical requirements in local laws which would unduly restrict freedom to provide services. However, this country of origin principle does not apply to the requirements applicable to physical goods as such, or the requirements applicable to the delivery of goods.

These formalities create practical hurdles and significant administrative overhead for online service providers, and undermine the future-readiness of the legal rules. Both the formalism and the legal duality can be understood as the reaction of a legislator who had "cold feet" to regulate in unknown and fast-evolving territory, and who did not trust the new digital environment.

4.3. Online naivety

Despite the Internet's pervasiveness and the increasing familiarity with the online environment, there exist many cases where society has not yet developed online customs, even though the offline counterparts are obvious and deeply rooted. Examples of such undeveloped online customs include:


\textsuperscript{72} See article 9 of the E-commerce Directive
- **Clicking is binding** – While every citizen will instinctively "think twice" before putting a signature under a document, many citizens do not realise that the online equivalents (such as the click of a mouse) can result in an equally binding legal transaction.

- **Using corporate e-mail for personal purposes** – While an average employee would never write a personal letter on corporate letterhead paper, many employees will use their corporate e-mail account for personal purposes. The legal repercussions of this mix of personal and corporate elements is not yet clear.

- **The Internet does not forget** – Average citizens will refrain from publishing their most private discussions or pictures in the newspapers. Yet, these same citizens will not hesitate to post the electronic equivalents on social networks or discussion boards — often failing to realise that these electronic discussions and pictures are there to stay.

- **There is no such thing as online anonymity** – Many citizens assume that they can anonymously use online services from their computer. Almost paradoxically, however, is it that in many cases it has never been easier to follow an individual's online traces. For example, some employees assume they can anonymously edit Wikipedia entries about their own company (or a competitor), until a third party publicly exposes who is linked to the IP address registered by Wikipedia.

- **Disrespect for others** – Citizens not only post private information about themselves online, but also post information about other citizens, while failing to realise that this information may be harmful. Examples include blog posts and social network posts "this is John at the local bar at 3am, who had a drop too much".

- **"Alice in Wonderland"** – Some citizens see themselves as Alice in Wonderland when visiting the online world: as everything looks nice, they sometimes fail to realise that the online world can seriously hurt, and that many actions are not entirely free of engagement.

- **Lacking security** – Careful citizens lock the door of their house or car, will not let unannounced strangers into the house and will refrain from visiting suspect neighbourhoods. These same citizens often neglect to update their virus scanner or install a firewall, will eagerly respond to a spam e-mail or install cool-looking software, and will almost always skip creating backups of the most important electronic documents.

Courts know how to deal with breaches of the offline customs: an employee uses corporate letterhead for personal purposes, or carelessly handles paper invoices, is likely to be sanctioned. Yet, society at large and courts in particular do not know how to handle the counterpart infringements performed online, due to a lack of established online customs and an insufficient understanding of all concepts and implications of the online environment. As a result, court reactions range from ignoring online issues, to setting the bar of the “bonus pater familias” standard too low for the online environment.

### 4.4. Privacy leakage

The trend of ever-increasing flows of personal data on the Internet concern users: statistics point out that 66% of internet users are concerned about leaving personal information on the Internet. Indeed, evolutions such as geographical localization, RFID tags and ubiquitous computing even have the

---

73 See, for example, the August 2009 case of two students who were boasting there cheating efforts, until the school board used the evidence as fraud to flunk both students: www.techcrunch.com/2009/08/25/facebook-conversations-used-as-evidence-in-exam-cheating-case/  

potential to result in 24/7 traceability. Almost paradoxically, however, many internet users do not refrain from giving away private information online.

Also, the businesses model of a significant number of – particularly online – service providers depends on sharing and reusing personal data, which has become the "new oil of the Internet and the new currency of the digital world". It will therefore be a challenge to find a reasonable trade-off between effectively protecting the privacy of citizens and providing sufficient opportunities for businesses, while at the same time ensuring that fundamental values such as freedom of expression and freedom of information are adequately respected. The problem of adequate privacy protection is exacerbated by the fact that we are just at the beginning of the digital age: no one has yet been born digital and lived into adulthood, and no one has yet experienced the aggregate effect of living a digitally mediated life over the course of ninety years.

An important part of this equation will consist of a reform of the current administrative and practical overhead involved with data protection issues. In practice, companies are confronted on a day-to-day basis with the various differences between data protection regimes across the EU Member States. For example, cross-country privacy audits for multinationals illustrate that data protection notifications are strictly necessary in some Member States, not necessary in other Member States, and sometimes necessary in still other Member States. Similarly, data protection authorities interpret rules in a different way, so that the export of the same personal data is allowed without formalities in one Member State, but strictly forbidden in other Member States. Although legal mechanisms exist (e.g., the Binding Corporate Rules or model clauses) to deal with some cross-border aspects of data protection legislation, there is a strong perception that a general overhaul may have become necessary.

4.5. Public support for established rules

Some legal frameworks do not seem to be supported (any longer) by a significant portion of the general public. This is particularly the case for data protection and copyright legislation, where many citizens have the impression that the current rules are outdated, overly restrictive and not aligned to their needs.

For example, in the field of copyright, one can observe a "copyright paradox", i.e. the situation that while content has never received more attention, there is a substantial neglect and disrespect for individual content. The switchover to digital content has indeed introduced new challenges in the field of intellectual property rights, including the use of technological means for fighting piracy.

As another example, citizens do not seem to care which national law applies to their online activities. Instead, they create their own rules and customs for the online environment, separate from the geographically bound national rules.

This lack of public support is especially relevant for minors (digital natives), whose online behaviour poses some very unique challenges. Due to new incentives to reveal information online about oneself, the level of privacy-awareness seems for young people to also have decreased, and their meaning of both "public" and "private" is shifting. In the field of online contracting, there is a discrepancy between the laws of most Member States, which only allow adults to enter into contractual transactions, and the daily practice, where children and teenagers frequently buy content and services online.

75 M. KUNEVA (European Commission), Keynote Speech on the Roundtable on Online Data Collection, Targeting and Profiling, Brussels, 31 March 2009
77 Ibid., page 54
Still, it is not clear how deeply rooted the resistance against current copyright and data protection legislation is. Many citizens – including minors – still believe it would be wrong for another citizen to reuse their texts or photos without proper accreditation. Similarly, while many citizens see no harm in posting their most intimate details on social networks, they do feel that their privacy is harmed when a friend would post a disgraceful photo on a publicly accessible profile. Certain aspects of the position towards privacy and copyright may therefore be shifting, but core values and principles may still be relevant.

4.6. Local versus global

The Internet is inherently cross-border: the mere act of sending an e-mail or visiting a website will trigger the transport of data streams across the globe. Users usually do not care where a server or service provider is located: they perceive many websites merely to be located "on the Internet" instead of "located in France" or "located in Hungary". This perception is particularly true for global brands and global websites, which are often perceived by users without reference to a particular country. In many of the emerging distributed service models – such as cloud computing and software-as-a-service – it is even no longer possible for many users (and service providers) to know the physical location of a server, as the decentralised nature of cloud computing prevents parties from mapping the geographical location of a server.

Still, many laws still use geographical criteria (territoriality) to define their applicability. Even laws that were specifically created to deal with the online environment, have been organised on the assumption that activities are on the whole geographically delimited, and that the right to regulate conduct is shared between geographically defined States on a predominantly geographic basis. This attachment to geographical criteria gives rise to many difficulties in the online context.

This issue is further aggravated by the fact that the geographical criteria are used in slightly different ways across the legal frameworks. For example, an online service provider is subject to the law of its country of establishment as regards the mandatory information to be published on his website, and as regards audiovisual media supplied by it (Audiovisual Media Services Directive). This same service provider is subject to the data protection laws of each Member State where one of its establishments processes personal data, is subject to the spam laws of each e-mail recipient's Member State, is subject to the defamation laws of the Member State of any citizen who feels harmed by its behaviour, and is subject to the consumer protection rules of the Member State of any consumer it deals with. Considering that legal cross-border relations are the rule rather than the exception in today's information society, the existing rules are too fragmented, overlapping and no longer adequate to deal with this evolution.

4.7. Weak enforceability

As e-commerce is becoming increasingly popular among European citizens, a larger number of cross-border disputes are destined to arise. Similarly, the increased participation in online communities, also gives rise to new disputes among the many members of the community.

Although Europe has pushed for alternative dispute mechanisms to be in place in the Member States (including the creation of ECC-Net), it is a challenge for legislators to come up with a cost-effective and fast dispute resolution procedure that respects the fundamental rights of parties. Moreover, even

---

78 Article 2.c of the E-commerce Directive recognises that the location of the technical means is not the relevant criterion to determine which Member State is competent to exercise its home country control over a service provider.

79 U. KOHL, Jurisdiction and the Internet, Cambridge University Press, 2007, page 4
when dispute resolutions are fast and cost-effective, it may be difficult to enforce the decision against a remotely located service provider. This weak enforceability is also linked to the above issue of the inherent cross-border nature of the Internet.

Resolving this conundrum is important, because it is a major hindrance to the further uptake of e-commerce. Indeed, 71% of consumers have indicated that a major inhibiting factor to their cross-border purchases are cross-border enforcement and redress while 39% of consumers think that it is harder to resolve problems such as complaints, returns, price reductions, or guarantees when purchasing from providers located in other EU countries\(^80\).

Not only consumers, but also online merchants are affected by this conundrum: according to a recent study\(^81\), 60% of cross border transactions could not be completed by consumers because the merchant did not ship the product to their country or did not offer adequate means for cross border payment. Cross-border enforcement issues were cited as one of the main reasons, in addition to the complexity of cross-border legal rules.

### 4.8. Endangered intermediaries

Intermediaries are important actors in the online environment, as they host the infrastructure and the software through which information is processed and on which online communities are built. While the eCommerce Directive has recognised the important but difficult role of online intermediaries and has introduced a special legal protection regime for some of these intermediaries, the position of intermediaries remains difficult. Courts do not know to which extent they should hold intermediaries liable for third party information processed by them; users do not know to which extent intermediaries can use the content they uploaded to the intermediary; governments want to lower the barrier to become an online intermediary, but at the same time impose policing functions on them; some (Web 2.0 and cloud computing) intermediaries that are key players today, are not covered as intended by the eCommerce Directive.

As from the moment an online intermediary gains sufficient popularity, its business model will be scrutinised, particularly from a copyright and patent infringement point of view. Accordingly, legal compliance and legal defence costs are becoming increasingly burdensome. Moreover, some intermediaries are pushed into the role of "online police officer" to monitor the behaviour of their users (and ban infringing users from their network), to ensure that no data transmitted by it infringes a third party's copyright.

Considering the crucial importance of these intermediaries, the question arises how a balanced situation can be created which sufficiently attracts players, yet also makes intermediaries responsible for certain aspects.

### 4.9. Network accessibility and free speech

Although Europe is one of the frontrunners with internet penetration reaching 48.1% of the population compared to 21.9% worldwide, the "digital divide" is still a reason for concern\(^82\). As the use of internet and broadband widens further, the risk of information exclusion for citizens that do not have access will

---


\(^82\) www.internetworldstats.com/stats.htm.
rise\textsuperscript{83}. This is the problem tackled by the principle "universal access", as set forth by the EU telecom legal framework. As this legal framework is currently being revised, it is outside the scope of this study.

A related issue is the \textbf{net neutrality}, \emph{i.e.} the question of whether network operators must treat the data that passes through their network as "neutral", or whether they are allowed to block some content or degrade access speed to certain network services. Governments are also increasingly attracted to block certain content, particularly when it concerns certain types of unwanted information (\emph{e.g.}, access to websites with terrorist information). These issues can have a fundamental impact on the future of the information society.

\subsection*{4.10. Democratic deficit of online communities}

The Internet has given rise to large communities of online citizens, built on top of both commercial platforms (\emph{e.g.}, eBay, MySpace, Second Life) and non-commercial platforms (\emph{e.g.}, Wikipedia and Linux development).

While such communities host thousands or even millions of members, \textit{the leadership of these communities is often highly centralised}, so that a handful of people can decide on the rules and direction of the community, and democratic decision procedures are not always equally represented. The question arises whether this situation is desirable, and how this democratic deficit can be countered — particularly in light of the fact that a significant part of many citizens' life depends on these online communities:

"More than 175 million people use Facebook. If it were a country, it would be the sixth most populated country in the world. Our [terms of service] aren't just a document that protect our rights; it's the governing document for how the service is used by everyone across the world. Given its importance, we need to make sure the terms reflect the principles and values of the people using the service." \textsuperscript{84}

Already, there are examples of large communities where users do not accept this situation, and have \textbf{protested} against new rules that were unilaterally imposed by the service provider\textsuperscript{85}. In the open source software community, such protests even occur regularly, as open source users always have the ability to create a new software product that is based on the contested software (the so-called "forking" process\textsuperscript{86}). The same applies to "open content" websites, such as Wikipedia\textsuperscript{87}. However, the pressure of creating a competing product is often not available for most other communities.

Sometimes, service providers have allowed their users to associate. For example, the eBay "Town Hall" meeting\textsuperscript{88} gives eBay members an opportunity to ask questions related to the eBay marketplace and to

\begin{itemize}
\item \textsuperscript{83} See, for example, the Commission Communication "How to transform the "digital dividend" into consumer benefits and up to €50 billion in economic growth for Europe?" of 10 July 2009 http://europa.eu/rapid/pressReleasesAction.do?reference=IP/09/1112&format=HTML&aged=0&language=EN
\item \textsuperscript{84} Mark Zuckerberg (Facebook CEO), http://blog.facebook.com/blog.php?post=54748167130
\item \textsuperscript{85} See, for example, the reaction of users against the decision of Facebook to change its terms and conditions: www.washingtonpost.com/news/2009/feb/19/facebook-users-speak-out-on-content-policy/. As a reaction, Facebook reverted the changes, and announced that its users would be able to provide input on future changes of the terms and conditions.
\item \textsuperscript{86} See http://en.wikipedia.org/wiki/Fork_(software_development)
\item \textsuperscript{87} See the Citizenium initiative, which was initially based on a copy of Wikipedia. However, the idea to use the existing articles of Wikipedia as a basis for further development, was abandoned in favour of emphasizing its own original articles.
\item \textsuperscript{88} See http://pages.ebay.com/townhall/
get answers from eBay’s leadership team. However, many of these initiatives are limited in scope, so that ultimately the real leadership of the communities remains highly centralised.

5. Findings per topic

These topics are explored in Chapters 4-13. A brief summary of each topic is set forth below.

5.1. The future of privacy and data protection

The emergence of Web 2.0 applications and services, new profiling and data harvesting business models, the semantic web and trends such as ubiquitous computing raise the question of whether the EU’s current data protection rules are still adequate.

A first issue is that the scope of the Data Protection Directive is too wide, mainly due to the excessive interpretation of the central concepts of “personal data” and “processing”. Furthermore, the Data Protection Directive’s provision regarding the applicable national law creates uncertainty, and often results in a situation where data controllers are simultaneously subject to the data protection rules of multiple Member States. As a result, both companies and private users are unnecessarily exposed to overhead caused by administrative data protection obligations.

Another issue consists of the rigid obligations for data transfers outside the EU, even though the Internet is inherently cross-border. In complex situations with multiple parties or with multiple countries involved, the possibility to transfer personal data outside the EU is unnecessarily restricted.

In addition, the Data Protection Directive imposes other onerous obligations on data controllers, for example by requiring notification of data processing activities. Moreover, it is not clear when a person or company qualifies as a “data controller”, as the distinction between data controllers and data processor only seems suitable to handle relatively straightforward situations.

Other problematic areas include the concepts of “sensitive data” and profiling data. The scope of the current concept of sensitive data is at the same time too large, too narrow, too vague and too diverse among Member States. As regards profiling data (which is becoming particularly important for Web 2.0 services), it is not clear whether such data constitutes personal data, and whether the processing of such data is subject to specific rules.

A final issue in the Data Protection Directive is the limited set of legal grounds for processing personal data. Although the consent of the data subject is the most commonly used legal ground in a typical e-business context, it is also the legal ground which is most commonly infringed. Other legal grounds are also problematic. For example, by limiting the “legal obligation ground” to EU law obligations, data controllers may find themselves in a situation where it is impossible to comply with both EU law and applicable foreign laws.

In addition to the issues created by the legal framework, additional shortcomings are caused by both Member States and data controllers. Member States have implemented the Data Protection Directive in different ways, which creates legal uncertainty for data controllers. Some Member States also fail to enforce data protection legislation effectively. Data controllers, on the other hand, often limit themselves to mere formal compliance with their obligations, without fully implementing data protection requirements in their systems and services. A fundamental rethinking of the data protection legislation has therefore become necessary.
5.2. Digital content and copyright

Over the years, many EU-level legal instruments and policy documents have been enacted in the field of copyright, the most important being the EU Copyright Directive and the Enforcement Directive. While both legal instruments have contributed to some harmonisation and market facilitation, both instruments also face many ambiguities, gaps and other shortcomings. Furthermore, the Copyright Directive and Enforcement Directive are not properly adapted to the online environment, and do not appropriately balance the rights of stakeholders.

Due to the limited level of harmonisation achieved by the Copyright Directive, there are many diverging implementations on the Member State level. This issue, together with the lack of a harmonised method of copyright management, has resulted in significant market fragmentation in the Internal Market, so that in practice many licensing contracts are still focused on national markets. The difficulty to get legal certainty on the reuse of content and on clearing rights also contributes to this issue.

Another important issue is the lack of a harmonised set of mandatory exceptions and limitations to the exclusive rights of authors. As a result, Member States can decide if and how to implement the exceptions and limitations. The list of exceptions also exhibits many ambiguities and leaves ample discretionary room to Member States. Consequently, the exceptions and limitations have become a cluttered chaos on the Member States level.

Technological protection measures (TPMs) also entail many legal issues. The Copyright Directive legally protects TPMs – which shifts the focus of the legal protection from the copyrighted work to the technology that protects it – but does not provide specific guidelines on the implementation of TPMs. In addition, the Copyright Directive does not allow circumvention of TPMs that are done for legitimate purposes (such as copying for private use). Further, the use of TPM technologies is liable to conflict with a user’s data protection and privacy rights.

As a result, the current legal instruments in the field of copyright are insufficient. They do not satisfy rights holders (which face a fragmented and pirated market) and do not satisfy users either (who face a list of ambiguities and a limited list of exceptions that does not take into account their daily concerns). A fundamental reform of copyright legislation has therefore become necessary.

5.3. Liability of online intermediaries

The eCommerce Directive has introduced a special liability regime for three types of services: mere conduit operators, "caching" providers and hosting providers. This regime has generally reached its goal of protecting the traditional internet access providers and web hosting companies.

However, over the years, several weaknesses of the liability regime have emerged. In particular, the deliberate legal gaps in its scope (e.g., no detailed notice-and-takedown procedure and no uniform conditions for injunctions) have led to considerable divergences across Member States.

It was found that the current special liability regime is too focused on three specific types of services. While the focus on these services was arguably relevant at the time when the Directive was drafted, many new types of services have developed, which are increasingly exposed to liability issues due to the fact that the scope of the special liability regime is too specific and too dependent on particular technologies. As a result, an entire list of services — in particular the most promising Web 2.0 services, cloud computing services and web services — are not protected. Conversely, in the United States and Japan, these service providers are very well protected against liability issues.

For example, the current protection for "hosting services" is very ambiguous, and has triggered diametrically opposing decisions from courts across the EU. The most important cause of confusion is
the requirement that a hosting service must "consist of" the storage of information, which leads many courts to reject the protection when information is also edited or otherwise processed by the service provider. In practice, only a few services that would deserve special protection consist entirely of storage activities.

Another shortcoming of the current special liability regime is that it provides little guidance on the possibility to issue injunctions. As a result, Member States vary to a significant degree extent by which they allow an injunction to be issued against an online service provider. The uncertainty surrounding the possibility to issue injunctions should not be underestimated, as injunctions can lead to costly lawsuits, public exposure and technical implementation costs for service providers. This has led to the contradictory situation that, although an online intermediary cannot be held liable for infringing material on its servers if it has no actual knowledge of this material or is not aware of acts of circumstances from which the illegal activity or information is apparent, it can nevertheless be forced to take costly measures to prevent the sharing of such material.

The legal gaps of the eCommerce Directive, its dependence on specific services, its various ambiguities and its restricted scope lead to diverging case law across (but sometimes also within) Member States. There is abundant evidence that courts and legal practitioners encounter difficulties to apply the special liability regime, and seem inclined to find arguments to put aside the special liability regime and instead revert to more general rules of legal doctrine. This results in considerable legal uncertainty for online service providers, in particular for new service models.

5.4. E-payment

Electronic payments and electronic money ("e-money") are frequently cited as being an obstacle for consumers to order goods or services online. The previous eMoney Directive was enacted in 2000 to assist e-money in delivering its full potential benefits and to avoid hampering technological innovation. However, the e-money market is far from having reached its full potential. This failure is linked to the fact that the Directive has given rise to many legal problems, such as the unclear definition of electronic money, the unclear scope of the Directive, a disproportionate prudential regime, inconsistent waivers and passporting procedures, and difficulties for e-money institutions to be profitable.

However, the European framework for e-money is currently being revised. The new Payment Services Directive has been adopted in 2007 and will enter into force in most Member States in November 2009. Meanwhile, a new eMoney Directive has been signed on 16 September 2009. Also, the recent Commission Recommendation regarding RFID illustrates that specific rules for contactless mobile payments are being considered.

While the new eMoney Directive solves some ambiguities, several others are still not resolved (e.g., the question to which extent a prepaid mobile phone card is e-money when used), and several new ambiguities are introduced as well (such as the exemption for e-money used in a "limited network" of service providers, and the exemption for value-added services).

Furthermore, the new eMoney Directive does not fundamentally change the waiver regime, which still does not apply on a European level, and does not exempt the e-payment provider from all regulatory compliance issues. These national waivers are still too burdensome in many cases: the exemption must be applied for on a national basis, and generally involves extensive administrative overhead for the e-payment provider.

As a result, the legal treatment of several types of e-payment services – particularly platform payment systems and mobile payment systems – is not clear. Interestingly however, precisely these types of e-payment services seem to be the future of online payments. We are therefore of the opinion that the
improvements brought by the new eMoney Directive will not be sufficient to trigger an uptake of the e-payments market, and that a more fundamental revision of the eMoney Directive is necessary.

5.5. **Electronic contracting**

Although the eCommerce Directive has fulfilled its role of initiating cross-border electronic contracting, several electronic contracting issues have surfaced. While the requirements of article 10 (pre-contractual requirements) and 11 (concerning primarily information duties) were answers to valid concerns at the time the eCommerce Directive was drafted, they have now either become too evident, have become a stumbling block for new technologies and business models, merely lead to increased compliance costs and/or overly protect consumers. Furthermore, they discriminate against the offline contracting process, and they do not deal with other important online contracting issues, such as lengthy terms and conditions. Finally, the current framework on electronic contracting does not go the full way and still excludes several types of contracts, which gives the impression that electronic contracting is only suitable for "less important" contracts.

Less legal issues exist in the field of electronic signatures, where the eSignatures Directive has reached its first objective of EU-wide legal recognition of e-signatures. However, it has not succeeded in getting companies and consumers to actually use electronic signatures on a large scale in a day-to-day context. Major hurdles include a lack of technical interoperability and market acceptance. We therefore welcome the Commission's Action Plan on e-signatures, which aims to offer a comprehensive and pragmatic framework to achieve interoperable e-signatures. An unresolved issue remains the long-term validation of e-signatures, which also requires to be addressed on a mainly technical level.

Electronic invoicing also suffers from insufficient market adoption. Contrary to the eSignatures Directive, however, the current legal framework is at least partially responsible. The current eInvoice Directive is plagued by a lack of harmonisation, legal clarity (e.g., whether legal entities can sign invoices), diverging Member State implementations (e.g., whether qualified or advanced electronic signatures are required) and unnecessary discrimination against electronic invoices. However, the proposal for a new eInvoice Directive seems to resolve these issues.

Finally, it should be noted that the EU legal framework does not provide any specific regulation on digital evidence. Across the European Union, legislation and case law by Member States in this area varies. Each Member State basically regulates e-evidence by analogical interpretation of existing rules of traditional evidence. A harmonised legal framework on digital evidence thus constitutes the "missing link" in the spectrum of legal instruments relating to e-contracts. All other steps found in a typical contractual process are already covered by other Directives (from the ordering process to the signature of the order and the invoicing process).

5.6. **Net neutrality**

The emergence of a connected society and the trend towards ubiquitous computing have made it clear that it is important for everyone to participate in the information society, on a non-discriminatory basis. In this context, the "net neutrality" debate has emerged, which boils down to the question of whether network operators must take a neutral position towards the data that passes through their networks. The discussion highlights a possible tension between network operators and Internet content providers.

Although the net neutrality debate used to be limited to the United States, several net neutrality interferences have also surfaced in Europe, and the number of (known) interferences seems to be rising. Furthermore, it can be assumed that many interferences exist, but have not yet publicly surfaced.
An analysis of the current EU legal regime reveals the fragmented nature of the current rules, and the fact that there exist few specific rules to effectively deal with neutrality interferences. Although more general rules of competition law, as well as the telecom SMP rules, can be used to deal with some situations where dominant access providers engage in neutrality interferences, the current rules seem to fall short when applied to non-dominant access providers. Similarly, data protection legislation could be used against net neutrality interferences, but only in specific circumstances, and depending on the technology used by the access provider. Furthermore, national regulatory authorities may not have the power and procedural tools tailored to detecting or dealing with potentially unwanted behaviour. In other words, when neutrality interferences will intensify, then it may be difficult in the short term for national regulators to effectively deal with (all of) them.

A similar conclusion applies to government regulation of content on the Internet. Although the actual number of issues has been limited so far, the rising importance of content filtering might create obstacles for the internal market. While content filtering was generally limited to obviously damaging information (terrorism and extreme pornography), an increasing number of Member States are now extending their blocking effort to other content, such as gambling websites and violent video games.

5.7. Spam

Depending on the source, it is estimated that 70% to 95% of global e-mail traffic consists of unsolicited electronic communications ("spam"). Spam is a horizontal issue, touching upon different aspects of telecommunication services, consumer protection, security, and privacy, at national and cross-border levels. Due to legal and technical difficulties, there is no simple solution or "silver bullet" to stop spam.

Although several EU-level instruments deal with spam, they have been largely ineffective. The are some legal problems with the current European approach with regard to spam, such as the fragmented legal framework (with spam provisions spread across four EU Directives), the absence of a clear definition of the notion of spam, uncertainty about the meaning of certain basic concepts in the regulation (such as the terms "subscriber", "sale" and "consent"), confusion with regard to the applicable law and the competent court, gaps in the legislation with regard to new technologies and new forms of spam (e.g. spam via instant messaging, spam via Bluetooth-enabled electronic devices and spam on message forums), as well as implementation differences in the Member States. In addition, the legal framework makes things overly complex. Examples of this complexity can be found in the fact that the scope of the E-privacy Directive is limited to natural persons, or in the limitation of the "soft opt-in" exception to unsolicited communications through e-mail.

Even so, the current legal framework sufficiently addresses the most prominent form of spam. Therefore, although various improvements can be made to the European anti-spam legislation, the most important problem seems to be the lack of sufficient enforcement mechanisms in some of the Member States.

5.8. Cybercrime

The existing European and international legal instruments suffice to deal with most forms of cybercrime. Only with regard to identity theft and DoS attacks, additional legislation should be considered.

Compared to the European anti-spam legislation, the legislation with regard to cybercrime is already relatively harmonised at the international level. The problems that do exist with regard to the current legislation are situated at the Member State level, rather than the European level. The lack of harmonisation on the Member State level is an impediment for effective action against cybercrime. Twelve Member States have not yet ratified the Cybercrime Convention, causing gaps in the legislation of the Member States.
The Framework Decision on Attacks against Information Systems suffers from a similar lack of harmonisation. The lack of harmonisation impacts the cooperation between national law enforcement authorities, which benefits from a harmonisation of crime definitions. Consequently, steps should be taken to encourage Member States to ratify the Cybercrime Convention in a consistent way in order to ensure further harmonisation of the legal framework with regard to cybercrime.

Besides these harmonisation issues, the European legislation with regard to cybercrime is sufficiently advanced and future-proof, and ready to deal with most situations. However, although the legal "groundwork" is present, effective enforcement seems to be lacking. The Commission has recognised that efficient structures for cross-border cooperation are lacking, being underutilised or not yet sufficiently developed, and that traditional mutual assistance mechanisms are too slow to deal with urgent cyber crime cases. Consequently, the European framework for judicial cooperation should be expanded. In addition, cooperation with the private sector should be increased, as such form of cooperation can be a valuable contribution to the fight against cybercrime.

5.9. Dispute resolution

While traditional state courts have long established their role in the resolution of offline conflicts, there is substantial evidence that they are not able to meet the requirements of the online environment. Parties that want to resolve their dispute through traditional state court proceedings, will encounter difficulties in determining the applicable law and the competent court, and may also face important issues during the actual cross-border enforcement of the judicial decision. The current legal instruments for dealing with jurisdiction (Brussels I) and applicable law (Rome I - II) are often difficult to apply to Web 2.0 online situations, as they mainly rely on the localisation of objective elements to determine the applicable law or the competence of a national state. Moreover, state court proceedings are often slow, costly and formal.

Alternative dispute resolution (ADR) is widely regarded as an alternative to state court proceedings, and has seen important growth in all economic areas. It has been recommended and accelerated by the European Commission, national authorities as well as international institutions. Furthermore, the growth of the Internet has brought important new possibilities to ADR. This has resulted in ODR, the synergy between ADR and information technology, which holds great promise as a method of resolving online disputes, due to increased time and cost savings. Numerous ODR service providers are available today, offering a variety of different methods to resolve disputes online, from automated negotiation to assisted negotiation, "blind bidding" and online arbitration.

Although ODR has proved to be successful in specific areas (such as the UDRP and .EU domain name procedures and auction settlements), it has seen fairly limited popularity outside these areas. The most important drawback is that ODR requires the parties to consent to the procedure, which is particularly problematic in a B2C context, where the web shop or online service provider does not generally have sufficient incentives to consent to the ODR procedure. Other issues include the recognition of ODR decisions and concerns about due process.

The European Commission has recognised these concerns, and has adopted a European "order for payment" procedure for uncontested pecuniary cross-border claims. It also adopted the European small claims procedure for cross-border disputes. While some aspects of the new small claims procedure (value limited to 2,000 EUR; data protection disputes are not covered; lack of adequate provisions supporting ADR and ODR) may hamper the adoption of this procedure, it holds great promise to resolve typical cross-border disputes of limited value, for which traditional court proceedings or ADR may be too costly or troublesome for parties to undertake. However, as both procedures only entered into force very recently, it is too early to tell whether they will be adequate for online disputes.
5.10. **Self-regulation**

The digital and cross-border nature of the Internet challenges many of the assumptions underlying traditional regulation, in particular the jurisdictional reach of a country and the possibility to enforce measures. The balance for a legislator between leaving enough flexibility for innovative services to develop and addressing problems firmly is difficult to find. In this context, self-regulation can be seen as an alternative to classic lawmaking.

Self-regulation is not a new answer to these challenges — in fact, it has been part of the Internet since its early conception, although it has not been the sole form of regulation on the Internet. There are several examples where self-regulation has flourished in specific areas, but even more examples where self-regulation has proved to be largely unsuccessful. Hence, self-regulation is still in the learning curve, and there is obvious room for improvement of each characteristic.

Self-regulation on the Internet is mainly a bottom-up procedure, where private parties take the initiative to address specific needs. However, states also participate in the creation of self-regulatory rules, either by creating the general background legal framework, by providing financial sponsoring, practical or legal guidance, or other assistance. Self-regulation and state legislation do not merely co-exist: they often complement each other and are intertwined, whereby self-regulation can "plug into" the more general rules set forth by state law.

Self-regulation has been recognised as a recommended approach by the European Commission and the Member States. Moreover, it is already recommended by various legal instruments that apply to the online environment, including the eCommerce Directive, the Copyright Directive and the Data Protection Directive.

From a legal point of view, the basic framework is already available for most areas where self-regulation can be beneficial. Although the legal framework is available, the actual implementation is often still problematic, particularly in the area of participation, enforcement and proper governance of self-regulatory organisations.

6. **General recommendations**

6.1. **Introduction: respecting core values**

The trends and challenges described above call for a review of the "acquis communautaire" for the information society, in order to prepare it for a true Single European Information Space, aimed at an open and competitive digital economy. This section 6 gives a high-level overview of general recommendations in a horizontal manner, across all topics covered by this study, in order to tackle the issues identified above. Specific recommendations per topic can be found in Chapters 4 to 13, and are also summarised in Chapter 2.

The review of the legal framework cannot, however, take place in a legal vacuum. Any recommendation on how to improve the legal rules, should respect a list of persisting values that are considered fundamental for the European information society (now and in the future), balancing the rights and interests of consumers, companies and online service providers. Such a list of core values for the information society is outlined below, and will be used as a benchmark for our recommendations below. Furthermore, we are convinced that Europe should be proud of these values, and should try to "export" them whenever it deals with third countries, for example during negotiations for treaties for the online environment (which we recommend for several domains, as explained below).
Inspiration for drawing up this list, was found in documents such as the European Convention on Human Rights, the Charter of Fundamental Rights of the European Union, the 2005 Tunis Commitment,89 preambles to existing legal instruments at the European level and several private sector initiatives90.

**Predictability** – Predictability is often cited as one of the values resulting from the rule of law91. Due to the fast pace of change in today's networked society, the change of legal rules is unavoidable. However, for these adapted legal rules to be effective, it is required that they are generally intelligible, clear and predictable to all actors involved92. This is not always the case in the current acquis communautaire93 and its implementation by the Member States94: the same rules sometimes lead to surprisingly different results.

Predictability is more than just a matter of fairness. It makes it easy for companies and individuals to conform their conduct to be law-abiding95. It also makes settlement easier, as litigation is unlikely to change the outcome of a dispute96. Moreover, it decreases the total cost of the legal system, because predictability lessens lower court reversals in appellate courts.

**Trust** – When there is no sufficient confidence in a legal framework, consumers and companies will refrain from entering into transactions, due to risks embedded in the legal system itself or because the system is inefficient in resolving potential disputes97.

For the law to inspire trust, it is not only necessary to make sure that respect for some of the other key values, such as predictability and enforceability is ensured. It is just as much a matter of informing consumers and companies of their rights and obligations, and making sure that possible problems are anticipated by the law.

**Reliability** – Connected with trust is reliability: the ability to rely on the legal framework when it is needed. Reliability differs from trust in that trust is seen as a concept that is associated with pre-transaction reliance, while reliability is more connected to post-transaction confidence. Reliability refers to the effect of the application of legislation, which should be computable and predictable, and these computations should be reliable98.

**Enforceability** – Enforceability of the law, whether by seeking redress in court or through alternative dispute resolution, is a prerequisite for trust in any legal system. Several types of unenforceability can be identified that are especially relevant in the Internet environment. Due to the cross-border nature of the

---

89 The full text of the Tunis Commitment can be found at www.itu.int/wise/docs2/tunis/off7.html.
90 See for example the http://Global Network Initiative, which aims to protect privacy and freedom of speech in the ICT sector.
91 See for example F. HAYEK, The Road to Serfdom, University Of Chicago, 1994.
93 For example, the definition of "hosting" services in article 14 of the eCommerce Directive is highly ambiguous, giving rise to legal uncertainty.
94 For example, French courts found eBay liable for counterfeit (judgement of 4 June 2008) and infringing the selective distribution agreements of third parties (judgement of 30 June 2008). Conversely, a Belgian court did not find eBay liable for counterfeit, in a highly similar case (judgement of 14 August 2008).
Internet, laws will often be unenforceable in practice because the court in question has no effective jurisdiction over the defendant\(^99\), or because the cost of enforcement outweighs the benefits of enforcement.

**Transparency** – Transparency implies a party's openness, communication, and accountability. This value is particularly relevant in the context of e-commerce and privacy protection\(^100\): due to the vast amounts of data being stored and processed in the information society, transparency on how this data is handled, is an essential value.

**Protection of privacy** – The protection of privacy is a fundamental value enshrined in the European Convention on Human Rights, the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and various conventions, treaties and national constitutions. Protection of privacy is, simultaneously, a core value and main challenge, as the relative anonymity offered by the Internet in the "old days" is effectively gone\(^101\).

**Freedom of expression** – Freedom of expression is one of the cornerstones of our democratic society. The Internet has created unprecedented possibilities for people to interact and express their opinions. At the same time however, it also creates opportunities for limiting and controlling this interaction and expression\(^102\).

The protection of this right is already provided for by article 11 of the Charter of Fundamental Rights of the European Union and various international treaties. However, freedom of expression is not to be interpreted as absolute\(^103\), as this value is prone to conflicts with other values such as the protection of privacy and ethics. Defamation and hate speech form an even bigger challenge in an online environment, as the identity of the source can be very difficult to trace\(^104\), and the distributed nature of the Internet makes flows of information difficult to control.

**Freedom of information** – The freedom of information is closely linked to the freedom of expression, and is equally protected by article 11 of the Charter of Fundamental Rights of the European Union. It guarantees the fulfilment of the freedoms of thought, conscience and religion and of expression, and covers the freedom of the press and the freedom of communication in general, regardless of frontiers. Historically, this right has protected the function of journalists as a public watchdog and as part of the system of checks and balances, necessary in a democratic society.

**Cultural and linguistic diversity** – Europe is characterised by cultural and linguistic diversity across its Member States. Many EU-level legal instruments recognise the importance of this diversity and explicitly specify that their content is without prejudice to measures taken in this regard by the Community or individual Member States.

**Property rights** – Property rights ensure that individuals and companies reap the benefits from productive activity. The European Court of Justice has confirmed that intellectual property falls within the

---


\(^103\) See for example article 10§2 ECHR, which states that "the exercise of these freedoms, […] may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society […]".

scope of protected possession\textsuperscript{105}. In a digital context, a balanced and reasonable approach towards respecting intellectual property rights has proven to be a difficult exercise.

**Network accessibility** – The centrality of the Internet in many areas of social, economic, and political activity is tantamount to marginality for those without, or with only limited, access to the Internet, as well as for those unable to use it effectively\textsuperscript{106}. Although more than 50% of the EU population regularly uses the Internet\textsuperscript{107}, significant differences exist between the different European countries and various socio-economic classes\textsuperscript{108}. Therefore, the legal framework for the information society has to support the effort of bringing the benefits of the information society into all segments of the population, including to people who are disadvantaged due to education, age, gender, disabilities, ethnicity or geographical location.

**Efficient use of infrastructure** – The efficient use of infrastructure represents the belief that a legal framework must take the advantages and the limitations of the infrastructure into account, as to make sure that the rules do not impose overly burdensome legal obligations on the actors. Efficient use is also related to the values of non-discrimination and accessibility, as for the use of infrastructure to be efficient, all individuals and groups have to be able to access it. Moreover, there is a strong link with the value of competition\textsuperscript{109}. The regulatory process of local loop unbundling is an example of this link, as it has enabled competition on the same infrastructure, stimulating efficient use.

6.2. **Adopt hybrid rules in the short term, but converged rules in the mid-term**

**Mid-term and long term** – Taking into account the reality of convergence, we are convinced that it is no longer appropriate to keep the duality and maintain separate laws for online and offline environments. This duality undermines the core value of the predictability of the legal rules, and also undermines the trust in these rules.

\textit{For example, the specific electronic contracting regime introduced by the eCommerce Directive excludes several types of contracts (such as family law and real estate contracts). These exceptions suggest that the legal rules for electronic contracting are not yet adequate for important contracts.}

In the medium and long term, the EU must therefore strive to adopt converged laws that simultaneously target both the online and the offline environment, and apply the same principles to both environments. It could even be envisaged to introduce a mandatory "convergence" test during the lawmaking process. The legislator should thereby adhere to the guiding principle that the online and the offline environment can only be treated differently when this results from the nature and specific characteristics of each environment. Such different treatments should, however, be limited to the fullest extent possible, and should also be constrained to implementation differences, because the principles should be equal for both environments.

\textit{For example, both the online and the offline environment should apply an opt-in regime for unsolicited messages, and should allow recipients to opt-out at any time, free of cost (= same principles). However, the specific method to opt-in may differ between the online and the offline environment. In the online environment, for example, a recipient can give his consent to receive commercial messages by...}

\textsuperscript{105} ECHR, Anheuser-Busch v. Portugal, 2005 and 2007.


\textsuperscript{107} See COM(2008) 199 final, Preparing Europe’s digital future i2010 - Mid-term review, page 10

\textsuperscript{108} For example, in 2007, 82% of interviewed individuals in the Netherlands accessed the Internet from home in the last three months, while this percentage in Romania is 16%. See Information society statistics at \url{http://ec.europa.eu/eurostat}

\textsuperscript{109} V. REDING, SPEECH/06/697, “From Service Competition to Infrastructure Competition: the Policy Options Now on the Table”.

---

Legal analysis of a Single Market for an Information Society – General overview
In other words, legislators must perform a mind switch: instead of upholding a starting position that the online environment must be dealt with separately, they must adhere to the starting point that the online and the offline environment should be treated equally, so that a different treatment becomes the exception instead of the rule. We therefore welcome the various efforts of the European Commission in this direction, such as the current proposal to completely equalise electronic and paper invoices, by abolishing all additional security-related requirements for electronic invoices.

**Short term** – While we are convinced that a unified legal system is the recommended solution in the medium and long term, we think that in the short term this unified system will not be appropriate in many areas, because society at large and many legal actors have not yet fully absorbed the online environment, its particularities and its consequences. Many established offline institutions and legal instruments are simply not yet adapted to the online environment, so that transitory hybrid legal rules may still be required.

Such is, for example, the case in the area of online liability, where we think that the special liability protection regime should be maintained and further expanded to include any type of service provider that handles a sufficient amount of third party data. The current case law regarding the special liability regime for online intermediaries has revealed that, even though the core of the online liability regime is clear, in many cases judges seem to have problems applying this regime in practice. While we believe that judges will in the long term "internalise" the special characteristics of the role of online intermediaries, we think it would hurt the further uptake of e-commerce when the special liability regime would be abolished in the short term.

A second reason for recommending hybrid legal rules in the short term, is that the online environment, while no longer in its infancy, has not yet sufficiently matured in our opinion (see, for example, the challenge of "online naivety" described in section 4.3 above). Exposing online actors and online technologies to the very same principles as the offline environment may then disturb the further development of the online environment. Therefore, a hybrid treatment seems justified in the short term.

Hence, we deem the principles upheld by the EU legislator in 2000 when drafting the eCommerce Directive\(^\text{110}\), to still be relevant in the short term.

For example, we recommend to clarify and expand the "coordinated field" of the eCommerce Directive, to avoid that online service providers would become subject to technical requirements in local laws which would unduly restrict freedom to provide services when doing business abroad. Although one could argue that this puts online service providers at an advantage (compared to their offline counterparts, who would be subject to foreign rules when doing business abroad), we are of the opinion that this position is justified — at least in the short term.

We would even recommend to create separate EU-level online courts that are dedicated to the efficient resolution of civil law that arise in the online world, in order to foster trust in the online environment. In the medium term, however, the proposed EU-level online courts can disappear, assuming that the traditional courts have sufficiently modernised through the use of information technology.

### 6.3. Remove unnecessary obstacles

We are not convinced that the many formalities and legal hurdles imposed on online services foster trust or offer better consumer protection. These formalities and legal hurdles were either adopted for the offline environment, or were adopted for the online environment but suffer from the legislator's "cold feet"
with legislating in the online environment. The time has come to abolish them and opt for more flexible legislation with no unnecessary compliance overhead.

For example:

- Article 10.1 of the eCommerce Directive impose several pre-contractual information duties. These formalities provide little consumer protection, are technology dependent (too focused on traditional websites), and mainly lead to unnecessary compliance costs.
- Article 11 of the eCommerce Directive requires a service provider to confirm an online order. No such (EU-level) obligation exists for offline contracts.
- Article 15 of the eCommerce Directive allows Member States to require an online service provider to promptly inform competent public authorities of alleged illegal activities undertaken by their users. Depending on the type of service considered and the interpretation of "illegal", this obligation may become very burdensome for some online service providers.
- The eInvoicing Directive subjects electronic invoices to a variety of specific rules that intend to secure the electronic invoice. No such security rules apply to traditional paper invoices.
- The eSignatures Directive imposes more than thirty different requirements on qualified electronic signatures. In comparison, very few requirements apply to traditional handwritten signatures.
- Many Member States require a "data controller" to submit a data protection notification to its national data protection authority. These submissions contribute very little to the transparency towards data subjects, while they do cause a clear administrative burden for data controllers (and the national authorities).
- Many website operators consider the creation of a privacy policy and a set of legal terms & conditions as a necessary but pointless legal compliance exercise. Out of fear for legal repercussions, these legal documents have also become long and difficult to read. We therefore recommend to introduce concise and optimised templates, to counter this trend.

### 6.4. Ensure technological neutrality

As a fundamental guideline, all laws – whether containing converged or hybrid legal rules – must be technologically neutral, because the experience with the eCommerce Directive, the eInvoicing Directive, the eSignatures Directive and the Copyright Directive has taught that the online environment evolves too quickly for legislators to catch up. Legal rules that are drafted with any particular technology in mind, will become a legal hurdle for new technology. Similar to our proposal to introduce a mandatory “convergence test” during the lawmaking process, it could be envisaged to also introduce a mandatory "neutrality test" to ensure that new legal rules are sufficiently neutral from a technological neutrality.

It should be borne in mind, however, that real technological neutrality is more difficult to achieve than may appear at first sight. For example, the eCommerce Directive claims to be neutral, and does not explicitly refer to specific technologies. In fact, in several of its provisions, the eCommerce Directive makes reference to "electronic means" without specifying the device to be used by the service recipient. A deeper inspection reveals, however, that this Directive is clearly written with traditional websites in mind, accessed from a regular desktop or laptop pc.

> For example, references to "Internet", "websites" and "online activities" are found in the recitals of the Directive. These concepts only relate to services provided via the Internet.

---

111 A few examples of the use of the expression "electronic means": Paragraphs (18), (34), (35), (37), (52). Articles 2, 9 and 11
In addition, article 5 requires online service providers to display an extensive list of information, in order to improve transparency.\(^{112}\) It is not difficult to make this information available on a traditional website, accessed from a typical pc. For a Directive dealing exclusively with the provision of online services via the Internet (WWW), the solution would be the correct one.

However, the eCommerce Directive is also applicable to other information society services such as a ring tone provider, or location-based services via SMS platforms. For the purchase of an SMS service, in many occasions, the service recipient becomes aware of the service via a TV ad, types a text message and places the order with the service provider. The decision process takes a matter of seconds and it is not necessary to access any website with information on that service provider. Therefore, complying with the criteria of having information on the service provider "easily, directly and permanently" available during the provision of the service is difficult, if not impossible to achieve.

Furthermore, article 10.3 of the eCommerce Directive requires contract terms and conditions be made available to the recipient in such a way that allows him to store and reproduce them. This requirement, along with the other steps and legal structure, was clearly conceived as if recipients of information society services were in front of a computer screen which would allow for storage of the terms and conditions. Due to the limitations of a mobile device (SMS messages are only allowed 160 characters, reduced memory capacity, etc), storing terms and conditions is readily feasible. However, information service providers may inform the recipients, through the SMS message, for example, of the location where these terms and conditions are accessible (i.e. relevant link may be provided).

6.5. Create citizen awareness

In order to increase consumer trust and resolve the "online naivety" of some citizens, the European Commission and the Member States must start awareness campaigns. These campaigns could deal with topics such as:

- the importance of privacy on the Internet
- how online service providers make use of personal data
- the long-term threats of sharing personal data online
- the (limited) availability of online dispute resolution procedures
- the importance of making sure that hardware and software are sufficiently secure
- the advantages of electronic signatures
- dealing with copyright
- where to go for additional information; etc.

This aware creation is crucial to ensure that, over time, online habits are established, which can be used to guide citizens and judges in developing a "bonus pater familias" standard for online behaviour. Such standard is important to assess to which extent users should be held responsible for their online behaviour, and to balance this user responsibility with the responsibility of online intermediaries.

We therefore welcome the initiatives the Commission has already taken in this regard, such as the recent eYouGuide\(^ {113}\), which provides an accessible overview of online rights for consumers.

\(^{112}\) This list comprises the name of the service provider; the geographic address at which the provider is established; details of the service provider, including electronic mail address; information on where the service provider is registered in a trade or similar public register; the particulars of the relevant supervisory authority; the VAT identification number; reference to a professional body to which the service provider is subject; a reference to the applicable professional rules and the means to access them.

6.6. **Boost self-regulation and standardisation**

As explained in Chapter 13, self-regulatory initiatives can be very useful policy tools. Self-regulation has been part of the Internet since its early conception, and is also promoted by many EU legal instruments. We think this support for self-regulation is strongly recommendable, and should in fact be further strengthened wherever possible.

Similarly, the Commission should further encourage the adoption of standards in relevant areas. Although standards are already used in the context of some Directives (particularly the eSignatures Directive), their use should be further extended.

Areas that are suitable for self regulation and adoption of standards include:

- **Data protection**: self-regulation of the content, style and presentation of privacy policies; sector-specific standards and best practices for security; standards on dealing with minors;
- **E-commerce**: the adoption of EU-level trustmarks in order to increase customer trust;
- **Advertising**: self-regulation of direct marketing and unsolicited commercial communications; behavioural advertising;
- **Dispute resolution**: adoption of minimum quality criteria for ADR/ODR service providers; and
- **Copyright**: interoperability standards for DRM; self-regulation on how service providers can cooperate with rights holders to deal with piracy and unlawful content.

6.7. **Clarify and enlarge the scope of the eCommerce Directive**

Due to the central role of the eCommerce Directive for the further uptake of e-commerce, we recommend to enlarge the scope of the eCommerce Directive. While doing so, we also recommend to clarify the current issues related to the scope of this Directive.

**Coordinated field** – The exact scope of the coordinated field is highly ambiguous: some authors suggest that it encompasses only what is explicitly regulated by the eCommerce Directive itself. Others – particularly those who have written about this matter immediately after the date of enactment of the eCommerce Directive – see it more broadly, and consider that any law that somehow impacts online service providers is included in the coordinated field (the only exceptions being those that are explicitly set forth by the eCommerce Directive, such as the offline delivery of goods).

For example, in a recent court case, a Belgian dating website sued a German dating website for breaching the Belgian Act on marriage bureaus. This Act does not distinguish between online and offline marriage bureaus. According to one of the Royal Decrees adopted pursuant to the Act, marriage bureaus must use a predefined contract (for which the content is defined by the Royal Decree) for their contracts. According to the Belgian dating website, the German website must also use this predefined contract, as it targets the Belgian market.

The German website contested this claim, however, arguing that the Belgian Act on marriage bureaus and the accompanying Royal Decree fall within the scope of the coordinated field of the eCommerce Directive, so that the German website is only subject to German legislation. Furthermore, the German website claimed that if the Belgian authorities would like to enforce the Belgian marriage bureaus Act to foreign service providers, they should have notified the Act to the European Commission, pursuant to article 3 of the eCommerce Directive.

This issue should obviously be clarified. In our opinion, as also stated above, the scope of the coordinated field must be as large as possible, in order to reduce the compliance burden of online

---

114 A. BULLESBACH, Y. POULLET en C. PRINS (ed.), Concise European IT Law, 2006, p. 227
service providers. Hence, it must be clarified that the coordinated field covers any rule of law that can somehow affect an online service provider, with the single exception of a rule that indiscriminately applies to both the online and the offline environment.

**Information society services** – The central definition of "information society services" is a subcategory of the general concept of "services", as defined to article 50 of the EC Treaty. However, the scope of article 50 of the EC Treaty may be too narrow for the purposes of the eCommerce Directive. For example, it not only excludes many governmental services offered online, but also risks to exclude many new types of services (particularly "freemium" services), which may then be exposed to unnecessary third party content liability issues, and would then not benefit from the freedom of establishment and the freedom of online service delivery.

When this ambiguity would not be resolved by case law, we recommend to consider adopting a different criterion. In the short or medium term, this different criterion could be used to define the scope of the special liability regime. However, in order to also use this different criterion for the freedom of establishment and the freedom of service delivery, a change of the EC Treaty will be necessary. Such will, obviously, only be possible in the long term.

**Exclusions of electronic contracts** – Article 9.2 contains a list of contracts for which Member States do not need to ensure contract conclusion by electronic means. This list of exceptions must be revised, and preferably abolished, when Member States become increasingly digitalised and trust in the use of technology grows.

**Exclusion of online gambling** – The general delimitation of the E-Commerce Directive in article 3.5 excludes gambling activities which involve wagering a stake with monetary value in games of chance, including lotteries and betting transactions. Nevertheless, online gambling is an area in which action may be required, since it was included in the scope of some Member States national e-commerce laws and has caused significant Internal Market problems.

While some past decisions of the ECJ suggested that the ECJ would eventually prohibit restrictive national gambling rules, the situation seems to be reversed in the current state of the ECJ's case law. In the Gambelli case, the ECJ decided that national legislation prohibiting gambling activities without a licence from the Member State concerned constitutes a restriction on the freedom to provide services. It is up to the national courts to determine whether such a restriction actually serves the aims which might justify it. In addition, the ECJ decided that Member State which encourage consumers to participate in gambling activities cannot invoke public order concerns in order to justify such restrictive measures.

---

115 It could, for example, be envisaged to abolish the requirement that activities must constitute economic activities, as it is difficult to justify why economic activities merit a better protection level than non-economic activities.

116 because the scope of the special liability regime is not necessarily restricted by the scope of article 50 of the EC Treaty (which deals with the essential freedoms)

117 Service providers established in one Member State offering online sports betting are required by other Member States – Denmark, Germany, Italy, and the Netherlands – to block access by their citizens to those online services.

118 “E-commerce: EU law boosting emerging sector”, IP/03/1580, Brussels, 21 November 2003

119 ECJ, Case C-243/01, Piergiorgio Gambelli et al., 6 November 2003, 54

120 Confirmed in ECJ, Case C-338/04, Placanica et al., 6 March 2007. See nr. 72

121 ECJ, Case C-243/01, Piergiorgio Gambelli et al., 6 November 2003
However, in the more recent Santa Casa case, the ECJ decided that imposing restrictions with respect to which operators can offer their services in a Member State can be justified in order to fight crime. This argument will likely be used by Member States that are looking to create national gambling monopolies, which raises questions with regard to the future of existing online gambling websites.

Instead of outright prohibiting these services, it seems more appropriate to include online gambling in the scope of the coordinated field of the eCommerce Directive and to create a harmonised regulatory framework for the online gaming market. Such a framework would allow to protect consumers against fraud and other criminal activities, while avoiding disruptions of the Internal Market.

6.8. **Enter into international treaties**

Considering that "the world is flat" and that the Internet is – by its very nature – a cross-border reality, it is an illusion to believe that the European Union can enforce its legislation around the globe. Instead, for some of the most important issues, we recommend to conclude international treaties, to provide appropriate legal answers to the new reality, and to ensure that at least the core of the European values can be preserved on the Internet.

Obviously, in order to enter into such international treaties, the EU may be required to water-down some of its policy options and values. However, Europe should be proud of its core values and should promote them during any discussions. Furthermore, watered down protection outside the EU will almost always be a better policy option than having no protection at all.

Such international treaties would particularly be appropriate in the field of **data protection**. Cross-border data flows are a reality to which the EU legal framework must take a realistic position, instead of a naive assumption that data flows can be contained within the borders of the EU. Even on an international level, there seems to be a consensus as regards the need for global standards with respect to the protection of personal data. There also seems to be a certain level of consensus, as regards the *basic principles* for data protection, as included in the OECD Guidelines and Convention 108. An international treaty would provide the opportunity to try to "export" the most important European data protection values, and to introduce new rights, such as the right to data portability and the "right to be forgotten".

International treaties are equally valuable in the field of **copyright**, where many treaties exist already. In fact, in order to implement some of copyright recommendations, it may be necessary to change the existing treaties.

The Commission should also investigate an **anti-spam** treaty aimed at harmonising certain aspects of the legal framework with regard to spam, such as applicable law, competent court, exceptions and covered technologies and cooperation in the persecution and conviction of spammers.

6.9. **Make access providers responsible for the provision of "clean Internet"**

In the medium to long term, it could be considered to make Internet access providers and telecom operators responsible for providing "clean internet". With the current trend towards cloud computing, the Internet is starting to evolve towards a model in which IT services (including internet access and e-mail) are becoming more and more utility-based (similar to tap water, electricity or gas supplies), thus increasing the importance of "clean" internet access.

---

122 ECJ, Case C-42/07, *Bwin vs. Santa Casa*, 8 September 2009
123 See section 8.4.1 of Chapter 4 (privacy and data protection)
124 See N. CARR, *The Big Switch: Rewiring the World, from Edison to Google*, 2008
Similar to the obligation of water suppliers to provide germ-free water and the obligation of electricity suppliers to provide a stable electricity current, access providers would be made responsible for providing a spam-free, malware-free and secured network connection to the Internet. This would be more efficient than each user / company installing its software and hardware to deal with spam and security issues. A handful of economists and security experts have indeed already suggested that Internet access providers are indeed in a good position to cost-effectively deal with these issues.

Although it may seem far-reaching to shift the responsibility for spam and security to the "gatekeepers" of the Internet, European legislation already contains rules in this direction. Article 4.1 of the ePrivacy Directive requires the provider of a publicly available electronic communication service to take appropriate technical and organisational measures to safeguard security of its services, if necessary in conjunction with the provider of the public communications network with respect to network security. Although this article does not explicitly mention it, Working Parting 29 is of the opinion that this article also applies to spam.

To mitigate the concern of Internet access providers that the scope of their responsibilities is increasing and that it is not technically possible to offer absolutely clean Internet, it could be envisaged to extend the current special liability regime (as set forth in the eCommerce Directive), so that Internet access providers would be protected against claims from their customers when they have offered a sufficiently clean level of Internet access.

Finally, we want to stress that the increased responsibility of Internet access providers must be strictly limited to security-related issues (spam, malware, security attacks, etc.). Internet access providers must not be required to "police" the Internet, to filter the Internet from content that is possibly illegal or harmful (particularly copyrighted files, defamatory statements and politically undesirable material). In this regard, we think that the analogy with water and electricity providers can again provide guidance: while such providers are responsible for germ-free water and stable electricity, they are not responsible for the possibly illegal uses of their water and electricity by customers (e.g., a customer who would electrocute his neighbour).

6.10. Start a fundamental discussion on data protection and copyright

From a societal point of view, current copyright and data protection legal frameworks share many similarities.

Both legal frameworks were conceived before there was any widespread use of the Internet and digital technologies in general. As a result, for both legal frameworks, there are many situations in which it is difficult, odd or even downright ill-suited to apply their rules to the online environment.

Copyright legislation was conceived in the analogue era, when copies were an exception and were generally of lesser quality. In a digital environment, however, copying has become the rule: any use of a work – even mere consultation – leads to many copies of the work. Due to the low barrier towards

---

125 This would be highly similar to the historical evolution of electricity provision, as described by N. CARR in The Big Switch (see footnote 124). While each company used to have its own electricity generator and did not trust central electricity provision (considering the pivotal importance of reliable electricity), the industry eventually realised that central electricity provision would be much more cost-efficient. Electricity thus became a public utility.

126 See, for example, Y. HUANG, G. XIANJUN and A. WHINSTON, "Defeating DDoS attacks by fixing the incentive chain", 2007, ACM Transactions on Internet Technology, 7(1), article 5, 1-5; B. SCHNEIER, "Do we really need a security industry?", Schneier on Security blog, 3 May 2007, www.schneier.com/blog/archives/2007/05/do_we_really_ne.html

copying and the fact that a copy is identical to the original work, copying third party material is widespread among internet users. Many internet users do not find any harm in these copying activities.

The Data Protection Directive was conceived in the mainframe era, when limited amounts of data were centrally stored by a small number of parties. Conversely, today’s internet features numerous parties collecting personal data in a decentralised way, with reuse of personal data – often for purposes of direct marketing – being the rule instead of the exception. Consequently, many of the objectives of the Directive are difficult to achieve on the Internet.

Also, for both the copyright and data protection legal framework, there is mounting evidence that many citizens have a personal conviction and behaviour that is, in various aspects, far away from the rules suggested by the law. This is particularly true for minors (“digital natives”), who grew up with digital technologies and have an entirely different perception than adults (“digital immigrants”). This directly threatens the core value of artists’ and producers’ property rights.

For example, a survey by the Pew Internet & American Life Project (www.pewinternet.com) concluded that 78% of people who download music are aware that they are violating the copyright legislation. They do not think that illegally downloading music files equals “stealing”. Of young people ages thirteen to seventeen, 83% believe that sharing digital music is morally acceptable.

Furthermore, for both data protection and copyright, online business models and concepts are emerging that, although framed within the current legal frameworks, significantly stretch – and often severely undermine – the core principles and values of these frameworks. While these business models hold great promise, they run foul of the core objectives of the current legal frameworks.

For example, open source and “creative commons” software licenses are primarily focused on giving users as many rights as possible, instead of restricting each user’s rights. Also in the field of copyright, many “upload” websites (such as scribd.com and rapidshare.com) encourage users to share their works. As a consequence, users also upload materials for which they do not have appropriate permissions.

In the field of data protection, users of social networks are inclined to publicly expose many personal details. Social networks subsequently use personal data for various other purposes, such as behavioural advertising. In several cases, such further processing falls foul of the core data protection principles.

The clash of values and opinions is also visible at the inter-Member State level. Some Member States (such as France) have reacted to these issues by adopting strict legislation to protect copyright. In other Member States (such as the Netherlands), there is a permissive attitude towards illegal downloading. Many other Member States have not yet expressed the direction of their policy.

As the legal uncertainty and the national differences hamper the uptake of the Internal Market, we are of the opinion that a fundamental debate is required that goes well beyond the mere legal issues. This debate should take into account Europe’s core legal values (particularly property rights, freedom of information, freedom of expression, privacy, diversity and enforceability), and should take into account the interests of consumers, online service providers and rights holders.

Although we are convinced that many improvements can be made to the current legal frameworks, we therefore think a more thorough revision may be required.

7. Open issues

Language barrier – Compared to countries such as the United States and Japan, which host a large homogenous group of citizens that speak the same language and share similar cultural values, the European Union is characterised by a multitude of languages and cultural values. These internal differences are a core value and important advantage of the European Union, but simultaneously also represent an important obstacle towards the creation of an internal market in the online society. Although it can be expected that information technology — particularly automated translation tools — will improve over time, it remains to be seen whether these technologies will sufficiently lower the language barrier to convince citizens of one Member State to buy products or services in another Member State.\footnote{Already, some online service providers (such as the Google search engine and social website Netlog) are experimenting with on-the-fly translation of content.}

Cyber terrorism – Even with strong computer crime laws, it cannot be excluded that acts of cyber terrorism will occur, as is also the case in the offline environment. We consider this a public defence matter, which is mainly beyond the scope of regular internet law. Although initiatives should be taken to enhance the security of web systems and increase the resilience of computer networks, this remains an open issue.

Local versus global – While we believe that most of the challenges identified in this report (legal duality, the legislator's "cold feet", online naivety of citizens, endangered intermediaries, etc.) can be resolved in the long term, the issue will remain that the Internet is inherently global and cross-border, while legal rules are local and geographically limited. Although an appropriate amount of self-regulation, international treaties and cross-border cooperation between authorities can mitigate this concern, the locality of the rules will also remain an open issue.
EU study on the

Legal analysis of a
Single Market for the Information Society

New rules for a new age?

4. The future of online privacy and data protection

November 2009
# Table of contents

Chapter 4 The future of online privacy and data protection...........................................................2

1. Introduction...............................................................................................................................2
   1.1. Background of the current legal framework...............................................................3
   1.2. Applicable Directives .......................................................................................................5

2. A changing social and technological landscape...................................................................7
   2.1. Web 1.0...........................................................................................................................8
   2.2. Web 2.0...........................................................................................................................8
   2.3. Massive data collection..................................................................................................12

3. Status of privacy in today's society....................................................................................17

4. Shortcomings of the current EU legal framework...............................................................18
   4.1. Concept of personal data...............................................................................................18
   4.2. "Processing" of personal data.......................................................................................22
   4.3. Vague and overlapping rules on the applicable law..................................................23
   4.4. Rigid obligations regarding the transfer to third countries..........................................26
   4.5. Administrative obligations..........................................................................................31
   4.6. Inadequate distinction between controllers and processors.......................................32
   4.7. Problematic scope of "sensitive data".........................................................................35
   4.8. Legal uncertainty with respect to data retention terms................................................36
   4.9. Legal uncertainty regarding profiling..........................................................................37
   4.10. Difficulties with respect to the legal grounds for processing......................................39

5. Policy shortcomings ..............................................................................................................40
   5.1. Lack of enforcement.......................................................................................................40
   5.2. Implementation differences between Member States.................................................41

6. Shortcomings caused by data controllers............................................................................41
   6.1. Mere formal compliance with transparency requirements..........................................41
   6.2. Privacy and data protection as an afterthought...........................................................43

7. Comparisons..........................................................................................................................44
   7.1. Comparison with the US..............................................................................................44
   7.2. Comparison with Japan..................................................................................................46

8. Conclusions.............................................................................................................................49

9. Recommendations..................................................................................................................51
   9.1. Guiding principles for each recommendation..............................................................51
   9.2. Short term......................................................................................................................52
   9.3. Mid-term.......................................................................................................................64

---

This study was commissioned by the European Commission's Information Society and Media Directorate-General, in response to the invitation to tender OJ 2007/S 202 244659 of 19/10/2007. The study does not, however, express the Commission's official views. The views expressed and all recommendations made are those of the authors.
Chapter 4
The future of online privacy and data protection

This chapter regarding the future of online privacy and data protection does not (nor does any other chapter in this study) represent the views of the European Commission, and is independent from and does not build upon the results of the Consultation on the legal framework for the fundamental right to protection of personal data issued by DG Freedom, Justice and Security on 9 July 2009 (ec.europa.eu/justice_home/news/consulting_public/news_consulting_0003_en.htm).

1. Introduction

In a landmark case of 2003, the European Court of Justice (ECJ) issued a preliminary ruling in the case against Ms Lindqvist, who was charged with breaching Swedish data protection laws for publishing on her personal website data regarding a number of people working with her on a voluntary basis in a parish of the Swedish church. The website contained information about Ms Lindqvist’s colleagues in the parish, including their names, telephone numbers and hobbies. She also mentioned on the website that one colleague had injured her foot and was on half-time on medical grounds. The colleagues concerned were not informed about the website, and had not consented to the publication of their data on the website. Moreover, the Swedish data protection authority was not informed.

According to the decision of the ECJ, the publishing of information on Ms Lindqvist’s website should be considered as a processing of personal data. Furthermore, the reference to the injured foot of Ms Lindqvist’s colleague is to be considered as so-called “sensitive” personal data, for which the processing is – in principle – prohibited. As a result, Ms Lindqvist had breached the EU data protection rules.

The ECJ’s interpretation of the Data Protection Directive did not come as a surprise for experts in data protection law, as the Court made a straightforward application of the basic principles of the EU Data Protection Directive. From a social and online perspective, however, the decision was quite remarkable, as the website created by Ms Lindqvist seemed rather trivial and harmless when compared to the then current websites.

Fast forward to today’s online context, where millions of citizens are publishing photos, blogs and texts about their family and friends on social community websites such as MySpace, Netlog and Facebook, often without these persons being informed of it. Similar to Ms Lindqvist, all these citizens are breaching the EU data protection rules, probably without even being aware of it. The Lindqvist case law is thus lurking in the background, waiting for yet another case to be brought before court. Meanwhile, the real privacy challenges can be found in the massive aggregation of data by a few players in the online

1 C-101/01 Lindqvist [2003] ECR I-12971
market, as well as the threat – some would say the opportunity – that personal information published today may still be accessible years ahead in the future.

The Lindqvist case can therefore be considered a prime example of the state of today’s EU data protection rules: valuable at the core, but outdated and overly concerned with formal obligations. This chapter will therefore assess the current state of the EU’s privacy and data protection rules in an online context.

1.1. Background of the current legal framework

1.1.1. Right to privacy

The foundation of the current EU data protection legislation framework can be found in the European Convention on Human Rights (ECHR), adopted under the auspices of the Council of Europe in 1950. Article 8 ECHR considers the right to privacy as a fundamental human right:

"Everyone has the right to respect for his private and family life, his home and his correspondence."

Article 8 ECHR introduces protection for certain types of information: information related to a certain place (home) and to certain types of relationships (family ties and correspondence). It imposes a minimum requirement for the protection of human dignity and prevents disclosure of such information in the public sphere or to third parties. Over time, the interpretation of the privacy protection enshrined in article 8 ECHR has substantially varied and evolved, with evolutions in technology often being a driving force behind the extension of interpretation of this minimum requirement 3.

In addition to the ECHR, the right to privacy can also be found in other international treaties — such as the Universal Declaration of Human Rights (1948) and the International Covenant on Civil and Political Rights (1966) — and various national constitutions.

1.1.2. Right to protection of personal data

A second generation of legislative efforts considered the protection of personal data as a separate fundamental right, distinct from the right to privacy. This new right is often described as the right of information self-determination, i.e. the right to have a say in how data relating to oneself are processed by others 4.

The introduction of a new right was considered necessary to protect citizens against the dangers caused by the explosion of information power brought about by new computing possibilities in the 1960s and 1970s (speed, bandwidth, inter-connectivity, ...). Data protection laws have therefore been characterised as regulatory reactions to technological developments. They particularly tried to provide an answer to growing public concerns regarding the possibility of integrating data into centralised databanks 5, businesses’ appetite for information, the growing interest of organisations in basing their decisions on data existing in structured databases (diminishing the role of data subjects in decision-making), the

---

3 Y. POULLET, Pour une troisième génération de réglementation de protection des données, in M.V. PEREZ ASINARI and P. PALAZZI (eds.), Challenges of privacy and data protection law, Brussels, Bruylant, 2008, p. 38
difficulty to trace the flow of data due to the magnitude and complexity of cross-organisational data flows, and the growing body of evidence indicating that the quality of data utilised by organisations is insufﬁciently precise, correct, complete and/or relevant. However, an equally important impetus for introducing these international instruments, was the concern for the maintenance of free trade⁶.

The distinctive right was first introduced in the EU by the 1981 Convention n° 108 of the Council of Europe⁷, preceded by the 1980 OECD Guidelines⁸, which both set forth basic principles for the processing of personal data. Convention n° 108 holds that “it is desirable to extend the safeguards for everyone’s rights and fundamental freedoms, and in particular the right to the respect for privacy, taking account of the increasing flow across frontiers of personal data undergoing automatic processing.”⁹ Similarly, the OECD Guidelines refer to privacy protection laws, which have been introduced “to prevent what are considered to be violations of fundamental human rights, such as the unlawful storage of personal data, the storage of inaccurate personal data, or the abuse or unauthorised disclosure of such data.”¹⁰

These texts consider the protection of personal data as a distinct right. The raison d’être for this “new”, distinct right must be seen against the background of the evolution of technology. Combined with the issue that the application of article 8 EHCR to new technologies became increasingly difficult (as article 8 mainly focused on the protection against public authorities and uncertain scope of “private life”), it was considered necessary to introduce a new right.

1.1.3. Differences between the right to privacy and the right to data protection

Although data protection and privacy share certain features and goals, and are frequently used as synonyms, they are not identical. They are therefore described as being “twins, but not identical”¹¹.

Although clearly engrained in privacy protection, data protection does not necessarily raise privacy issues. Contrary to privacy rules, data protection rules are not prohibitive: they organise and control the way personal data are processed. According to the data protection rules, personal data can only be legitimately processed if some conditions pertaining to the transparency of the processing, the participation of the data subject and the accountability of the data controller are met¹².

Data protection is therefore both more narrow and more broad than privacy, as both concepts aim to protect partially other rights and values¹³. Data protection revolves around the processing of data, and therefore also covers the freedom of expression and the free flow of information. Privacy, on the other hand, also covers issues relating to the protection of an individual’s personal space — covering issues such as private communication, unwarranted investigations, physical integrity, protection of family life,

---

⁷ Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, adopted on 28 January 1981
⁹ Preamble of Convention n° 108
¹⁰ Preface OECD Guidelines
etc. Nonetheless, privacy remains the starting point for identifying and determining the principles of data protection.

1.1.4. **Scope of this chapter**

This chapter will mainly focus on data protection in the strict sense, although privacy protection will also be covered where relevant. Please note that some other topics that also deal with privacy (such as spam, net neutrality, online security and DRM) will be covered in other chapters of the study.

1.2. **Applicable Directives**

1.2.1. **Data Protection Directive**

The Data Protection Directive reused and extended the ideas of Convention n° 108. In addition to protecting citizens' fundamental rights, the Directive was targeted at the development of the internal market, as national laws of Member States diverged with respect to their rules regarding data protection, although most national rules were based on (or at least strongly influenced by) Convention n° 108\(^\text{14}\). The Data Protection Directive was adopted to harmonise the legislation of Member States and, thus, to ensure a free flow of personal data between Member States, which would in turn enable the free flow of goods and services, labour and capital\(^\text{15}\). Both objectives of the Directive (internal market and protection of fundamental rights) are considered equally important\(^\text{16}\).

Both Convention n° 108 and the OECD Guidelines remain applicable today, although their relevance is largely confined to support the interpretation of the Data Protection Directive. This report will therefore focus on the Data Protection Directive.

1.2.2. **E-privacy Directive**

The Data Protection Directive constitutes the fundamental legal framework for the processing of personal data. Since its adoption in 1995, various other Directives have been adopted which complement the Data Protection Directive in specific areas. For the purposes of this report, however, the E-privacy Directive\(^\text{17}\) is the most important complementary Directive\(^\text{18}\).

The E-privacy Directive was considered necessary to deal with the strong increase in communication and information technology, particularly the use of the Internet and developments such as digital mobile networks and electronic mail. However, the scope of the E-privacy Directive is often misunderstood.

---

\(^{14}\) Consideration 7 explains that "the difference in levels of protection of the rights and freedoms of individuals, notably the right to privacy, with regard to the processing of personal data (...) may prevent the transmission of such data from the territory of one Member State to that of another Member State; (...) whereas this difference in levels of protection is due to the existence of a wide variety of national laws, regulations and administrative provisions."

\(^{15}\) P. HUSTINX, o.c.

\(^{16}\) First report from the Commission, p. 3


Although its long title ("Directive concerning the processing of personal data and the protection of privacy in the electronic communications sector") and short title ("Directive on privacy and electronic communications") suggest that it contains a comprehensive overview of rules regarding data protection in the online world, this is actually not the case. As the E-privacy Directive is merely an additional layer on top of the fundamental layer provided by the Data Protection Directive, it only complements the Data Protection Directive, and deals with a few specific issues in the online context.

More specifically, the scope of the E-privacy Directive is limited to security of telecom networks (article 4), confidentiality of telecommunications (article 5), limitations on the data processed and stored by telecom operators (articles 6 - 12), unsolicited communications (article 13) and standardisation (article 14).

Out of these topics, only articles 4 and 5 are partially relevant for this report: article 4 is discussed in relation to data security breaches (section 9.2.3 below), while article 5 is discussed in relation to cookies (section 4.3.2). The other articles of the E-privacy Directive either do not present particular issues (data processed by telecom operators), or are dealt with by other chapters of the study.

1.2.3. Core principles

Continuing the course embarked by Convention n° 108 and the 1980 OECD Guidelines, the Data Protection Directive is based on the following principles. As will be further discussed in this chapter, we are of the opinion that these principles should (continue to) apply in an online context.

Accountability – Although not expressly set forth by the Data Protection Directive, the principle of accountability ensues from the various obligations imposed on data controllers. The Directive wants to enable "data subjects" — i.e., natural persons whose personal data are being processed — to contact and hold one party accountable for each processing that takes place. Such party is called the "data controller", and is considered by the Directive as the central actor which is responsible for any data processing. Any party to which a data controller delegates processing activities, is called a "data processor". As will be seen below (page 32), the distinction between data controller and data processors is being criticized, as the distinction is difficult to be drawn in more complex setups.

Fair and lawful processing – According to the Data Protection Directive, personal data can only be processed in a fair and lawful way, which means that the processing must necessarily be based on one of the legal grounds listed in article 7 of the Data Protection Directive. It also implies that the processing must, in principle, be in line with a data subject's reasonable expectations. This principle is crucial for today's online context, where personal data is often processed beyond the reasonable expectations of the data subjects.

Purpose limitation & specification – One of the core principles of the Data Protection Directive is that personal data can only be processed for specified, explicit and legitimate purposes. It is strictly prohibited for a data controller to further process personal data in a way. This principle is relevant to assess to which extent online "data harvesting" companies can use personal data for purposes that are not compatible with the purposes for which the data was initially collected.

Minimum storage term – Personal data can only be kept in an identifiable form during the period that is necessary for the purposes for which the data was collected. The Data Protection Directive requires personal data to be deleted or anonymised as soon as the necessity criterion is no longer met. Hence, the Data Protection Directive upholds the principle of a minimum storage term. This principle contradicts

19 see deep packet inspection in the chapter 9 (net neutrality), as well as chapter 10 (spam)
the assumption of a significant number of web companies today, which consider the personal data collected as "their property", and want to keep the data for an indefinite period of time.

**Transparency** – Data controllers must adequately inform data subjects of the types of personal data that are being collected, and the processing that takes place. As will be further explained below in section 6.1, data controllers in an online context often neglect this transparency requirement, are aim for mere formal compliance.

**Data quality** – Personal data that is processed must be adequate, relevant, not excessive, accurate and kept up to date. Hence, the Data Protection Directive does not allow a data controller to store personal data because *it might* possibly become useful in the future. Such data is not adequate, not relevant and/or excessive, and must therefore not be stored by the data controller (or be deleted or anonymised after collection).

**Security** – Personal data must be adequately protected against any type of harm. The level of security that is required, must be assessed by the data controller by balancing the risks, costs and importance of sensitiveness of the data concerned.

**Special categories of data** – While the Directive allows processing of most types of personal data (provided the aforementioned conditions are fulfilled), it upholds a principle prohibition to process certain types of personal data. Such so-called "sensitive personal data" — data relating to race or ethnicity, political opinions, religious or philosophical beliefs, as well as trade-union membership — can only be processed in exceptional circumstances, when more strict prerequisites are met. This principle is frequently (inadvertently) breached in the online context, in light of the consequences of the Lindqvist case law.

**Data minimisation** – Taking into account the principles of purpose limitation, minimum storage term and data quality, it is clear that the Data Protection Directive adheres to the principle of "data minimisation", which means that the processing must be restricted to the minimum amount possible. While not explicitly forth in the Data Protection Directive, this principle is adopted by the German data protection rules.

**Technology neutral** – The Directive is technology neutral, and does not make any references to specific technologies. Also, "personal data" is defined in such a way that it can be used and interpreted in a technologically neutral manner.

2. **A changing social and technological landscape**

*Today’s social and technological context is vastly different from the context at the time Convention n° 108 and the Data Protection Directive were adopted. This section 2 therefore describes new trends and technologies that impact the current legal framework for privacy and data protection. The emergence of these trends and technologies raises the question of whether the current data protection rules are still adequate.*

---

20 §3a of the German Federal Data Protection Act provides that data processing systems must strive to collect and process as few personal data as possible, and that (pseudo)anonymisation should be used when possible
2.1. **Web 1.0**

**Overview** – Political discussions on what eventually became the Data Protection Directive, started in 1990\(^{21}\). Even when the Directive was adopted in 1995, the existence of the Internet was still largely unknown to the general public, as even large software manufacturers assumed the Internet was a mere transitory trend\(^{22}\). As a result, several important privacy-impacting features of the Internet — decentralised storage of information, inherent trans-border nature, worldwide and public exposure of data, low threshold towards exchange of data — were not truly taken into account in the Directive.

While the E-privacy Directive was adopted to mitigate some important concerns in the context of online services, it mainly targets telecom operators, by issuing rules with respect to confidentiality of information, the use of traffic and location data, billing requirements and telephone directories\(^{23}\). Accordingly, the E-privacy Directive did not alleviate the fundamental concerns with respect to the reconciliation of the nature of the Internet and the strict requirements of the Data Protection Directive.

**Impact** – While the discrepancy with the EU data protection rules is particularly strong for the new "Web 2.0" Internet, it should be stressed that the traditional "Web 1.0" Internet\(^{24}\) also held a considerable amount of friction with the EU privacy and data protection rules, such as the inherent cross-border nature, the public exposure of sensitive personal data published on websites, and the low-threshold monitoring.

**No amendment in 2003** – Web 1.0 can therefore be described as having sown the seeds of the current privacy and data protection issues faced by Web 2.0. However, in the Web 1.0 era, it was considered that this friction was still manageable, and could be overcome by increased cooperation, refined case law, the adoption of the E-privacy Directive, as well as a more flexible interpretation of the existing rules. This view was also shared by the European Commission in its first report on the Data Protection Directive\(^{25}\).

2.2. **Web 2.0**

The Internet has evolved from a medium allowing limited two-way information provision in the mid nineties to what has been called "Web 2.0": a mature, distinctive medium characterized by user participation, openness, and network effects\(^{26}\). Properly channelled, Web 2.0 means connecting minds and creativity on a scale never before imagined\(^{27}\).

Web 2.0 is coined as a collection of different concurrent phenomena, for which the most important – from a privacy and data protection point of view – are described separately in the sections below.

\(^{21}\) The first draft was published in 1990 (Proposal Commission; Com 90/0314 Final), followed by a second draft in 1992 and a third draft 1993.

\(^{22}\) For example Microsoft: "As recently as 1995, Microsoft dismissed the Internet as a passing fad.", in J. WHITTAKER, *The Internet: the basics*, Routledge, 2002

\(^{23}\) As an exception, the rules regarding unsolicited communications (spam) apply to any party using electronic mail.

\(^{24}\) I.e., the web as used before the advent of the Web 2.0 phenomenon: see [http://en.wikipedia.org/wiki/Web_1.0](http://en.wikipedia.org/wiki/Web_1.0)

\(^{25}\) "Few contributors explicitly advocated the modification of the Directive." (p. 7); "the Commission notes its view that a modification of the Directive is neither necessary nor desirable at present is shared by a comfortable majority of Member States and also of national supervisory authorities." (p. 8)

\(^{26}\) T. O’REILLY, "Web 2.0 Principles and Best Practices", O’Reilly Radar Report

\(^{27}\) V. REDING, SPEECH/08/616, "Digital Europe: the Internet Mega-trends that will Shape Tomorrow’s Europe."
2.2.1. Social networks, virtual worlds and user generated content

Overview – The increased level of Internet and computer penetration have led to the growth of websites for user-generated content\textsuperscript{28}, virtual worlds\textsuperscript{29} and social networks\textsuperscript{30} (hereafter jointly referred to as "community sites"). Community sites have attracted a huge – and particularly young – audience, and have taken their place among the highest ranking websites in the world\textsuperscript{31}. They provide a collection of various ways for users to interact, such as text chat, voice chat, blogging, discussion forums, instant messaging, e-mail, video communication, etc. — effectively providing a sense of connectedness and intimacy among their members.

Impact on privacy – Community sites present various privacy issues:

Users give out too much personal information about themselves online, under the assumption that their information will only be consulted by friends and family members, so that they remain safe behind their computer screen. Although most community sites allow their users to reconfigure to which extent their personal data should be made public, users are often encouraged — by the website operator (e.g. through the default settings of the website) or through peer pressure — to share as much personal data as possible. Furthermore, even when the configuration of the data exposure is set to "friends and family only", users may not be aware that their list of online friends may include hundreds of people that they would not consider as friends in the offline context.

Community sites blur the boundary between private and public spheres, as private information is posted on a public medium.

For example, employees increasingly use community sites throughout their work day to stay in contact with their friends and family members\textsuperscript{32}. Employers, on the other hand, use community sites to find interesting potential employees.

Data posted on social networks can be easily downloaded by third parties to create a "digital dossier" of someone, which can in turn be used for purposes different from the ones the profile owner had considered\textsuperscript{33} \textsuperscript{34}.

Community sites expose various pieces of information about their members, which lowers the threshold towards identity theft. For example, social networks encourage their members to publish interesting bits of personal data (home address, phone, agenda schedule, social activities, …) that can easily be used for impersonating purposes.

Community sites have become virtual meeting places, where harassment and bullying can take place, particularly when combined with mobile phone technology\textsuperscript{35}.

\textsuperscript{28} such as YouTube and Flickr
\textsuperscript{29} such as SecondLife, Eve Online, World of Warcraft, etc.
\textsuperscript{30} such as Facebook, Netlog, Myspace, LinkedIn, Hyves, Twitter, etc.
\textsuperscript{31} At the time of writing, the Alexa rankings of Facebook, Myspace and Netlog are respectively fifth, seventh and sixty-sixth. \textit{See www.alexa.com/site/ds/top_sites}
\textsuperscript{32} For example, already in 2007 a survey carried out by web filter company Barracuda Networks found that 50% of businesses are blocking MySpace or Facebook to counter this trend: \textit{see www.barracudanetworks.com/news/news_and_events/index.php?mid=222}
\textsuperscript{33} G. HOGBEN (ENISA), \textit{ENISA Position Paper No.1 Security Issues and Recommendations for Online Social Networks}, October 2007, p. 8
\textsuperscript{34} The topic of unsolicited data aggregation is further discussed below in section 2.3.3
\textsuperscript{35} Mobile phone technology provides easy and instant digital camera and video facilities. The filming of an assault and then posting the video on social networking sites is considered to enhance the image of the attacker. See COUNCIL OF
Impact on data protection – In addition to various privacy issues, community sites also present important data protection issues:

The business model of community websites is aimed at the secondary use of the data gathered from their members (e.g., for marketing purposes). Such secondary use may conflict with the purpose limitation principle set forth in the Data Protection Directive. Anecdotal evidence indeed suggests that users do not fully understand the business model of community websites, and the possibility of such secondary use of data.

Due to the wide range of tools offered to members, the frequency and intensity of use, and the difficulty to migrate to other websites, community websites become centralised silos of personal data.

The centralised aggregation of different types of media (blogs, short messages, mails, photos and videos) constitutes an interesting breeding ground for cross-media data mining purposes. For example, by linking photos “tagged” by members with other photos through ever more powerful face recognition software or content-based image retrieval technology, pseudo-anonymous untagged photos can suddenly become valuable information.

There is ambiguity as to whether information posted on community websites (or even entire profiles) can be effectively deleted by members.

For example, the Facebook privacy policy states that “Removed information may persist in backup copies for a reasonable period of time but will not be generally available to members of Facebook.”.

2.2.2. Cloud computing, software-as-a-service and mashups

Description – Cloud computing refers to the increasingly popular computing metaphor whereby services are provided from the “cloud” (i.e., the Internet), without users having the knowledge of, or control over the technology infrastructure that supports them. Cloud computing is marketed as optimising computing resources, so that companies can request additional computing power at any moment, when the need arises. Customers engaging in cloud computing do not own the physical infrastructure serving, but instead consume computing resources as a service.

Cloud computing is closely related to grid computing (where computers are allowed to access the resources of other computers), as the computing power is often distributed across multiple computers, which can be located across the globe, and may even be operated by different vendors.

Examples of cloud computing services include Amazon’s Elastic Compute Cloud (EC2), Microsoft’s Azure, and Google’s AppEngine.

---

36 Content-based image retrieval (CBIR) is a technology for searching digital images in large databases.

37 CEPIS, o.c., p. 9

38 CEPIS, o.c., p. 11

39 Software development company IBM defines cloud computing as “an emerging computing paradigm where data and services reside in massively scalable data centres and can be ubiquitously accessed from any connected devices over the Internet” (see www.ibm.com/ibm/cloud)


41 Digital software magazine, November / December 2008, volume 27, issue 8
Cloud computing often incorporates software-as-a-service (SaaS), also called "utility computing", which is a business model whereby software services are rented and provided through the Internet on an as-needed basis, instead of being licensed through traditional software licenses. Such services can then be combined with other software services, possibly from various vendors. Services offered under this model, are often run from within a user's Internet browser.

Examples of SaaS services include Salesforce's online CRM software, Adobe's photoshop.com online photo editing software, Google Apps, and the WebEx web conferencing tools.

A mashup is a computing model in which internal and external software services are combined in a standardised way, in order to come up with a single integrated tool\(^{42}\). Mashup services are also apt to be combined with semantic web applications\(^{43}\).

A well-known example of a mashup is the use of cartographic data from one vendor to add location information to real estate data from another vendor, thereby creating a new and distinct software service that was not originally provided by either source\(^{44}\). Another example is Yahoo! Pipes, which allows users to build mashups by combining software services from Yahoo and various third parties.

It is important to note that cloud computing, SaaS and mashups are not limited to enterprise computing. Indeed, their distinctive features (centralised management of software, planned backups, availability from any client computers equipped with Internet access, etc.) are equally attractive for home users.

**Data protection issues** – Although technical literature considers cloud computing, software-as-a-service and mashups to be three distinct concepts, they all point towards the shift from a traditional, centralised computing model that is hosted by — or at least under the control of — the customer, to a new distributed computing model whereby the provision of computing services is delegated to third parties and the customer's decreased level control is exchanged for an increased level of flexibility\(^{45}\).

In our opinion, the most important data protection issue for these technologies can be found in the diminished control of the customer (data controller) over the data that is being processed by the parties to which the processing is delegated. For example, the very essence of cloud computing entails that a customer does not need to know, does not want to know and often cannot know where its data is being stored or processed. Instead of centrally hosting the data within a company's building, or hiring space in a well-known data centre, the data will now be stored "in the cloud" — i.e. distributed across data centres anywhere in the world.

Although delegation of processing is certainly not new, it is the significant degree with which control is delegated, the potentially vast amount of third parties involved, and the highly distributed model which can cause collisions with the requirements imposed by article 17.2 of the Data Protection Directive with respect to the selection and control of data processors.

A second data protection concern lies in cross-border transfers. In a typical cloud computing model, the data will be simultaneously stored on, and processed by, servers which can be located anywhere in the world and will collaborate in real-time to process the data. In fact, the geographical spread of data is acclaimed to be an important advantage of cloud computing, as — compared to a centralised, single


\(^{43}\) Described below, in section 2.3.2

\(^{44}\) Example taken from http://en.wikipedia.org/wiki/Mashup_%28web_application_hybrid%29

points of failure model — this better protects data against catastrophic failures\textsuperscript{46}. As a result, data will constantly cross geographical borders, which is liable to conflict with the strict rules on the transfer of personal data outside the EU\textsuperscript{47}.

**Security issues** — While only indirectly relevant from a data protection point of view, it should be pointed out that the decentralised nature of these new technologies poses new security questions to IT managers, because the old certainties that came with internally managed systems and well defined system boundaries, are no longer present\textsuperscript{48}. While decentralised data storage also provides security advantages, it should be recognised that they also present specific security disadvantages.

2.3. **Massive data collection**

2.3.1. **Profiling and data harvesting business models**

**Definition and general use** — Profiling can be defined as a computerised method involving data mining from data warehouses, which makes it possible to place individuals with a certain degree of probability in a particular category in order to take individual decisions relating to them\textsuperscript{49}. Profiling can be applied in a variety of different domains and for a variety of purposes. For example, by using profiling, companies can predict the behaviour of different types of customers, so that marketing strategies can be adjusted to fit specific categories, or even genuinely personalised marketing comes into reach. Profiling capacities have exponentially grown as a result of both the advances in technology, and the increasing availability of interesting data to analyze\textsuperscript{50}.

From a data protection and privacy point of view, profiling does not necessarily result in the identification of the natural persons concerned. In other words, for most applications, the profiler does not need to know the real name, contact details or other data that would directly identify the natural person.

**Application to the online context** — Profiling has expanded enormously since the arrival of Web 2.0. A significant amount of new companies on the Internet have a business model that is directly targeted at harvesting data from data subjects, and subsequently converting these massive streams of data into profiles. These profiles can then be used to make suggestions or recommendations to users, to improve

\textsuperscript{46} "Unlike desktop computing, where a hard disk crash can destroy all your valuable data, a computer crashing in the cloud doesn’t affect the storage of your data. That’s because data in the cloud is automatically duplicated, so nothing is ever lost." see M. MILLER, Cloud computing. Web-based applications that change the way you work and collaborate online, Que, 1st edition, 2008, p. 26

\textsuperscript{47} Some service providers are, however, aware of these issues under current EU data protection rules. Amazon, for example, offers "availability zones", whereby customers can choose regions in which their data is being stored and processed.

\textsuperscript{48} CEPIS, o.c., p. 1


services, to learn more about customers, or to generate personalised advertising on the Internet\textsuperscript{51}. Profiling is not necessarily a threat to users: authorities also recognise its value\textsuperscript{52}.

Such new business models often thrive on the aggregation of personal data, which has become a very valuable asset to companies, and is therefore often acclaimed to be the "new oil of the Internet and the new currency of the digital world"\textsuperscript{53}. Internet users are thus paying for services with their personal data and their exposure to (personalised) advertisements\textsuperscript{54}.

**Examples** – The following examples demonstrate today's wide variety of profiling applications:

- **Online bookstore Amazon** offers functions such as "Customers who bought this item also bought..." and "What do customers ultimately buy after viewing this item?", to make recommendations to users. These recommendations are based on the surfing and buying behaviour of other users in the online bookstore.

- The "Web History" feature of search engine Google stores each particular user's online behaviour, including their individual clicking behaviour, in order to deliver a better and more personalised search experience. This service may also use additional information from other Google services in order to deliver a more personalised experience\textsuperscript{55}.

  The Google "AdSense" advertising program uses cookies (installed on partner websites) to track the types of pages visited and content viewed by the user. Based on this information, Google shows interest-based advertisements: "For example, if you frequently visit travel websites, Google may show more ads related to travel. In addition to ads based on interest categories, Google also allows advertisers to show you ads based on your previous interactions with them, such as visits to their websites."\textsuperscript{56}

- **Online radio station Last.fm** offers a personalised radio station for each user, which selects music based on the listening behaviour of the user's profile, as compared to the profile of users with a similar taste of music.

- The "genius" feature of the online music shop iTunes recommends songs by combining the user's own ratings of music with the ratings of other users in Apple's database.

- The "Sentry" and "FamilySafe" software packages allow parents to monitor their child's activities online, by tracking each chat conversation, e-mail sent and website visited by the child. In September 2009 it was reported that the developer of these software packages also used the (often highly private) data of the child in a separate data mining service, to give businesses a glimpse of

---


\textsuperscript{52} See the Council of Europe’s document on profiling: "Considering that profiling may be in the legitimate interests of both the person who uses it and the person to whom it is applied, such as by leading to better market segmentation, allowing the analysis of risks and fraud, and adapting offers to meet demand; and considering that profiling may thus provide benefits for users, the economy, and society at large (...) ", available at http://www.coe.int/t/dg4/legal_affairs/legal_co-operation/data_protection/events/t-pd_and_t-pd-bur_meetings/2T.PD-BUR_2009_02rev4_en.pdf

\textsuperscript{53} M. KUNEVA (European Commission), Keynote Speech on the Roundtable on Online Data Collection, Targeting and Profiling, Brussels, 31 March 2009

\textsuperscript{54} M. KUNEVA, o.c.

\textsuperscript{55} See the privacy policy at www.google.com/history/privacy.html?hl=en

\textsuperscript{56} See the privacy policy FAQ at www.google.com/privacy_ads.html
children's chatter online, upcoming movies, computer games or clothing trends. Such information can help advertisers craft their marketing messages as buzz builds about a product\textsuperscript{57}.

**Impact on data protection** – Profiling and data harvesting inherently require a service provider to collect large amounts of user data in order to offer its services. Such user data is often collected surreptitiously, for example when cookies are used to monitor a user's clickstream, or via the inclusion of web bugs that are embedded in the invisible HTML code of a webpage\textsuperscript{58}. Moreover, data is preferably stored during an extended or even unlimited period of time. Such setup obviously contrasts with the data minimisation and transparency requirements laid down in the Data Protection Directive.

**Impact on privacy** – Although profiling is often very useful for users, profiling activities may also have drawbacks when they are used to take automatic decisions regarding users\textsuperscript{59}. Furthermore, even in cases where only abstract profiling data are used, issues of privacy intrusion may arise. It should be noted, however, that some companies that perform profiling, are aware of the privacy issues involved, and offer tools to configure to which extent personal data is being collected and processed.

### 2.3.2. Semantic web

**Description** – The so-called "semantic web" is a vision on the future of the World Wide Web, in which the semantics of information and services on the web are clearly defined by adding another layer of information to each webpage, which would make it possible for computers to better understand the content of the web\textsuperscript{60}. The semantic web thus provides a better structuring of data, which facilitates easier and more accurate information retrieving.

Although the semantic web is still in its infancy, most basic technologies are already in place, and some of them are already used in real applications. The semantic web is often proclaimed to become the next generation of the Internet, i.e. “Web 3.0“\textsuperscript{61}.

**Advantages** – One of the primary advantages of the semantic web is that it can enable data integration, so that data from various sources and in various formats can be combined and aggregated. Another advantage is that it enables computers to "understand" the content of the web, which facilitates more intelligent search queries and content retrieval. Through this data integration and understanding of the web, computers would be able to better combine pieces of data on the Internet (data aggregation).

**Threats** – It is clear that the data aggregation threats that already exist on the Internet, will be accelerated when the semantic web would become widely available. While the promise of enabling computers to "understand" and easily combine the knowledge found on various web pages can trigger useful and harmless applications, this new capabilities can equally be used to secretly build profiles of natural persons, as the semantic web allows to uncover information or patterns which may compromise confidentiality and privacy obligations.

\textsuperscript{57} [www.physorg.com/news171296608.html](http://www.physorg.com/news171296608.html)


\textsuperscript{59} See section 4.9 for a further discussion on profiling

\textsuperscript{60} See the Frequently Asked Questions of the W3C ([www.w3.org/2001/sw/SW-FAQ-.swgoels](http://www.w3.org/2001/sw/SW-FAQ-.swgoels))

\textsuperscript{61} P. MIKA, *Social Networks and the Semantic Web*, 2007, Springer, p. 23
2.3.3. Unsolicited data aggregation

Description – While profiling has many useful (harmless) applications and does not necessarily provide direct links to natural persons, and while the semantic web is still in its infancy, there is already a new type of business model, which we will describe here as "unsolicited data aggregation". This business model is targeted at the unsolicited – i.e. without any request at all from the data subject – collection, processing and aggregation of personal data available on the Internet, in order to come up with profiles or databases of natural persons. In other words, it collects unrelated pieces, which are put together to compile a full profile of a specific person.

This business model can use various technologies (data mining, statistical analyses, existing face recognition, voice recognition, etc.) and various sources of information (search engines, community sites, photo tagging websites, discussion forums, "deep packet inspection", etc.) for its data harvesting purposes. The profiles or databases can then be used for different business purposes, such as targeted marketing, background checks of employees, or quick information retrieval about specific individuals.

Examples – The following examples illustrate the concept of unsolicited data aggregation:

Plink gathered information that is freely available on the web, and displayed what it found on its website. On this website, users could search for specific persons, and they would be presented with the various bits of information found on the Internet about this person. Plink ultimately failed due to concerns from users about their privacy. After all, users were surprised that their data was published on Plink, as they never signed up to it.

Digital media company Phorm caught significant media attention when it announced to be in talks with several UK Internet access providers to deliver targeted advertising, based on "deep packet inspection" technology. The service would collect user interests and match them with advertisers, who wish to target that type of user.

2.3.4. Ambient intelligence

Description – Ambient intelligence — also called "ubiquitous computing" or "pervasive computing" in the US — can be concisely described as a vision on the future of consumer electronics, telecommunications and computing, in which virtually every product and service (clothes, money, wall paint, carpets, cars, etc.) have embedded intelligence. In this vision, the information society has become the convergence of ubiquitous computing, ubiquitous communication and interfaces that dynamically adapt to the user. In an ambient intelligence enabled environment, heterogeneous devices can communicate seamlessly with each other, "learn" through intelligent software and monitor user activities to predict what the user will do next. Ambient intelligence is sometimes also coined as the "Internet of things", although that term focuses on the objects involved.

RFID – One of the already existing technologies that is frequently linked with ambient intelligence, is Radio Frequency Identification (RFID), which consists of chips ("tags") that can be used for identification and tracking purposes using radio waves. RFID tags are already being used on a large scale for supply

Note that, to our knowledge, this term has not been used before.


I.e. a technology which analyses a user's Internet traffic, by analysing the low-level TCP/IP packets of Internet data. See Chapter 9 (net neutrality) for more information

See http://webwise.phorm.com

P. AHONEN, P. ALAHUHTA, B. DASKALA e.a., Safeguards in a world of ambient intelligence, Springer, 2008, p. xxi and 1
chain management, animal tracking, passport control and other purposes. Furthermore, e-health applications (such as the monitoring of vital health parameters) are being developed. The seamless connection of RFID tags through the Internet promises to allow far-reaching control over our environment.

**Advantages** – Ambient intelligence promises advantages of improved user friendliness of devices, improved efficiency of services, user empowerment and support for human interactions, as people will be surrounded by easy-to-use interfaces that are capable of interaction in an unobtrusive way.

**Threats** – Ambient intelligence is dependent on the permanent and real-time processing of personal data by massively deployed small devices. Intensive registration, monitoring and profiling are inherent characteristics of ambient intelligence.

From a privacy point of view, the most important threat of ambient intelligence lies in the increased surveillance possibilities, as the technology makes it possible to follow citizens’ preferences and behaviour. For example, even though most RFID tags can only store a very limited amount of information, they can be used to track the behaviour of natural persons wherever they go. A second privacy threat lies in the blurring of the boundaries between public and private spheres, as the ambient devices (for example body tags) track persons beyond the transition from professional or public to private spheres.

From a data protection point of view, on the other hand, the threat of ambient intelligence lies primarily in the aggregate collection of data by a massive amount of interconnected ambient devices, which enables extensive profiling. Convention n° 108 and the Data Protection Directive were conceived in an era where computing processes were fairly limited (e.g., mainly a few centralised mainframes), and were not conceived for data processing by millions of independent devices.

As a result, the very core of the rules on data protections are said to be entirely at odds with ambient intelligence. First, ambient intelligence typically thrives in a data maximisation context, which can be difficult to reconcile with the principle of data minimisation. Second, the purpose limitation principle is endangered, as the purpose for which data is being collected, is often not known beforehand, neither to

---

68 The “Study on the requirements and options for Radio Frequency Identification (RFID) application in healthcare” identifies the main obstacles for and uncertainties with respect to the deployment of RFID in European Healthcare. One of the critical uncertainties identified are privacy concerns. The survey conducted by the researchers revealed that privacy was one of the three most important barriers to RFID applications. However, the privacy barrier was felt to be relatively easy to overcome compared to most other barriers. See RAND, Study on the requirements and options for Radio Frequency Identification (RFID) application in healthcare, April 2009, p. 43, available at http://ec.europa.eu/information_society/activities/health/docs/studies/rfid200907/rfid-final-report.pdf
69 P. AHONEN, P. ALAHUHTA, B. DASKALA e.a., p. xxi and 1
70 P. AHONEN, P. ALAHUHTA, B. DASKALA e.a., p. 144-145
71 P. DE HERT, Legal safeguards, section 3.1
72 E.g., the "Oyster" contactless payment card used in the London Underground uses RFID tags to record each metro trip, time of entry and time of exit. Through combination with the other data available about each person in the computer systems, it is possible to store a person’s entire underground travelling behaviour.
73 P DE HERT, Legal safeguards, section 4.1
the data subject, not to the service provider. Third, the informed consent is difficult to apply to ambient intelligence, as the devices monitor citizens preferably in an unobtrusive, covert way\textsuperscript{74}.

3. **Status of privacy in today's society**

**Introduction** – The aforementioned social and technological evolutions have substantially changed both the reality and the perception of privacy. The aggregate of today's technologies and new services produces an extraordinary amount of personal data, available to an increasing number of actors. L. LESSIG even argues that, as these technologies further mature, there will be essentially no way for anyone living within ordinary society to escape from this\textsuperscript{75}. In this respect, already in 1999, Sun CEO Scott McNealy made the infamous statement "you already have zero privacy - get over it"\textsuperscript{76}.

The perception that we have – at least partially – lost control over our privacy, seems to have triggered a new way of dealing with privacy. Recent developments show a trend towards personal data being regarded as a commodity, not only between service providers and businesses, but also by data subjects themselves. New business models further encourage people to disclose personal data, in exchange for different services and functionalities: "(…) it's a trade-off, right, where you will give some of your privacy in order to gain some functionality (…) ultimately leave it to user choice so the user can decide"\textsuperscript{77}.

**Evaluation** – The question arises, however, whether an unlimited possibility to trade off personal data is desirable, and whether there is a point in time, where one knows too much about a person. Indeed, the impact of an unlimited trade-off right on one's privacy can be enormous, and may not always be obvious, due to the phased and fragmented nature of such trade-off.

\begin{quotation}
The public commotion regarding Facebook's surreptitious change of its terms and conditions last year\textsuperscript{78}, seems to indicate that there is public support for limiting the possibilities of exchanging personal data and privacy for functionality. When a blogger announced that Facebook had changed its terms and conditions, granting Facebook an eternal right to use any uploaded content (even after removal of such content by the subscriber), bloggers and social media around the world quickly picked up this news to protest against this change.
\end{quotation}

In our view, society should indeed be careful as regards the commoditisation of personal data, since the close link between personal data and privacy implies that such would effect the commoditisation of privacy. Even more, privacy is – and should remain to be – a fundamental human right, worthy of the necessary statutory protective mechanisms. Especially in today's climate where trade-off between personal data and functionality has become common practice, it is important to ensure adequate mechanism for the protection of privacy are in place.

**Negative definition** – The commoditisation of privacy seems to ensue from the idea that the concept of privacy should be defined in relation to the intrusions thereof. Privacy is then interpreted as the protection from unjustified burdens, or defined in relation to the amount of harm caused by the trade-
The question arises, however, whether any intrusion of privacy is acceptable, and whether privacy should be determined as a kind of dignity, whereby the very idea of an intrusion is an offense to this dignity.

Similarly, P. DE HERT and S. GUTWIRTH also refer to the concept of interference when defining the negative role of privacy, i.e. protecting individuals against interference in their autonomy by both governments and private actors.

Positive definition – Positively defined, however, privacy guarantees individuals their freedom of self-determination, their right to be different and their autonomy to engage in relationships, their freedom of choice, their autonomy as regards – for example – their sexuality, health, personality building, social appearance and behaviour, and so on.

H. BURKET builds further on this idea, and considers privacy as a "fundamentally fundamental right", a right fundamental to the use of fundamental rights in an information society. In our view, given the changed nature of today's information society, the idea of privacy as a fundamentally fundamental right should be the point of departure when determining rules of data protection and processing in an online context. We believe that personal data of individuals should be protected regardless of their involvement in new technologies or the ever-growing use of Web 2.0 applications.

4. Shortcomings of the current EU legal framework

4.1. Concept of personal data

A first – and crucial – issue with respect to the EU data protection legal framework, is the scope of the concept "personal data". Article 2.a of the Data Protection Directive defines personal data as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."

This definition includes several distinct elements ("information", "relating to", "identified or identifiable" and "natural person") that must be cumulatively present in order for a certain data to be considered as personal data. It can already be pointed out that these elements are used to severely stretch the scope of the concept "personal data", particularly due to the reference to indirect identification. This wide interpretation is bound to cause problems in an online context.

4.1.1. Relative or absolute approach?

Overview – Of particular importance in the interpretation of personal data is the expression "identified or identifiable". In this respect, the recitals of the Data Protection Directive provides that account should be taken of all the means "likely reasonably to be used either by the controller or by any other person to
identify the said person" 84. This raises the question of whether a relative or absolute approach should be upheld with respect to the scope of personal data.

The relative versus absolute approach is particularly important with respect to the ongoing discussion of whether IP addresses can be considered as "personal data". When the absolute approach is followed, IP addresses shall be considered as personal data, because the Internet access provider can easily match the IP address with his subscriber's details.

If, on the other hand, the relative approach is followed, then — in most Member States — IP addresses only constitute personal data for Internet access providers and legal authorities (who can order the Internet access providers to expose the accompanying subscriber details). For all other parties, the IP addresses will as such not constitute personal data, as they are not "likely reasonable" to have other data available to identify the natural person behind an IP address85.

Both the Spanish Supreme Court86 and the Swedish Supreme Administrative Court87 have recently ruled that IP addresses must be considered as personal data. Both cases concerned the tracking of IP addresses in the context of illegal downloading.

The Spanish Court further clarified that by using a program on a P2P network, a person should know that much of the data entered on the network is of a public nature, including his IP address. Since this IP address must be considered as data of a public nature, the Spanish Civil Guard was not required to obtain judicial authorization before initiating the process of tracking down the user's IP address. The tracking procedure was lawful and not subject to the information requirements set out in article 11 of the Data Protection Directive.

The absolute approach emphasizes the idea that account should be taken of the means used by any other person. Thus, any situation where the combination of certain data with complementary information held by any other party (whether related to the data controller or not) allows linking such data to a natural person, would render the data "personal data". In other words, the qualification of "personal data" is independent from the persons considered: as soon as data qualifies as "personal data" for one person, it also qualifies as "personal data" for any other person according to the absolute approach.

Several commentators reject such an absolute interpretation of personal data, and find that personal data is a relative concept: the same data can be anonymous for one data holder, while being identifiable for another data holder88. According to these commentators, the emphasis should lie on the fact that the means likely reasonably to be used, should be taken into account.

Within the EU, it is not always clear which of these approaches is maintained. As a result, there is substantial uncertainty as regards the scope of the concept "personal data", and hence, the scope of the Data Protection Directive. Working Party 29, as well as the Member States, have adopted divergent points of view.

Practical example: Internet search services. A company wanted to provide search services related to address bar searches and DNS error traffic, by returning a standard search result page in case end-users type an invalid URL in the address bar of their browser (either a keyword or an error). For this purpose, the company cooperated with a major search engine provider, and

84 Recital 26 of the Preamble to the Data Protection Directive
85 This assumes that Internet access providers will not voluntarily hand over their subscribers’ personal data, and that possible litigation against Internet access providers is not a means "likely reasonably" to be used.
86 Supreme Court, 9 May 2008, Juzgado de Instrucción No7 de Sevilla v. Angela, available at www.caselex.com
supplied the search engine provider with the IP address of the end-users, so as to allow the provision of localized search results.

Since the company did not have access to the internet service providers’ databases with IP addresses and identification data of end-users, it was reasonably impossible for the company to identify any individual based on the data it processed. Nonetheless, the company had to take into account the risk of being considered as a data controller under EU law, due to the lack of a harmonized interpretation of the concept “personal data”, especially in relation to IP addresses.

Working Party 29 – Working Party 29 maintains an ambiguous position towards the question of whether a relative or an absolute interpretation of personal data should be applied. On the one hand, it acknowledges that the scope of the Data Protection Directive should not be overstretched, and that there are situations where the information will not be considered as personal data, as the combination with the complementary information is not "likely reasonably". Furthermore, it emphasized that "a mere hypothetical possibility to single out the individual is not enough to consider the person as 'identifiable'." This position suggests a relative approach.

Working Party 29 gives an example which relates to the use of serial numbers by pharmaceutical companies for the purposes of scientific research. When doctors only transmit random serial numbers to identify their patients, and when all measures have been taken to prevent the patients from being identified by the pharmaceutical company, Working Party 29 considers that the pharmaceutical company has no "likely reasonably" means to be used to identify the data subjects. Hence, the Working Party does not consider such serial numbers as personal data, despite the fact that they emanate from sensitive medical data. The Working Party even confirmed this view for similarly configured medical tests where the serial numbers would be transferred to the United States.

However, in other instances, Working Party 29 leans towards an absolute interpretation of personal data. For example, in its opinion on data protection issues related to search engines, the Working Party explained its view on IP addresses, for which identification can typically only be achieved indirectly with the help of Internet access providers. As law enforcement and national security authorities may order an ISP to provide the customer details associated with an IP address, Working Party 29 considers the IP addresses stored by search engines as personal data.

EU Member States approach – Even among EU Member States, there does not seem to be a consensus on whether to use a relative or absolute approach as regards the concept of personal data. For example, with respect to pseudonymised data, some Member States consider such data only as personal data with respect to a person who has access to both the data and the key, whereas such data

90 Ibid, p. 15: "If, taking into account 'all the means likely reasonably to be used by the controller or any other person', that possibility does not exist or is negligible, the person should not be considered as 'identifiable', and the information would not be considered as personal data"
91 Ibid, p. 15
92 Ibid, p. 20
94 And, in some Member States, private parties, through civil litigation
95 Opinion 148, p. 8
are not considered personal data for a person without access to the key. In this respect, Austrian law refers to "indirectly personal data", which is data of which a data controller, processor or recipient cannot determine the identity of the data subject with legally permissible means. The processing of such indirectly personal data is not entirely subject to the strict rules for processing personal data — for example, their transfer outside the EU does not require approval of the Austrian DPA and the data subject has no right to rectification or erasure, nor a right to object with respect to the processing of such data.

In the same sense, the UK Information Commissioner's Office finds that "the fact that there is a very slight hypothetical possibility that someone might be able to reconstruct the data in such a way that the data subject is identified is not sufficient to make the individual identifiable for the purposes of the Directive."

Belgian law maintains a different approach with respect to pseudonymised data. In principle all data, which still can be linked to an individual, are regarded as "personal", even if the data are processed by someone who cannot make that link.

4.1.2. Other issues related to the concept of "personal data"

As regards the other three elements of the definition of "personal data", the question also arises whether the current interpretation maintained in Europe is overly excessive. This current interpretation is mainly due to the almost unlimited scope enabled by the use of the word "indirectly" in the definition of personal data.

Relating to – With respect to the "relating to" criterion, Working Party 29 maintains a rather extensive interpretation as well. It finds that, in order to consider that data "relates" to an individual, it is sufficient that either a "content", "purpose", or "result" element should be present:

The "content" element is present when certain information is "about" a person.

The "purpose" element refers to circumstances where the data is used or likely to be used with the purpose to evaluate, treat in a certain way or influence the status or behaviour of an individual.

An example given by Working Party 29 demonstrates the implications of this interpretation: "A system of satellite location is set up by a taxi company which makes it possible to determine the position of available taxis in real time. The purpose of the processing is to provide better service and save fuel, by assigning to each client ordering a cab the car that is closest to the client's address. Strictly speaking the data needed for that system is data relating to cars, not about the drivers. The purpose of the processing is not to evaluate the performance of taxi drivers, for instance through the optimization of their itineraries. Yet, the system does allow monitoring the performance of taxi drivers and checking whether they respect speed limits, seek appropriate itineraries, are at the steering wheel or are resting outside, etc. It can therefore have a considerable impact on these individuals, and as such the data may

---

98 Ibid, §12(3)(2)
99 Ibid, §29
101 Technical analysis to the Commission's First report on the implementation of the Data Protection Directive, o.c., p. 3
The "result" element is considered present if the use of data is likely to have an impact on a person's rights and interests.\textsuperscript{103}

Obviously, the interpretation of the "relating to" criterion is very extensive. Also this interpretation seems overly extensive, particularly when taking into account that the theory regarding "content", "purpose" or "result" cannot as such be found in the Data Protection Directive.

**Natural person** – The European Court of Justice has made clear that nothing prevents the Member States from extending the scope of their national legislation to areas not included within the scope of the Data Protection Directive, provided that no other provision of community law precludes it.\textsuperscript{104} In this respect, two Member States have extended the definition of personal data to legal persons. In Italy\textsuperscript{105} and Austria,\textsuperscript{106} data subjects can be either natural or legal persons.

**Including unstructured data** – It is important to note that, within an electronic context,\textsuperscript{108} the Data Protection Directive does not distinguish between structured data and unstructured data. As a result, the Data Protection Directive not only applies to data stored in databases or lists (structured data), but also to e-mails, text documents, blogs, videos, music, etc. (unstructured data). When taking into account the wide scope of the definition of "processing", as described in the next section, it is clear that the scope of the Data Protection Directive extends to surprising areas.\textsuperscript{109}

### 4.2. "Processing" of personal data

**Introduction** – The EU data protection rules only apply when personal data are "processed". Article 2.b of the Data Protection Directive defines the "processing" of personal data in a very broad way, which includes virtually any type of operation in relation to personal data: "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction".

**Amount of data processed** – The Data Protection Directive does not distinguish between processing activities based on the amount of personal data being processed. Even processing the smallest amount of personal data entails the applicability of the Data Protection Directive.
For example, the transfer outside the EU of a set of documents which only contain incidental personal data (such as the name of an addressee of a letter or meeting notes which contain the names of the persons present during the meeting) constitutes the processing of personal data. Hence, the company transferring such documents must comply with the Data Protection Directive, including the notification requirements and obligations in respect of data transfers outside the EU.

Impact on the online context – According to the Lindqvist case law of the European Court of Justice\textsuperscript{110}, the mere act of placing information on the Internet (for example, on a personal homepage) constitutes “processing” of personal data. Hence, almost any act performed on personal data constitutes a “processing” activity, including:

- publishing a blog in which another person is criticized;
- the mere act of consulting a website on which personal data is being published;
- drafting an e-mail, in which other persons are mentioned;
- storing e-mail in a (corporate\textsuperscript{111}) e-mail box; and
- drafting an electronic contract that mentions other persons.

Evaluation – Although the Working Party has not yet published an opinion about the scope of the definition of “processing”, it can be assumed — based on the Working Party’s very broad interpretation of the concept of personal data\textsuperscript{112} — that the opinion of the Working Party will align with the examples set forth above. As a consequence, almost any operation in an online context (which is, by definition, by automatic means) will constitute a processing of personal data. When the wide interpretation of personal data is factored in, this means that the scope of the Data Protection Directive, and the various ensuing obligations, becomes very extensive: citizens that merely surf the web, therefore constantly process personal data, without being aware of it.

4.3. Vague and overlapping rules on the applicable law

Article 4.1 of the Data Protection Directive holds that a Member State shall apply its national law to the processing of personal data in, essentially, two situations: either when the data is being processed "in the context of the activities of an establishment of a controller on the territory of the Member State", or when a controller established outside the European Union "makes use of equipment (...) situated on the territory of the Member State".

This article provides the rules for determining whether EU data protection law applies to certain processing activities, and specifies which national law shall be applicable in such case. The main purpose of this article 4.1 is to avoid both conflicts of law as well as lacunae where no law applies\textsuperscript{113}. The Commission has recognized that this is one of the most important provisions of the Data Protection Directive from the perspective of the internal market, and that its correct implementation is crucial for the functioning of the system\textsuperscript{114}.

\textsuperscript{110} See the introductory section on p. 2
\textsuperscript{111} e-mails for purely personal or household activities, are exempted on the basis of article 3.2
\textsuperscript{112} Working Party, Opinion 4/2007 on the concept of personal data (WP 136)
\textsuperscript{113} Analysis and impact study on the implementation of Directive EC 95/46 in Member States, i.c., p. 6
4.3.1. Establishment

The first main rule set forth by article 4.1 of the Data Protection Directive uses the controller’s “establishment” on the territory of a Member State as the determining criterion for the applicable law: when the processing takes place “in the context of the activities of an establishment”, this Member State’s national data protection rules shall apply. However, many Member States’ national implementations of article 4.1 differ from the original wording of the Directive. Furthermore, several Member States maintain their own extensive interpretation of the concept “establishment”. Accordingly, the application of this article has created considerable uncertainties towards data controllers.

**United Kingdom** – The United Kingdom uses a straightforward implementation of the Directive: article 5.1.a provides that the UK Data Protection Act applies when the data controller is established in the United Kingdom and the data are processed in the context of that establishment. Article 5.3 further specifies the concept “establishment”: (a) an individual who is ordinarily resident in the United Kingdom, (b) a body incorporated under the law of, or of any part of, the United Kingdom, (c) a partnership or other unincorporated association formed under the law of any part of the United Kingdom, and (d) any person who does not fall within paragraph (a), (b) or (c) but maintains in the United Kingdom an office, branch or agency through which he carries on any activity, or a regular practice.

**Spain** – Spanish data protection law contains provisions on the territorial application that differ from the general rule set out in the Directive. Article 2 of the Spanish Data Protection Act refers to the processing of personal data which is carried out on the Spanish territory as part of the activities of an establishment of the data controller. Contrary to the Data Protection Directive, Spanish law does not properly describe the first rule of article 4.1, which states that the controllers’ establishment is the determinant ground for an application of the respective Member State’s law.

**Greece** – The Greek Data Protection Act does not require the processing having to take place “within the context of the activities” of an establishment of the data controller on its territory, in order for Greek law to be applicable.

**Finland and Sweden** – In Finland and Sweden, any economic activity by a company might lead to the company being considered “established” for the purpose of applying local data protection law. This could mean, for example, that the mere presence in Finland or Sweden of salespeople concluding commercial contracts that result in the processing of personal data of Finnish or Swedish citizens could cause the company to be established in those countries for data protection purposes.

4.3.2. Use of equipment

**Overview** – Article 4.1.c of the Data Protection Directive provides that Member States must apply their national law if a controller that is not established on EU territory, makes use of equipment situated on their territory. This provision was introduced to avoid that data controllers could easily escape the EU

---

115 First report of the Commission, p. 17
119 Analysis and impact study on the implementation of Directive EC 95/46 in Member States, i.e., p. 6
120 C. KUNER, o.c., p. 118
121 For instance, in an unpublished case, McDonald’s was found to be “established” in Finland based on advertising that was transmitted into the country from abroad via cable television. See C. KUNER, o.c., p. 84
data protection rules by moving their place of establishment out of the EU, but nevertheless collecting personal data within the EU. The EU data protection rules would therefore even apply in a situation where a data controller would remotely operate a computer, telecommunications network or other physical object located within the EU, via its establishment outside the EU.\(^\text{122}\)

While the legal intentions behind the "use of equipment" can be appreciated, it should be recognized that this provision has created a great deal of uncertainty, because the concept of "equipment" is interpreted rather extensively, so that EU law often applies beyond the territorial boundaries of the Member States. Moreover, several Member States have used variations and extensions of the concept "equipment" in their national laws. Some countries use a term of which the translation into English refers to "means" rather than to "equipment".\(^\text{123}\) Whereas "equipment" may be interpreted as a physical apparatus, "means" has a far more comprehensive meaning, as all processing can be considered to involve "means".\(^\text{124}\)

The problems caused by the wide scope of article 4.1.c of the Data Protection Directive were already recognised by the European Commission and various stakeholders in the first review of the Data Protection Directive\(^\text{125}\), but has become even more problematic in an online context due to the extremely wide application of the concept of "equipment" to so-called cookies.

**The cookie case** – Cookies are small bits of information that are stored by the visitor's web browser at the request of the website operator. Cookies typically do not store large amounts of (personal) data: most web browsers do not even allow cookies larger than 4 kilobytes stored in a given domain.\(^\text{126}\) In practice, cookies are typically used to store relatively unimportant and harmless information, such as a user's preferred language, shopping cart contents or personal website preferences. However, cookies can also store unique identifiers that allow website operators to identify visitors during a subsequent visit, as well as easy data aggregation across websites. In such circumstances, cookies act as the crucial key towards online profiling of website visitor, which is the reason why cookies have gained a bad reputation from a data protection point of view, despite the fact that cookies themselves can only store a very limited amount of information.\(^\text{127}\)

In principle, article 5.2 of the E-privacy Directive requires website operators to provide visitors with clear and comprehensive information on the use and purpose of cookies. Furthermore, visitors should have the possibility to refuse accepting cookies, unless "strictly necessary" to provide an online service. In practice, however, these requirements remain dead letter. Visitors are only informed of cookies through opaque provisions (if any) in a website's privacy policy. Also, considering that the use of cookies is only "strictly necessary" for a few websites,\(^\text{128}\) most websites should present visitors with the option to refuse cookies,\(^\text{129}\) which is clearly not the case.

---

\(^\text{122}\) C. KUNER, o.c., p. 120

\(^\text{123}\) For example, in French: "moyens", Italian: "mezzi" and Spanish: "medios", technical analysis to the Commission's First report on the implementation of the Data Protection Directive, l.c., p. 7

\(^\text{124}\) Ibid.

\(^\text{125}\) First Report of the Commission, p. 17

\(^\text{126}\) See http://en.wikipedia.org/wiki/HTTP_cookie

\(^\text{127}\) It should be noted, however, that new technology (so-called Flash cookies and domStorage cookies) allow a website operator to store larger amounts of data.

\(^\text{128}\) E.g., to store the content of a "shopping basket" on a webshop

\(^\text{129}\) It could be argued, however, that the possibility to refuse cookies is almost always met, due to the fact that a user can change his web browser's default cookie settings. However, the Working Party 29 does not seem to agree with this point of
Working Party 29 is of the opinion that a user’s personal computer can qualify as equipment in the sense of the Directive. When a website operator uses cookies on a website, it is considered that the website visitor’s PC is “used” by the website operator for processing personal data. Accordingly, Working Party 29 is of the opinion that the national law of the Member State where a user’s personal computer is located, applies to the website operator’s processing of the visitor’s personal data.

This consequences of this interpretation cannot be underestimated: considering that the majority of websites outside the EU makes use of some type of — permanent or temporary — cookie, the position of the Working Party would imply that the majority of foreign websites is subject to the EU data protection rules. Furthermore, this implies that such website operators would become subject to a multitude of national laws, as the applicable law would depend on the then current location of the visitor of the website.

4.3.3. Law applicable to privacy & data protection breaches

Discouragement to litigate – There is a substantial amount of legal uncertainty regarding the question which law will apply in cases of breaches of privacy law or data protection laws, for example when a citizen claims under tort law that a data controller has harmed is rights by unlawfully processing his personal data. As a result, citizens will be less inclined to enforce their rights in cross-border cases, considering that any court action is liable to be countered by complex procedural questions, and legal action may (depending on the circumstances) perhaps only be brought before the courts of another Member State. The cost, complexity and efforts involved such litigation will deter most citizens from seeking redress, particularly when taking into account that the impact of individual data protection breaches is often rather low (at least when considered in isolation).

Rome II – Policymakers recognised these concerns, and tried to include clear rules on the applicable law during the drafting process of the so-called “Rome II” regulation regarding the law applicable to non-contractual obligations. However, the adoption of such rules constituted one of the most heated debates that hampered the drafting of Rome II, so that it was dropped eventually.

4.4. Rigid obligations regarding the transfer to third countries

4.4.1. Overview of article 25

Article 25 of the Data Protection Directive provides that the transfer of personal data to a third country may only take place if the third country in question ensures an adequate level of protection. When this

view: “The responsibility for their processing cannot be reduced to the responsibility of the user for taking or not taking certain precautions in his browser settings.” (Opinion 148 on search engines, p. 20)

Working document n° 56

The Rome II regulation ("Regulation no 864/2007 of 11 July 2007 on the law applicable to non-contractual obligations") creates a harmonized set of rules within the European Union to decide which law will be applicable to non-contractual obligations between parties, similar to the preceding Rome I Convention (1980) that addressed applicable law for contractual obligations.

The lack of resolution in Rome II over which Member State’s law applies, had brought fierce protest from publishers, journalists, and broadcasters organizations that feared the detrimental effects of forum shopping on the freedom of expression.
level of protection is not offered by the third country, and none of the derogations set forth in article 26.1 apply, legal workarounds must be sought to ensure that the EU level of protection is continued to be guaranteed when data is exported to third countries. Article 25 thus prevents that the high level of protection offered by the EU Data protection rules would be virtually annihilated in an international context. While the original intentions of this EU-centric, unilateral approach to information processing can be appreciated, it may no longer reflects today’s reality.

Assumptions no longer hold true – Article 25 is based on the assumption that data processing can be limited to certain physical and geographical boundaries. This assumption was reasonably realistic at the time the Data Protection Directive was adopted because — although large-scale networks were already employed by large organisations and companies — cross-border data flows were fairly limited and generally manageable at the time. However, as from the public adoption of the Internet, this assumption has become increasingly difficult to sustain, as servers are located across the world, particularly in the United States.

With the advent of Web 2.0 and its distributed computing concepts such as cloud computing and software-as-a-service, the assumption is clearly out of date: where the physical location of one or more servers was still controllable in the traditional "client-server" setup of Web 1.0, the decentralised nature of cloud computing prevents parties from mapping the geographical location of the computer servers used to process its personal data. Hence, the Data Protection Directive does not seem adequate to deal with the consequences of today’s globalised society and the rise and development of the Internet.

Rigid adequacy test – Fourteen years after the adoption of the Data Protection Directive, only six countries have been found to provide an adequate level of protection with respect to personal data: Switzerland, Canada, Argentina, Guernsey, Jersey and the Isle of Man. Emerging new economies such as India, Brazil, Japan and Russia, have not yet been recognized as providing adequate protection. This lack of an extended "white list" for adequate data protection, is partly the result of the rigid criteria applied by the Commission. De facto, the test being applied to third countries constitutes an equivalence (i.e. transposition) test rather than an adequacy test.

Issues linked to exceptions – While the Data Protection Directive provides for several exceptions, various issues can be identified that undermine the practical importance or viability of these exceptions.

Article 26.1.a allows a transfer when the unambiguous consent of the data subject has been obtained for the proposed transfer. Consequently, privacy policies often state that the data subject indeed consents to such transfer, which seemingly results in formal compliance with the Data Protection Directive. However, as described in section 6.1 below, consent in an online context is not problem-free. Furthermore, consent is particularly problematic for some data subjects, such as employees towards their employers, and young persons in general. Finally, it should be noted that consent is a precarious legal basis, because it can always be revoked. As a result, online service providers are recommended to only rely on consent as a legal basis for transfer in specific circumstances.

133 See section 2.2.2 on p. 10
134 An overview of all Commission decisions on the adequacy of the protection of personal data in third countries is available at http://ec.europa.eu/justice_home/fsj/privacy/thirdcountries/index_en.htm#countries
136 Some national data protection authorities do not recognise employee consent as a valid legal ground, as their "consent" can be easily undermined by the implicit pressure from the employer: see Opinion 8/2001 of Working Party 29 on the processing of personal data in the employment context.
Article 26.1.b allows a transfer to third countries when the transfer is necessary for the performance of a contract with the data subject (or the implementation of pre-contractual measures). Although this derogation seems useful in many contexts, national data protection authorities significantly narrow down the scope of this derogation, due to the strict application of the "necessity" criterion.\(^\text{137}\)

The scope of the derogation set forth in article 26.1.c (necessity for the conclusion or performance of a contract concluded in the interest of the data subject) is equally limited, due to a narrow interpretation of the "necessity" criterion.\(^\text{138}\)

In addition to the derogations, several legal "workarounds" are available to allow parties to transfer personal data to third countries that do not offer an adequate level of protection. These are discussed below in sections 4.4.2, 4.4.3 and 4.4.4.

Paradox – An interesting illustration of the consequences of the EU-centric approach of the Data Protection Directive can be found in the paradox that personal data which was collected in a third country, and is then transferred to the EU for further processing, can – in principle – not be transferred back to the original third country, because the Data Protection Directive considers such country to offer no adequate protection. This paradox is due to the fact that the Data Protection Directive does not differentiate between personal data collected inside or outside Europe, and does not provide exceptions for lawful processing when data is collected in accordance with the local laws where the data was initially collected. This paradox could severely undermine the competitive position of European companies that want to offer data processing services. Considering the ever-increasing focus on data hosting and management services, this disadvantage should not be underestimated.

The competitive disadvantage which may be suffered by European companies becomes even more clear when one envisages a situation whereby personal data can be lawfully collected in a third country, but cannot be processed under EU data protection rules.

\[\text{For example, trade-union membership data can be lawfully collected in third country X without explicit consent. Although a company established in X is allowed to collect such data within X, this data cannot be transferred to Europe for further processing, as the Data Protection Directive does not allow the processing of trade-union membership data without the explicit consent of the data subjects concerned.}\]

4.4.2. EU model clauses

Article 26.4 of the Data Protection Directive provides that the European Commission may decide that certain standard contractual clauses offer sufficient safeguards as required by the Data Protection Directive. By entering into a contract that is based on such contractual clauses, an entity established in the EU can then lawfully transfer personal data to a party outside the EU.

The European Commission has approved three sets of contractual clauses, two of which apply to transfers from data controllers to controllers in third countries, and one of which applies to transfers from data controllers to processors in third countries.\(^\text{139}\)

---

\(^{137}\) See, for example, p. 19 of the policy paper of the Dutch data protection authorities on the transfer to third countries (available at www.dutchdpa.nl/documenten/en_int_policy_paper.shtml): "the transfer in question should be necessary. In other words, this exception does not apply if a transfer would be useful or facilitate the performance of the contract, but is not really necessary" (highlights added). See p. 13 of WP 105 "on a common interpretation of Article 26(1)" from Working Party 29: "Furthermore, a strict interpretation of this exception means that the data transferred must be truly necessary to the purpose of the performance of this contract or of these precontractual measures."

\(^{138}\) See p. 13 and 14 of WP 105: "[the transfer] must pass the corresponding "necessity test". (...) This test requires a close and substantial connection between the data subject's interest and the purposes of the contract."
Evaluation – Whereas these model clauses provide an adequate solution when only a limited number of parties are involved in the transfer, the model clauses become very difficult to use in practice if multiple parties are involved\textsuperscript{141}. In addition to the difficult management of these contracts when a large number of parties is involved, it should also be mentioned that Member States still require additional formalities to be fulfilled, even if the parties involved conclude a model clauses agreement.

\begin{quote}
For example, under Dutch data protection law, personal data may be transferred outside the EU only when the Dutch data protection authority has granted a permit, even if the data are transferred using the EU-approved standard contractual clauses\textsuperscript{142}.
\end{quote}

While the EU model clauses may seem an efficient legal instrument for data protection compliance, it should be pointed out that the administrative overhead and practical issues involved may be prohibitive for a sheer number of business situations, when the required speed of a transaction is difficult to be reconciled with the contracting process involved for the model clauses.

Practical example: complex outsourcing. A multinational corporation intended to outsource the human resources business processes of 23 of its European entities to an offshore service provider. The services to be provided included processes relating to recruitment and employee life cycles. To this end, the European entities needed to provide the offshore service provider with a substantial amount of personal data concerning past, current and future employees.

As the different entities of the corporation need to be considered as 23 separate data controllers, the corporation had to conclude a model clauses agreement with the service provider for each of its 23 entities. Moreover, the corporation incurred considerable legal costs, since it had to verify in each of these 23 countries whether the national law imposed additional requirements for data transfers based on the EU model clauses. In addition, this procedure entailed a substantial delay in the negotiation process with the service provider, as in some cases, it had to obtain the permission of the national data protection authority.

Sub-processing – The European Commission recently acknowledged the need to adapt the standard contractual clauses, especially in the context of global outsourcing where companies not only transfer their data to a processor, but to “sub processors” and even “sub-sub processors”\textsuperscript{143}. The Commission therefore envisages the adoption of a new decision based on article 26.4 of the Data Protection Directive.

The draft Commission decision would allow a processor established in a third country to carry out onward transfers for the purposes of sub processing only with an authorization granted by the controller. Processors established in the EU which want to subcontract their activities to a processor outside the EU

\begin{footnotes}
\item[139] Decision 2001/497/EC and Decision 2004/915/EC
\item[140] Decision 2002/16/EC
\item[141] For example, when two companies are involved, one contract needs to be executed. When four companies are involved, six contracts need to be executed. When twenty companies are involved, 190 contracts would need to be executed. Alternative approaches (e.g., the use of a “master agreement” that is signed by each party involved) may then prove a more efficient solution, although they require careful drafting and planning.
\end{footnotes}
would need to continue to use the current model clauses. As pointed out by Working Party 29, this approach could cause a competitive disadvantage to European processing companies, since they would be required to bear an administrative burden greater than that of processing companies outside the EU.

Working Party 29 also pointed out the risk of major chains of sub processors, that might act independently of the data controller's instructions. It therefore accepted the introduction of a "multi-layered" sub processing clause, so as to ensure that the model clauses are apt to deal with the reality existing business models, which tend to sub-contract and subsequently sub-sub-contract processing activities.

Although the proposed new decision based on article 26.4 of the Data Protection Directive addresses some issues of the model clauses, the problems identified above would remain to exist.

4.4.3. Binding Corporate Rules

Binding Corporate Rules (BCRs) are a tool to protect the privacy of data subjects, while facilitating international global transfers of personal data to corporate groups in countries without sufficient data protection legislation. Through the use of BCRs, an entire corporate group can become a "safe haven", in which personal data can be freely transferred from one group member to another. BCRs thus eliminate the need for each group member to conclude individual data transfer contracts with all other group members.

Evaluation – While the advantages of BCRs are clear, they are currently subject to a lengthy and complex approval process. Companies must submit their BCRs for approval with the data protection authority of each Member State from which they intend to transfer data. As a result, and due to disagreements among data protection authorities, very few BCR applications have been approved by multiple data protection authorities, which severely impacts their practical utility. Consequently, despite their interesting promises, BCRs have not been successful up to now.

In order to counter these Working Party 29 has created a working document which sets forth a cooperation procedure, so as to allow companies to limit the process of application for approval to one leading coordinator authority of one Member State. This coordinated procedure is intended to allow the company to obtain all required authorisations from all Member States where it operates via a single application procedure. It should be noted, however, that this is merely a coordinated procedure, and not a system of mutual recognition. Recently, thirteen data protection authorities have agreed to recognise the lead authority on a BCR application and to accept its approval of a BCR as the basis for their concurrent approval of the BCR application. Nine Member States had already accepted this "mutual recognition" procedure (France, Germany, Ireland, Italy, the United Kingdom, the Netherlands, Spain,

\[144\] Ibid., p. 3
\[145\] Ibid.
\[146\] Ibid., p. 4 and 5
Latvia and Luxembourg) and have recently been joined by four additional Member States (Norway, Iceland, Liechtenstein and Cyprus)\(^{149}\).

### 4.4.4. US Safe Harbor system

The US Safe Harbor system is a list administered by the International Trade Administration (ITA) of the US Department of Commerce. US companies that subscribe to the list undertake to respect the data protection principles set forth in the Data Protection Directive. Such companies are then considered to provide adequate protection in the context of data transfers. This enables EU business transactions for such US companies, since their joining the system implies that they can do business without additional administrative burdens (such as continuous conclusion of model clauses agreements).

**Evaluation** – While the safe harbor system provides for an efficient solution, it is obviously limited to companies established in the US. It could be interesting, however, to introduce similar voluntary accreditation lists for other countries.

### 4.5. Administrative obligations

In its report on the notification obligations (WP 106)\(^{150}\), Working Party 29 has provided an analysis of the current system of notification in the EU Member States. Working Party 29 has identified three main purposes for notification\(^{151}\):

- It is a major token of transparency for data subjects, and can be the starting point for lodging a complaint with the competent authorities, via the controls carried out in the Register of processing operations (or of notifications).
- It helps in raising the awareness of controllers of notification duties and keeps them "tuned" to the need for complying with data protection requirements.
- It allows data protection authorities to keep abreast of the data processing situation in their countries and, at the same time, enables several analyses to be carried out with a view to refining the approach to recommendation, audits and inspections.

However, in practice, it is highly questionable whether these aims are actually being achieved. Especially with respect to data subjects, it is unlikely that notifications made by data controllers contribute to transparency towards them, as a vast majority of European citizens is unaware of such obligation for controllers which their personal data.

Although the Data Protection Directive intended to avoid unsuitable administrative formalities, *inter alia* by providing exemptions from the notification obligation and simplification of the notification in specific cases\(^{152}\), the actual practice shows to be different. The exemptions provided by national law are often rarely applicable in practice. In addition, notification requirements often impose excessive administrative burdens upon data controllers.

---

\(^{149}\) Ibid.


\(^{151}\) Ibid, p. 6

\(^{152}\) Recital 46 and article 18 Data Protection Directive
For example, even after substantial simplification of the notification procedures by the Italian Data Protection Code which entered into force on 1 January 2004, notification in Italy still requires completion of a form that is 86 pages long. Some countries (for example Sweden and Lithuania) do not yet provide the possibility to complete the notification forms online, and require the notification to be sent to the data protection authority by letter. The UK and Ireland even require notifications to be renewed annually. Several countries (for example, Denmark, Ireland, Poland and UK) require payment of fees with respect to the notification, such fees to be paid annually and for large companies amounting up to £500 annually in the case of the UK.

As recognized by Working Party 29, these often excessive administrative requirements in relation to notification not only represent a burden for business, but undermine the whole rationale of notification by becoming an excessive burden for the data protection authorities.

4.6. Inadequate distinction between controllers and processors

Introduction – The Data Protection Directive makes a fundamental distinction between data controllers and data processors, based on the criterion of "determination of the purposes and means of the processing". Any entity which alone or jointly with others determines the purposes and means of the processing of personal data, is considered a "data controller", while all entities that process personal data on behalf of a controller, are considered "data processors". The consequence of the qualification as a controller should not be underestimated, as controllers are held accountable to both regulators and data subjects under the Data Protection Directive. The distinction has other practical consequences as well.

Evaluation – While the definition of data controller is clear in straightforward situations, it has become increasingly difficult to apply it to more complex situations, particularly when there are several parties that partially define either the means or the purpose of the processing. The following examples can clarify the difficulties encountered on a day-to-day basis:

---

155 Ibid.
156 Ibid.
157 Ibid.
161 Article 2.d and 2.e of the Data Protection Directive
162 For example, two different types of EU model clauses apply (controller-to-controller and controller-to-processor): see section 4.4.2
In a typical outsourcing relationship, it could be argued that the customer defines the overall means and purpose of the processing of personal data, because all data is ultimately processed for the business purposes of the customer, and the customer also selects the service provider as the "means" to process the personal data.

However, when each outsourced service is analysed in detail, it will become clear that in most typical outsourcing setups, it will be the service provider that defines how the data will processed. Most outsourcing contracts are mainly concerned about the output from the service provider, and leave it up to the service provider to figure out how the output can be achieved in the most efficient way. Under the current definition, it could therefore be argued that both the customer and the service provider should be considered as data controllers. On social websites such as Hyves, Facebook, Netlog and MySpace, both the website operator and many of the users of the website will qualify as data controller under the current definition (for example, when the user uploads photos). In practice, however, it will be clear that it will be the website operator who will predominantly define the purpose and the means of the processing.

This is confirmed by a recent opinion of Working Party 29, which finds that many social network users will – in principle – not be subject to data controller obligations, as they generally process personal data "in the course of a purely personal or household activity". However, in the following instances, a user's activities will not be covered by the so-called "household exemption":

- where the activities of a user extend beyond a purely personal or household activity, for example when the social network is used for professional reasons, or when members maintain a very large number of "friends" (links to other users) on their profile;
- when there is public access to profile information, or if the profile information is indexable by search engines; and
- where the application of the household exemption is constrained by the need to guarantee the rights of third parties, particularly with respect to sensitive data.

In practice, many social network users do maintain a large number of friends, or use their profile partially for professional reasons, or make their profile (partially) indexable by search engines. All such users will therefore need to be considered as data controllers according to the Working Party. This situation leads to several awkward consequences, most of which are not explicitly discussed by the Working Party:

- These users must inform all data subjects (i.e., their network "friends") about the fact that their personal data is being stored and published by the data controller. This obligation would thus require a user to inform each friend and third party about the fact that a photo or text is published in which he or she is portrayed or mentioned.
- These users are responsible for ensuring that all personal data is appropriately protected. However, while some security precautions (such as safeguarding the network login credentials) can obviously be taken by them, they have virtually no influence on the security of the underlying software and infrastructure of the social network.
- They are prohibited from using (or allowing third parties to use) the personal data for a purpose that lies outside one of the purposes for which the data was initially collected. However, many social

---

165 Opinion 5/2009 on online social networking (WP 136), 12 June 2009
166 Ibid., p. 6
networks perform various data mining operations on the data uploaded by their users. It is questionable whether such data mining still lies within the scope of the original purpose for which the data was collected by the user.

- In many Member States, social network users will need to notify their national data protection authority of their profile.

- Users must ask explicit permission from friends and third parties to publish information about them. Although explicit consent is not required when the processing is "necessary for the purposes of the legitimate interests pursued by the data controller", it will nevertheless be required when the interests of the data controller are overridden by the fundamental rights and freedoms of the data subject. This involves a delicate balancing exercise between the interests of the data controller and the interests of the data subject, which may be difficult to perform in practice (e.g., does a picture of a friend in a bikini on the beach breach the interests of this friend?). Furthermore, explicit consent – in some EU Member States even written consent – will always be necessary when sensitive data (such as racial, ethnical, medical and religious data) is processed. Likely for these reasons, the Working Party seems to be of the opinion that explicit consent is usually required, as it recommends social network operators to remind users to obtain consent from their friends and third parties when uploading pictures or information about them.

**Popular online services** often define in their general terms and conditions that for any personal data processed through the service, the user – and not the service provider – will be considered the data controller. Although such contractual provision clearly tries to lay the liability burden with the user, it mainly emphasizes the subordinate position of the user vis-à-vis the service provider. It is therefore questionable whether it is really the user who defines the means of the processing, as the software is typically controlled by the service provider. Consequently, service providers face legal uncertainty.

**Corporate structure** – Another issue linked to the definition of data controller, is that different entities of a single company are considered as third parties towards each other. This is due to the fact that the current data protection rules do not take into account corporate group structures, as illustrated by Recital 19 of the Data Protection Directive. As a consequence, any exchange of data between such different entities requires its own legal basis, even when these entities would have their seat on the same address, or would be managed by the same persons. To the extent such different entities process personal data for the same purposes, this rule often creates substantial and unnecessary burdens for companies.

---

167 For example, when a user takes a picture of some friends during a party, uploads this picture to the social network and "tags" the picture to indicate who is being portrayed, the tagged information will be used by many social networks to enrich their search database and, thus, to allow third parties to easily retrieve many details on natural persons (even when they do not have an account on the social network). Arguably, such use of the picture data may lay outside the purpose for which the picture was initially taken.

168 While Working Party 29 points out that it does not consider images on the Internet to constitute sensitive data "in general", the barrier towards qualification as sensitive data is not very high, as illustrated by the Lindqvist case (C101-01).

169 “Whereas establishment on the territory of a Member State implies the effective and real exercise of activity through stable arrangements; whereas the legal form of such an establishment, whether simply branch or a subsidiary with a legal personality, is not the determining factor in this respect; whereas, when a single controller is established on the territory of several Member States, particularly by means of subsidiaries, he must ensure, in order to avoid any circumvention of national rules, that each of the establishments fulfils the obligations imposed by the national law applicable to its activities.”
4.7. Problematic scope of "sensitive data"

Article 8.1 of the Data Protection Directive\textsuperscript{170} introduces the principle that the processing of so-called sensitive personal data (i.e. data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health or sex life) shall be prohibited. Article 8.2 provides for specific derogations from this principle, relating to, for example, the vital interests of the data subjects and the explicit consent of the data subject. Member States are allowed to provide for additional derogations, for reasons of substantial public interest.

The concept of sensitive data was introduced because it was felt to be necessary to demarcate specific categories of sensitive data that would merit further protection, as they were likely to lead to encroachments on individual rights and interests\textsuperscript{171}. However, following the 2003 Lindqvist case\textsuperscript{172}, the definition of sensitive data is up for debate, particularly in an online context.

Transposition differences – Even more so than the concept of personal data in general, the interpretation as to which type of data should be considered sensitive is highly dependent on social, cultural and historical factors. For example, in today’s European society, it is questionable whether information on a person’s philosophical beliefs is still considered to be sensitive.

Within the EU, this is demonstrated by the different definitions of sensitive data adopted by the Member States\textsuperscript{173}. Also, some Member States define certain data as sensitive data which are not included in article 8(1) Data Protection Directive. For example, in Finland "special categories" include data on social affiliation, social welfare benefits and socially oriented actions targeted at a data subject (e.g., taking children into custody by social welfare authorities) as well as credit data regarding a person\textsuperscript{174}, while Greek data protection law also regards membership in any association and data on social welfare as sensitive\textsuperscript{175}. Similarly, data on trade-union membership is not considered to deserve special protection in Iceland, as trade-union membership is publicly known\textsuperscript{176}.

Implied sensitive data – The question also arises whether the current definition of sensitive data takes sufficient account of the implied sensitive nature of certain non-sensitive data. For example, names can reveal the ethnic origin and/or religion of an individual, culinary preferences (kosher, halal, vegetarian or vegan) can reveal religious or philosophical beliefs, photographs of people can reveal ethnic origin, the marital status about two persons can reveal data about their sexual preferences, and public library administration regarding book loans can reveal political, philosophical and health-related data of the readers.

In their proposals for amendment of the Data Protection Directive\textsuperscript{177}, Austria, Finland, Sweden and the UK argued that such “essentially incidental revelations” of characteristics as described in article 8(1)

\textsuperscript{170} The idea of sensitive data was also found in Convention n° 108 (article 4.1)
\textsuperscript{172} As described on p. 2
\textsuperscript{173} For an overview, see A. CAMMILLERI-SUBRENAT and C. LEVALLOIS-BARTH, Sensitive Data Protection in the European Union, Bruylant, Brussels, 2007, p. 27 et seq.
\textsuperscript{174} Section 20 of the Finnish Personal Data Act, unofficial translation available at www.tietosuoja.fi/uploads/hopxtvf.HTM
\textsuperscript{175} Technical analysis to the Commission’s First report on the implementation of the Data Protection Directive, o.c., p. 11
\textsuperscript{177} Proposals for amendment made by Austria, Finland, Sweden and the United Kingdom, Explanatory Note, September 2002, no. 6, available at www.dca.gov.uk/ccpd/dpdamend.htm
Data Protection Directive, do not amount to sensitive data for the purposes of that article. It is, however, not clear at all under the current data protection rules to which extent personal data should be contextualized\textsuperscript{178} so as to ensure that the processing thereof does not intend to circumvent the more stringent rules applicable to the processing of sensitive data.

**Excluded types of data** – Many types of data which most citizens would consider as sensitive, are not considered as "sensitive data" in the sense of the Data Protection Directive. Examples include financial data, personal solvency, salary data, social security numbers, genetic information and biometric information. One can even envisage indirect types of personal data, which only become sensitive when combined with other data. For example, unique identifiers used to link heterogeneous databases are not sensitive as such (they are mere numbers), but can become highly "sensitive" once they are used to effectively combine databases of genuine sensitive data. Meanwhile, the Data Protection Directive does not protect these types of data.

**Impact on the online context** – The processing of sensitive personal data in an online context is prohibited, unless either the explicit consent of the data subject concerned is obtained, or the data is manifestly made public by the data subject (other exceptions exist, but are not relevant for the typical online context\textsuperscript{179}). Accordingly, and taking into account the Lindqvist case law, the current data protection rules shall be breached in most typical cases when a personal blog mentions that a family member is allergic to house dust mite — or even mentions a friend’s or family member’s dietary preferences\textsuperscript{180}. The same applies to a newspaper who publishes pictures of the recent congress of a political party. Similarly, while a non-profit organisation could publish the annual salary and family fortune from all members of the national parliament without breaking data protection rules, the same organisation cannot publish the number of days each member was absent, as such could reveal health-related data.

**Evaluation** – The scope of the current concept of sensitive data is at the same time too large (including harmless data, such as the fact that someone has a cold), too narrow (not including delicate data such as financial details), too vague (are "implied" types of sensitive data covered?) and too diverse among Member States. The question arises whether the categories of data included in the definition of the Data Protection Directive should be reconsidered.

### 4.8. Legal uncertainty with respect to data retention terms

**Maximum terms for personal data** – Article 6.1.e of the Data Protection Directive provides that personal data may be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. This provision creates considerable uncertainty for companies, due to the vagueness of the criterion "no longer than is necessary". While this criterion can be used to obtain some guidance — for example, it is clear that it is exaggerated to use cookies with a lifetime of 30 years — the criterion lacks refinement for more granular questions.

Although national data protection authorities have provided some guidelines with respect to certain types of data, the divergences between the Member States demonstrate the difficulty to apply article 6.1.e. For example:

\textsuperscript{178} See S. SIMITIS, Revisiting sensitive data, 1999

\textsuperscript{179} For example, health-related data can be processed for the purposes of preventive medicine, medical diagnosis or treatment, provided the data is processed by a health professional. A service where a medically trained professional would offer personalised medical advice online, would therefore qualify as a sound example where one of the exceptions applies.

\textsuperscript{180} when implied sensitive data is also considered as personal data
The following specific time limits are applied for sound and image data: Belgium: images recorded in public places (one day); Denmark: general surveillance data, e.g. in supermarkets (30 days); France: surveillance data of public places (one month), processing of information concerning number plates on cars by customs officials (four or, exceptionally, 24 hours); Greece: CCTV data (15 days, prolongation possible in exceptional cases and upon permission of the data protection authority); Italy: access control (one week); Portugal: CCTV data (30 days); Spain: CCTV data (30 days); Sweden: CCTV data (30 days); United Kingdom: CCTV data in pubs (7 days), CCTV data in public places (31 days), cash machines (three months)\(^{181}\).

The maximum lifetime of search log files has been publicly debated in 2007 between Working Party 29, Google and several other search engines\(^{182}\). Google argued that it was necessary to store log files for a period of 18-24 months\(^{183}\) for reasons of security and service improvement, prevention of "click fraud" and fighting webspam, while 6 months was the maximum period generally recommended by Working Party 29. As for cookies, the Working Party did not even specify a maximum period, and instead referred to the "necessity" criterion.

**Minimum term for "processing data"** – The ECJ recently issued a preliminary ruling on the existence of a link between this article 6 and the right of access. More specifically, the ECJ examined whether the right of access to information on the recipients and on the content of the personal data disclosed to such recipients ("processing data") could depend on the length of time for which those personal data are stored\(^{184}\).

The ECJ ruled that the right of access must necessarily also apply to the past, so as to ensure the effectiveness of the right to rectification, the right to object and the right to judicial recourse. It is up to the Member States to decide the length of time during which data controllers must store such processing data, and during which data subjects must be able to exercise their right of access.

When deciding upon this term, Member States must try to achieve a balance between the interest of the data subject as regards his privacy on the one hand, and the burden imposed on the controller to store these processing data on the other hand. One of the relevant parameters in this respect, is the term during which the data controller stores the personal data pursuant to article 6.

The ECJ further confirmed that the information duty of data controllers as set out in articles 10 and 11, which includes an obligation to inform the data subject of the recipients of his personal data, does not imply that a right of access to processing data for the past, is redundant.

### 4.9. Legal uncertainty regarding profiling

**Is profiling data "personal data" and does the act of profiling qualify as processing?** – In its opinion on the concept of personal data, Working Party 29 has clarified that data are also considered to "relate" to an individual (and can thus qualify as personal data) if they are likely to be used to evaluate, etc.

\(^{181}\) Technical analysis to the Commission’s First report on the implementation of the Data Protection Directive, o.c., p.63-64


\(^{183}\) Google eventually reduced the retention term to 9 months and Yahoo to 3 months. Microsoft indicated to be willing to reduce the retention term to 6 months, but only when the other search engines would do the same (see [http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/others/2009_10_23_letter_wp_microsoft.pdf](http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/others/2009_10_23_letter_wp_microsoft.pdf)).

\(^{184}\) ECJ 7 May 2009, Rijkeboer, C-553/07
treat in a certain way or influence the status or behaviour of an individual. Taking into account the purpose of profiling activities, profiling data therefore qualifies as personal data under the current EU data protection rules according to the opinion of Working Party 29. This aligns with the position of the Council of Europe.

However, the question arises whether such interpretation does not extend the scope of personal data too widely. While it is not contested that some profiling data qualifies without any doubt as “personal data” because it can be linked to natural persons, it is questionable whether this should also be the case for data that cannot be linked to a natural person (so-called “abstract profiles”).

For example, through the use of web cookies, marketing companies may be able to gather interesting information about individuals that surf the web. When such companies would gather significant amounts of data about each person (the websites he visits, the date / time / duration of each visit, his geographical location, his operating system and browser, his browser settings, ...), they can build up interesting profiles of each visitor. However, as long as this company gets no direct hooks that would allow it to identify the natural person associated with a profile, is it really necessary to apply all safeguards and compliance measures that are associated with the qualification as personal data?

Processing profile data — In addition to the question of whether profiling data should qualify as personal data, the issue arises as to whether the act of profiling should be subject to specific data protection rules.

The Data Protection Directive does not provide general rules with respect to profile generation. However, despite the lack of general rules regarding profiling, there is one article (15.1) which deals with a particular type of profiling, although it does not directly restrict the creation of profiles. As will be discussed below, it is rather vague whether article 15.1 applies to profiling data, and it may not always be adequate in dealing with all issues and difficulties raised by profiling activities.

Article 15.1 holds that every person has the right not to be subject to a decision which produces legal effects concerning him (or significantly affects him) and which is based solely on the automated processing of data intended to evaluate certain personal aspects relating to him (such as his performance at work, creditworthiness, reliability, conduct, etc.).

With respect to the element "decision", the question arises whether a human decision maker must be involved in the decision making, or whether an action of computer software (e.g., an intelligent agent) in response to certain data input can also be considered a decision.

For example, is the decision to display an advertisement X to one person A, and advertisement Y to person B, a “decision” in the sense of article 15?

With respect to the second element (legal effects / significant effects), it is unclear whether the "significant effects" should be interpreted objectively or subjectively, which type of effects are envisaged (material and/or immaterial) and whether the effects must be of an adverse nature or not.

185 Opinion 136, p. 11
188 This section provides a summary of the detailed analysis made by L. BYGRAVE, o.c.
For example, is the decision to allow certain profiles (such as male website visitors between the age of 18-24) to make use of an enhanced version of a particular online service, a decision with significant effects?

The fourth condition seems to imply that article 15.1 applies not only to personal profiles (relating to one specific individual), but also to abstract profiles, as article 15.1 refers to "data" and not "personal data".

Article 15.2 introduces the exception that automated decisions can be taken when this decision is taken in the course of entering into or executing a contract. Problematic in this respect is the underlying assumption that that fulfillment of a data subject's request for entering into or executing a contract will never be problematic.

For example, a decision taken on the basis of automatic processing in the context of a credit loan application, may not always be the best decision from the point of view of the person involved, even if such person is eventually granted the loan. Should the decision not have been taken based on the data processed, such person may have been granted a loan at better conditions.

4.10. Difficulties with respect to the legal grounds for processing

Article 7 of the Data Protection Directive provides for a limited set of legal grounds for processing personal data. In a general e-business context, the unambiguous consent of the data subject, the necessity to execute a contract, and the compliance with a legal obligation to which a data controller is subject, are the most important legal grounds. However, the "consent" and "legal obligation" grounds cause considerable legal difficulties when applied to today's online context. Furthermore, the legal ground which allows the processing of sensitive data based on the fact that the data subject made those data publicly available creates additional interpretation difficulties.

Consent – Article 2.h of the Data Protection Directive provides that the consent of a data subject requires a "freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed". Although the consent of the data subject is arguably the most commonly used legal ground to justify processing in a typical e-business context, it is also the legal ground which is most commonly infringed, despite the seemingly formal compliance achieved by the service provider.

Indeed, although "Yes, I accept" checkboxes have become a de facto standard for online service providers to obtain the consent of a customer to process their personal data, it is highly questionable to which extent this acceptance is the informed indication of the data subject's wish that his data would be processed by the service provider. This questionability is mainly caused by insufficient privacy policies, as further described in section 6.1 on page 41.

Legal obligation of the controller – National laws often provide numerous obligations for data controllers to provide certain information (including personal data), to third parties. However, not all such obligations are automatically considered "legal obligations" within the meaning of the Data Protection Directive. Specifically, article 7.c does not apply to legal obligations provided by non-EC laws, as these are not bound to the principle of proportionality. However, if a special agreement is

---

189 which are often being public authorities


191 Ibid.
concluded between the European Community and a third country for such purposes, legal obligations imposed by third countries may be accepted as a legal basis for the disclosure of personal data\(^\text{192}\).

This creates considerable uncertainty for data controllers, since a situation could arise where they are subject to a legal obligation to disclose personal data on the one hand, and subject to a legal obligation which prohibits them to disclose such personal data, on the other hand. In such case, every decision they make will imply a breach of law\(^\text{193}\).

**Public data** – Article 8.2.e provides that sensitive data may be processed if the processing relates to data which are manifestly made public by the data subject. In such case, the controller is not required to obtain the data subject's consent, nor to ensure that any other legal basis for processing is available.

Article 7 on the other hand, which contains the legal grounds for processing personal data in general, does not provide a similar legal ground for processing. Hence, sensitive data, which require additional protection due to their sensitive nature, may be processed when made publicly available by the data subject, whereas "regular" personal data may not be processed solely on the basis that those data were made available by the data subject. In this respect, the Data Protection Directive seems to be inconsistent.

In addition, it is not clear in which cases personal data must be considered as "made manifestly public by the data subject".

> For example, it remains vague whether a statement on a social network profile to which access is limited to all members of the network must be considered as information that has been manifestly made public.

Finally, a literal interpretation of article 8.2.e seems to allow unlimited harvesting activities. Article 6.1.b of the Data Protection Directive provides that personal data may not be processed in a way that is incompatible with the purposes for which the data were collected. The processing possibilities thus relate to the purpose of *collection*, rather than the purpose for which the data subject *provided* the information. Accordingly, it could be argued that any personal data made public by a data subject, may be used for any purposes a controller sees fit\(^\text{194}\).

## 5. Policy shortcomings

### 5.1. Lack of enforcement

Several national data protection authorities make effective use of their possibilities to enforce data protection legislation. For example, the data protection authority of the German federal state of Schleswig-Holstein ordered the global subsidiaries of a multinational to delete personal data of a former German employee\(^\text{195}\). With respect to audit and inspection competences, some data protection authorities...

---


\(^{193}\) See, for example, the opinion of Working Party 29 on legal discovery procedures in US procedural law

\(^{194}\) Provided of course that such purposes comply with the requirements set out in article 6.1.b of the Data Protection Directive

\(^{195}\) C. KUNER, *o.c.*, p. 51
authorities annually perform hundreds of audits\textsuperscript{196}. The Dutch, French and Spanish data protection authorities have already imposed severe fines for illegitimate processing of personal data\textsuperscript{197}.

However, in other Member States, the enforcement of data protection legislation seems to be less effective, due to a lack of appropriate enforcement legislation, often combined with a lack of resources, a lack of personnel, ineffective measures to enforce data protection compliance, as well as their focus on a wide range of tasks (among which enforcement actions have a rather low priority). This under-resourced enforcement effort of supervisory authorities was already reported by the Commission in its first report on the Data Protection Directive\textsuperscript{198}.

5.2. Implementation differences between Member States

It has already been reported that there are important transposition differences between Member States, despite the harmonising goals of the Data Protection Directive\textsuperscript{199}. Examples include articles 4 (applicable law), 7 (grounds for legitimate processing), 8.1 (sensitive data), 10 (information to data subjects), 13 (exceptions) and 26 (exceptions as regards transfers to third countries).

For example, several Member States limit the access rights of data subjects as they allow a limitation of requests per year and allow the payment of a fee for access. E.g., in the UK, controllers may charge a fee up to £10 for access to each entry, and in Finland, controllers may charge their costs in accessing the data and data subjects may only submit one request per year\textsuperscript{200}.

6. Shortcomings caused by data controllers

6.1. Mere formal compliance with transparency requirements

Introduction – Pursuant to article 10 of the Data Protection Directive, data controllers are required to inform data subjects about various aspects of the processing of their personal data, such as the identity of the controller, the purpose(s) of the processing, the (categories of) recipients, the obligatory or voluntary nature of questions, and the existence of a right of access and rectification.

In practice, most data controllers try to meet this legal requirement by publishing a so-called “privacy policy” on their website. This privacy policy typically serves a dual function, as it is also used by data controllers during the process of obtaining the data subject’s consent with the data processing that will take place\textsuperscript{201}. Pursuant to article 2.h of the Data Protection Directive, the customer’s consent then constitutes a legal ground for the lawful processing of personal data.

Shortcomings of most privacy policies – Although privacy policies are the \textit{de facto} standard to meet the Data Protection Directive’s transparency requirements and obtain a lawful ground for processing, a substantial number of privacy policies actually fail to meet their goals, for the following reasons:

\textsuperscript{196} Ibid, p. 52
\textsuperscript{197} Ibid, p. 52 and 56
\textsuperscript{198} First report of the Commission, p. 12
\textsuperscript{199} “(...) the divergences that still mark the data protection legislation of the Member States are too great”: First Report of the Commission, p. 11
\textsuperscript{200} C. KUNER, o.c., p. 64
\textsuperscript{201} See section 39 on p. 39
- **Length** – Privacy policies are often too long, which detracts data subjects from actually consulting the policies. The length of these texts is frequently caused by superfluous paragraphs.\(^{202}\)

- **Legalese** – Privacy policies are often written by lawyers, which results in documents that reflect a contractual style, containing formal and technical wording, which makes them difficult to understand.

- **Vagueness and obscurity** – Privacy policies tend to be particularly vague in areas where a clear explanation matters the most\(^{203}\). Even worse, some privacy policies deliberately try to obscure reality.\(^{204}\)

- **Boiler plate** – Privacy policies are frequently copied and pasted from other policies, without paying regard to the actual content of the document. Accordingly, many privacy policies are not adapted to the specific content or workflow of a certain website.

- **Not adequately updated** – Finally, it often arises that privacy policies are never updated once they are published, even though the content and the nature of the website evolves. This should not come as a surprise, as privacy policies are regarded by many website operators as a pure formality, for which the drafting is outsourced once to an external lawyer, or copied from another example.

**Evaluation** – In the current state of affairs, it is our opinion that most website operators consider privacy policies to be a mere compliance burden, on which only a minimum effort should be spent. As a result, it is highly questionable whether privacy policies are actually read by visitors of the website. Users are thus signing up to services for which they do not know how their personal data will be handled.

An interesting illustration is the recent update to the Facebook privacy policy, which was implemented after a complaint from the Canadian privacy regulator, which found that the previous policy was "confusing and incomplete."\(^{205}\)

Anecdotal evidence indeed suggests that "there is plenty of evidence to suggest that no one—whether native to digital life or not—reads privacy policies or does much to adjust the default settings for online services. (...) Even the most sophisticated young people made clear that they almost never read these policies or compared the privacy policies among services."\(^{206}\) Consequently, it is doubtful whether the Data Protection Directive's transparency requirements are actually met by most of today’s privacy policies.

**P3P** – The Platform for Privacy Preferences Project (P3P) is a technical protocol that allows websites to formally publish how they use personal data from the visitor. Internet browsers can then convey this information in a user-friendly way, and even to make automated decisions, based on these practices.

---

\(^{202}\) For example, paragraphs that describe security measures in a superficial and generic way ("we protect your data by maintaining physical, electronic and procedural safeguards", or "we will implement appropriate controls to monitor and assure compliance with this privacy policy"), paragraphs that want to clarify that the privacy policy does not apply to other website ("This site may contain links or references to other Web sites to which this Privacy Policy does not apply. We encourage you to read the privacy policy of every Web site you visit.") or paragraphs that explain highly obvious matters ("We only collect personally identifiable information about you (such as your name, address, telephone number, fax number, or e-mail address) when fill out a contact form.")

\(^{203}\) For example, the important topic of whether data is shared with third parties, is often concisely handled by stating that "We only share your personal data with our partners".

\(^{204}\) For example, a statement such as "We provide your personal data to our trusted partners, which may use your personal information to help us communicate with you about offers from us and our marketing partners." really tries to say that personal data is sold or rented to other companies, which can use it for direct marketing purposes.

\(^{205}\) See [www.guardian.co.uk/media/pda/2009/oct/30/facebook-privacy-policy](http://www.guardian.co.uk/media/pda/2009/oct/30/facebook-privacy-policy)

when appropriate. For example, a user could configure his browser to automatically disable cookies from certain websites that are not in line with his privacy desires. As a result, users need not read the privacy policies at every site they visit.

Although the philosophy behind the P3P project would solve most of the shortcomings of today's privacy policies, the project is suspended due to insufficient support from current browsers\(^{207}\). The reasons for this failure can be attributed to the complexity of the user interface, the false sense of security given to novice users that browse websites that are approved by P3P\(^{208}\), and perhaps also a lack of consumer interest in privacy protection. Finally, the project is criticised for lacking legal enforcement towards companies that do not comply with their own privacy policies. However, this lack of real enforcement is a general issue\(^{209}\) that is not restricted to the P3P project.

6.2. Privacy and data protection as an afterthought

**Design of software and systems** – Software, online services and computer systems are not typically designed with privacy or data protection in mind. Instead, most software and online services are designed for data maximisation, whereby privacy and data protection features are only included when such is required for compliance reasons, or when users specifically request such features.

This is illustrated by the following examples:

- **Web servers** such as the popular "open source" Apache automatically log various kinds of traffic data, without the website administrator being required to configure any setting\(^{210}\).

- When Apple Inc. introduced a new version of its popular "iTunes" music software, the "MiniStore" feature — which provides links to other interesting music by sending information about a song selected in a user's personal playlist back to Apple — was automatically enabled, without users being informed about the new feature sending the information back to Apple\(^{211}\). In response to protest from users, the software now explicitly asks the user whether it is allowed to send information back to Apple.

- By default, a Facebook profile is set to allow only self-selected friends to be able to view the profile. However, the default search visibility settings allow everyone to see a user's profile picture, friend list and fan pages. Moreover, a public search listing is automatically created and submitted for search engine indexing. Users thus automatically reveal their personal data when they do not alter the default settings of their profile.

**Management** – Also at other layers of the corporate structure (marketing departments, managers and executive officers), there seems to be an ongoing lack of privacy and data protection awareness among data controllers. For many organisations, data protection is a compliance-driven process, which often

\(^{207}\) See the P3P website (www.w3.org/P3P/)


\(^{209}\) See section 4.5 on p. 40


results in a "tick the box" approach to data protection management. Consequently, companies often fail to consider privacy and data protection in a broader context.  

7. Comparisons

7.1. Comparison with the US

This section provides a high-level overview of how the United States deal with online privacy and data protection.

7.1.1. Overview

"...there are, on the two sides of the Atlantic, two different cultures of privacy, which are home to different intuitive sensibilities, and which have produced two significantly different laws of privacy..."

Introduction – The legal framework for the protection of privacy and personal data in the US is vastly different from the EU legal framework, partially due to a different approach to the concept of privacy. Although this complicates a comparison between both legal frameworks, it can be useful to examine the US approach to privacy and personal data protection.

Contrary to the EU, where privacy is considered to be a fundamental human right, US privacy law is the right to freedom from intrusions by the government, especially in one's own home. While many Americans citizens also consider privacy to be some kind of right, it is only considered to be "fundamental" (constitutional) when a citizen's personal data is threatened by governmental abuse. Although privacy is not mentioned as such in the US Constitution, there are several "zones of privacy" in the US Constitution according to the Supreme Court. Americans therefore view privacy protection as an individual interest, which needs to be balanced with the interests of business and society as a whole. As a result, American privacy legislation tends to be limited to situations where certain sectors of business have the potential to abuse privacy, or when businesses hold sensitive personal data.

Piecemeal approach – Compared to the EU, US privacy laws are far more limited in scope:

The EU Data Protection Directive constitutes a comprehensive legislative framework, that spans across alls industry sectors, and applies to both authorities and private parties. Conversely, the US upholds a sector-based approach, which relies on a mix of legislation, regulation and self-regulation. (It should be noted, however, that various efforts have already been undertaken to introduce comprehensive data protection legislation in the US.)

---

212 Information Commissioner’s Office (ICO), Privacy by design, p. 3 and 6, available at www.privacygroup.org/downloads/f00000228.pdf
214 D. SOLOVE, M. ROTENBERG and P. SCHWARTZ, o.c., p. 876
215 Case Griswold v. Connecticut, 1965
Deeply rooted in the Data Protection Directive is the concept of "personal data", which encompasses any type of information that can somehow be linked to a natural person\textsuperscript{217}. Conversely, US privacy laws rely on the concept of "personally identifiable information" (PII), which requires information to be specifically associated with an individual person.

\begin{quote}
For example, under the 1998 Children’s Online Privacy Protection Act, only the following information is covered: first name (or initial) and last name; home address; e-mail address or screen name revealing an e-mail address; Social Security Number; telephone number; as well as any information about a child's age, gender, hobbies, preferences, etc., (provided it is associated with identifying information).
\end{quote}

7.1.2. Legislation

This section 7.1.2 provides an overview of the various US laws that deals with privacy protection. As will be seen below, most of these laws mainly urge companies to adopt and publish privacy policies on their websites.

**Federal Trade Commission Act (1914)** – The abuse of personal information can constitute an "unfair and deceptive practice", which can be sanctioned by the Federal Trade Commission with cease and desist orders\textsuperscript{218}. According to the case law issued pursuant to the Federal Trade Commission Act, companies must adopt privacy policies for Internet sites and applications\textsuperscript{219}.

**California Online Privacy Protection Act (2003)** – This law requires companies to publish a privacy policy on any website that collects personally identifiable information about any Californian citizen.

**Anti-spyware laws (2004)** – California and Utah have passed anti-spyware laws, which make it illegal to provide software that surreptitiously installs software, modifies settings, disables protection, or collects information.

**Children’s Online Privacy Protection Act (1998)** – This law affects any business that deals with consumers and gathers personal information from anyone (not only children) through the Internet. Websites that are subject to this law, must publish a privacy policy, which must include a section that deals specifically with information practices towards children.

**Gramm-Leach-Bliley Act (1999)** – This law deals with financial privacy, and applies to any financial institution. Financial institutions must provide an initial notice to consumers about their privacy policies, and must provide annual notices of their privacy policies to their customers, as well as the possibility to opt out of certain disclosures.

**Health Insurance Portability & Accountability Act (1996)** – This law requires patient consent before information is released, even for routine uses such as insurance approval. Patients must be able to see and get copies of their records, and request amendments. Furthermore, medical organisations must adopt written privacy procedures.

**Data breach notifications** – California was the first US state to adopt a law that requires data controllers that suffer data breaches to notify the affected data subjects. Following the Californian example, most other US states have adopted similar data breach notification laws. In light of the variation in state laws, a number of bills have been filed in the federal parliament, to pass federal data breach legislation.

\textsuperscript{217} See section 4.1 for an elaborate discussion

\textsuperscript{218} In addition to the federal Act, most US states have also adopted similar consumer protection laws.

7.1.3. **Self regulation**

Based on the idea of minimum state intervention, the US data protection framework is, to a large extent, created by information practices established through industry self-regulation.\(^{220}\)

In its 1998 report "Privacy Online"\(^{221}\), the US Federal State Commission described five core principles of privacy protection, common to a diverse range of EU and US documents on privacy. The principles identified are: notice/awareness, choice/consent, access/participation, integrity/security (and enforcement/redress). Two years later\(^{222}\), the US Federal State Commission reported that only 20% of the busiest sites on the World Wide Web implement to some extent all four fair information practices in their privacy disclosures\(^{223}\). The Commission therefore concluded that "such [self-regulatory] efforts alone cannot ensure that the online marketplace as a whole will emulate the standards adopted by industry leaders. While there will continue to be a major role for industry self-regulation in the future, the Commission recommends that Congress enact legislation that, in conjunction with continuing self-regulatory programs, will ensure adequate protection of consumer privacy online."\(^{224}\)

7.2. **Comparison with Japan**

7.2.1. **Overview**

In 2003, Japan enacted the Act on the Protection of Personal Information (Act. No. 57 of 2003)\(^{225}\). Similar to the Data Protection Directive, the Japanese Act is inspired by the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. The general principles of the Japanese Act are aligned with the principles of the Data Protection Directive. To a limited extent, the Japanese Act also shows influences of the US approach, especially as regards the lack of a single responsible government entity and the sector-based approach\(^{226}\).

7.2.2. **Basic concepts**

**Personal information and data** – The Act distinguishes between "personal information" and "personal data". Personal information is defined as information about a living individual which can identify the specific individual by name, date of birth, or other description contained in such information (including such information as will allow easy reference to other information and will thereby enable the identification of the specific individual). Personal data is personal information which is stored on a personal information database. The criterion of the personal information database is similar to the concept of personal data filing systems in the Data Protection Directive. Whereas all the provisions of the

---

\(^{220}\) J. DUMORTIER and C. GOEMANS, "Online data Privacy and Standardization: Towards a More Effective Protection?", in *A Decade of Research @ the Crossroads of Law and ICT*, Larcier, Brussels, 2001, p. 57

\(^{221}\) Available at www.ftc.gov/reports/privacy3/ftc.shtm

\(^{222}\) Available at www.ftc.gov/reports/privacy2000/privacy2000text.pdf


\(^{224}\) *Ibid.*, p. ii

\(^{225}\) Unofficial English translation available at www.japaneselawtranslation.go.jp

\(^{226}\) More than 35 sets of guidelines have already been issued by responsible ministries, across 24 industry sectors. These guidelines are not legally binding as such, but do indicate the manner in which the ministries will interpret the Act, and should therefore be complied with O. ITO and N. PARKER, "Data protection law in Japan: a European perspective", *World Data Protection Report* 2008/12, p. 3-4
Act apply to personal data, personal information which is not stored in a database, is not always subject to the Act.

Whereas some ministerial guidelines contain special rules applicable to certain types of sensitive personal information, the Japanese Act does not recognise special categories of personal data in a general manner.

**Personal information handler** – A personal information handler is defined as a person or entity that uses a personal information database for its business activities. Contrary to EU data protection law, Japanese law does not distinguish between "controllers" and "processors", depending on the extent to which one is involved in determining the purposes and means of processing. The mere use of personal information databases suffices to be considered as a personal information handler and implies the obligation to comply with the Act.

Furthermore, the Enforcement Regulations of the Act (Cabinet Order No. 507 of 2003) contain a remarkable scope exemption. Article 2 provides that personal information handlers of which the personal information database they use for their business activities has not held personal information with respect to more than 5000 individuals at any time during the previous six months, is exempted from the obligations imposed on personal information handlers. Accordingly, small and medium-sized companies are often excluded from the scope of the Japanese Act.

**Geographical applicability** – The Japanese Act does not contain any specific provisions relating to the geographical scope of its applicability. It is, however, generally accepted that the Act only applies to companies (Japanese or foreign) which handle a personal information database in Japan.

### 7.2.3. Personal information handler’s obligations

**Collection, maintenance and retention** – Business operators may not acquire personal information by deception or other wrongful means. They must endeavour to maintain personal data accurate and up to date. Contrary to EU law, Japanese law does not require personal data to be adequate, relevant and not excessive, nor does it require that personal data is not kept for longer than necessary.

**Use of personal data** – Personal data may not be used beyond the scope necessary for achieving the purpose of use, without obtaining the prior consent of the persons concerned. However, Japanese law leaves room for processing data for additional purposes.

**Information obligations** – The personal information handler must promptly notify the data subjects of the purpose of use upon acquiring personal information. This purpose of use may also be announced publicly, either before or promptly after the acquiring. Japanese law further specifies that the personal

---


228 O. ITO and N. PARKER, o.c., p. 5

229 Article 17 Japanese data protection act

230 Article 19 Japanese data protection act

231 O. ITO and N. PARKER, o.c., p. 7

232 Article 16.1 Japanese data protection act

233 Article 18.1 Japanese data protection act
information handler must specify the purpose of use as much as possible\textsuperscript{234}. It is therefore not allowed to merely provide a vague or generic description\textsuperscript{235}.

In general, personal information handlers must make the following information accessible to persons involved: name of the information handler, purpose for which the data are held and the procedures to be followed in order to request the correction or deletion of information, or the suspension of use thereof\textsuperscript{236}.

**Data subject rights** – In addition to the right to being informed as described above, data subjects have the right to request correction, deletion or suspension of any retained personal data. They may also request the suspension of the use, or the suspension of the provision to a third party of personal data. This right to request correction, deletion or suspension applies in case the personal data is not accurate, is being used outside the purpose of use, was obtained wrongfully, or is being provided to third parties unlawfully\textsuperscript{237}.

Personal information handlers also have an obligation to endeavour to appropriately and promptly process any complaints about the handling of personal information\textsuperscript{238}.

**Security, protection and supervision** – Personal information handlers must endeavour to maintain personal data accurate and up to date, within the scope necessary for the purpose of processing\textsuperscript{239}. They must also supervise any employees or subcontractors to which they entrust the handling of personal information, to ensure the security control of the entrusted personal data\textsuperscript{240}. Personal information handlers must take the necessary and proper measures for preventing leakage, loss or damage, and for other security control of the personal data.

**No notification obligation** – As already indicated, Japan does not have a single authority responsible for personal data processing. Furthermore, business operators which process personal data and are subject to Japanese law, do not have any obligation to notify or register their activities\textsuperscript{241}. Accordingly, the administrative burden for personal information handlers subject to Japanese law, is smaller compared to the administrative obligations for data controllers subject to EU law.

### 7.2.4. Data transfers

**Consent required** – Article 23 of the Japanese Act provides that a business operator handling personal information must obtain a person’s consent prior to providing his personal data to a third party. As under EU law, affiliates and group entities must be considered as third parties if they are legally separate entities\textsuperscript{242}.

**Third parties** – Similar to EU law, Japanese law provides that affiliates and group entities must be considered as third parties, if they are legally separate entities\textsuperscript{243}. However, in the following cases, the

---

\textsuperscript{234} Article 15 Japanese data protection act  
\textsuperscript{235} See also O. ITO and N. PARKER, o.c., p. 6  
\textsuperscript{236} Article 24 Japanese data protection act  
\textsuperscript{237} Articles 25-30 Japanese data protection act, and O. ITO and N. PARKER, o.c., p. 7  
\textsuperscript{238} Article 31 Japanese data protection act  
\textsuperscript{239} Article 19 Japanese data protection act  
\textsuperscript{240} Articles 21 and 22 Japanese data protection act  
\textsuperscript{241} O. ITO and N. PARKER, o.c., p. 6  
\textsuperscript{242} Ibid., p. 7  
\textsuperscript{243} Ibid.
party receiving the personal data shall not be deemed a third party for the purpose of applying the data transfer rules:

- in case the business operator transfers the personal data to an entity entrusted with the handling of such data, within the scope necessary for achieving the purpose (similar to "processors" under EU law);
- in case of succession of business in a merger or otherwise; and
- in case separate individuals or entities jointly use personal data, and the persons concerned are notified in advance of, or have access to information with respect to the personal data being used, the scope of the use, the purpose of use and the name of the individual or business operator responsible for the management of the personal data.

**General exceptions** – The Act further provides a number of general exceptions in which the consent is not required. These exceptions relate to transfers based on laws and regulations, public policy issues such as health and the sound growth of children, and to the protection of life, body or property.

**Opt-out exception** – Article 23.2 provides that, if it is known at the moment of collecting the personal information, a business operator must not obtain consent if the persons concerned are provided with a possibility to "opt out". In such cases, the business operator must notify the persons involved of, or make available in a readily accessible form, the following information: the fact that and which personal data will be transferred to third parties, the means or method of provision to the third party; the fact that the provision of personal data will be stopped upon request.

**Transfer outside Japan** – Contrary to EU law, Japanese law does not contain any provisions specifically relating to transfers outside Japan. To the extent a transfer outside Japan implies a provision of personal data to third parties, the rules as described above will apply.

### 7.2.5. Evaluation

A comparison with Japan indicates that, while many core data protection rules are similar to the EU, there are several interesting aspects in Japanese law that provide for more flexibility and less compliance overhead for data controllers. In particular, the central definition of "personal information" seems to avoid an overly broad scope of the data protection rules. Also, the third country transfer prohibition – a major compliance issue under EU law – is notably absent. These aspects can put the EU rules in a different perspective.

### 8. Conclusions

1. Today's **social and technological context is vastly different** from the context at the time the Data Protection Directive was adopted. Especially the advent of the Internet has substantially changed the scale and manner of personal data processing. The emergence of Web 2.0 applications and services (including social networks, user generated content, cloud computing, and mashups), new profiling and data harvesting business models, the semantic web and ubiquitous computing all raise the question of whether the current data protection rules are still adequate.

---

244 Article 23.4 Japanese Data protection act
245 *ibid.*, p. 8
2. In this changed context, the **scope of the Data Protection Directive is too wide**, mainly due to the very wide interpretation of the concept "personal data". The scope of this concept is severely stretched, particularly as regards the reference to indirect identification. In addition, the concept "processing" is defined very broadly and has been interpreted by the European Court of Justice in such a way that almost any operation with respect to personal data – particularly in an online context – will constitute processing.

3. Furthermore, the **rules regarding applicable national law create uncertainty and are far-reaching**, due to diverging Member State implementations and an extensive interpretation of the criteria "establishment" and "use of equipment". The concept "use of equipment" is interpreted in such a way that EU law often even applies beyond the territorial boundaries of the Member States.

4. As regards the new and emerging technologies, the assumption no longer holds true that the processing of personal data can be limited to certain physical and geographical boundaries. Nonetheless, EU law imposes **rigid obligations for data transfers** outside the EU. Particularly in complex situations with multiple parties or with multiple countries involved, the possibility to transfer personal data outside the EU may be severely impeded.

5. In addition, the Data Protection Directive imposes other **onerous obligations on data controllers** as regards the notification of their activities to the authorities. With respect to this notification obligation, the often excessive administrative requirements not only represent a burden for business, but even undermine the whole rationale of notification by becoming an excessive burden for the data protection authorities. Other **data controller obligations remain too vague**. For example, the obligation regarding the retention term of personal data creates uncertainty due to the vagueness of the criterion "no longer than is necessary".

6. Moreover, it is not always clear whether a person or company must comply with these data controller obligations, as the **distinction between controllers and processor is no longer apt** to deal with today’s more complex situations. This is particularly problematic when there are several parties involved that partially define either the means or the purpose of the processing.

7. Other **problematic data concepts** include sensitive data and profiling data. The scope of the current concept of sensitive data is at the same time too large, too narrow, too vague and too diverse among Member States. As regards profiling data, it is not clear whether these data constitute personal data, nor whether the processing of profiling data is subject to specific rules.

8. The limited set of **legal grounds for processing personal data cause considerable difficulties** when applied to today’s online context. Although the consent of the data subject is the most commonly used legal ground in a typical e-business context, it is also the legal ground which is most commonly infringed. By limiting the legal obligation ground to EU law obligations, data controllers may find themselves in a situation where it is impossible to comply with both EU law and applicable foreign laws.

9. In addition to the issues created by the legal framework, **additional shortcomings are caused by both Member States and data controllers**. Member States interpret the Data Protection Directive differently, which creates legal uncertainty for data controllers. Some Member States also fail to enforce data protection legislation effectively. Data controllers on the other hand often limit themselves to mere formal compliance with their obligations, without fully implementing data protection requirements in their systems and services.
9. Recommendations

In this section 9, we provide a list of recommendations to resolve the various issues identified in this chapter. A distinction is made between recommendations that can be implemented on the short term (2010-2015), the mid-term (2015-2020) and the long term (2020 and beyond). These time frames align with the relative political and legal difficulty to implement these recommendations, as well as the urgency involved. Hence, the threshold for implementing recommendations for the short term is relatively low, or the urgency involved is rather high. Conversely, recommendations for the mid-term require important legal modifications, or may receive more political resistance. Recommendations for the long term are of a more visionary nature.

Please note that – as is also the case for all other chapters – all of these recommendations present the views of the authors. These recommendations do not represent the view of the European Commission.

9.1. Guiding principles for each recommendation

In formulating the detailed recommendations below, we have adhered to the following general recommendations. These general recommendations are based on the above analysis of the pitfalls and shortcomings of the current legal framework.

Amendment of the Data Protection Directive – The Commission decided in 2003 against an amendment of the Data Protection Directive, mainly because experience with the Directive was very limited at that time, and some difficulties were thought to be able to be resolved without amending the Directive (e.g., by modifying national law or encouraging closer co-operation between supervisory authorities)\(^\text{246}\). In our opinion, however, the time has now come to effectively amend the Directive, at least with regard to data processing in an online context\(^\text{247}\), taking into account the following general recommendations set out below.

Back to the core principles of the Data Protection Directive – It is increasingly claimed that the old privacy and data protection paradigms are no longer relevant in today’s networked society: commentators argue that things have already progressed too far for law to intervene. This results in claims such as "you already have zero privacy - get over it"\(^\text{248}\), "privacy is dead", and "the meaning of ‘public’ and ‘private’ is shifting"\(^\text{249}\).

We are convinced, however, that the core principles of the Data Protection Directive should remain in the years to come: in our opinion, it is not necessary to reinvent the wheel, nor to cut back on the high level of data protection in the EU\(^\text{250}\). However, the administrative overhead and extensive interpretations of the

\(^{246}\) First report of the Commission, p. 7

\(^{247}\) This opinion is shared by the recent 2009 study undertaken by Rand Europe for the UK’s Information Commissioner’s Office (ICO), available at www.rand.org/pubs/working_papers/WR607: (p. vii) "Overall, we found that as we move toward a globally networked society, the Directive as it stands will not suffice in the long term. While the widely applauded principles of the Directive will remain as a useful front-end, they will need to be supported by a harms-based back-end in order to cope with the growing challenge of globalisation and international data flows."

\(^{248}\) Statement by Scott McNealy, former CEO of Sun Microsystems, 1999

\(^{249}\) J. PALFREY and U. GASSER, o.c., p. 58

\(^{250}\) Similarly, the Rand study recommends "Abandoning the Directive as it currently stands is widely (although not unanimously) seen as the worst option, as it has served, and continues to serve, as a stimulus to taking data protection seriously." because "A lot can be achieved by better implementation of the current rules, for instance by establishing consensus over the interpretation of several key concepts and a possible shift in emphasis in the interpretation of other"
current data protection rules should be scaled back, so that the rules are stripped to their core values. In our opinion, the abolishment of unnecessary formal requirements will free up time and resources, which will allow both data controllers and data protection authorities to focus on issues that really matter.

More harmonisation – Another way to reduce the current overhead, is to reach more convergent interpretations of the Directive across the EU. We therefore strongly recommend more harmonisation among Member States, to reduce the level of divergence of interpretations of the Data Protection Directive.

Realistic approach – The current data protection rules are overly burdensome, so that compliance is not realistic in a sheer number of circumstances. As a result, data protection rules (deliberately or involuntarily) too often remain a dead letter. Conversely, the recommendations below try to achieve a realistic and manageable balance between the protection of data subjects and compliance requirements for data controllers, taking into account that the intensity of the processing of personal data will only increase in the future.

No one silver bullet – The issues described earlier in this chapter illustrate the complexity of the topics concerned. It is therefore an illusion to assume that today’s data protection issues can be resolved by the adoption of one or two measures. As with other complex problems in the digital era, there is no single simple solution. Instead, we think that a wide range of legal, technical and educational measures must be combined.

Data protection as a competitive advantage – Policy makers and regulators should develop data protection rules that encourage companies to consider data protection rules as a competitive advantage instead of a regulatory burden. Although no comparison will hold, data protection rules could in this regard be considered analogous to the trend of green products and services: what used to be a mere cost driver for which the added value was only appreciated by a limited number of customers, has now become a major – and, depending on the product or service concerned – indispensable selling point.

Reasonable balance between data protection and business interests – As is evident from the overview of US law, US companies are at a competitive advantage vis-à-vis European companies, as they are not subject to strict data protection rules: instead of opt-in, US companies can apply opt-out principles; reuse of data is possible without prior consent of data subjects; spam policies are less strict than the EU; etc. The EU data protection rules should try to find a reasonable balance between protecting its citizens, and allowing businesses to flourish in the market. Obviously, this goal will requires careful consideration and balancing, particularly when the other goal of making data protection a competitive advantage for European companies, is factored into the equation.

9.2. Short term

9.2.1. Realigning the definition of personal data

Although we appreciate that — compared to the scope of the US concept of "personally identifiable information" — the scope of "personal data" must be wide in order to ensure a high level of protection, we are concerned about the very wide interpretation, as currently upheld by Working Party 29 and the various national data protection authorities.

251 See section 7 above
In particular, we think that the "absolute approach" towards personal data and the almost unlimited extent of the scope triggered by the use of the word "indirectly", should be constrained. It should be clarified in the Data Protection Directive that the question of whether data constitutes personal data, must be assessed in relation to the data controller, as well as in relation to any other data controller with whom the first data controller shares the personal data. In other words, we recommend to opt for an approach between the relative and absolute approach. It could even be envisaged to "contextualise" the definition of personal data, i.e. to take into account the context in which data is used in order to assess whether it constitutes personal data (see also the discussion on sensitive data below).

We recommend to significantly restrict the scope of the interpretation of the word "indirectly", for example by clarifying that the "indirect means" should be "within reach of", or "under the control of", the data controller.

For example, it could be specified that coded (pseudonymised) data no longer qualifies as personal data for a certain party when the original data has been encoded by an independent third party. E.g., encoded medical data would no longer qualify as personal data for a pharmaceutical company, when the original patient records are held by the hospital, which sends the records to a third party, which pseudonymises the data before sending it to the pharmaceutical company.

We also recommend to clarify that abstract profiling data does not constitute personal data.

With respect to the wide definition of "processing" in article 2.b of the Data Protection Directive, it could also be envisaged to restrict personal data to structured data (excluding unstructured data found in descriptive texts, e-mails, blogs, etc.). Provided appropriate limitations are set to data harvesting techniques — particularly unsolicited data aggregation — we think this limitation can constitute a reasonable and realistic data protection balance.

9.2.2. Reinforcing transparency measures for the online context

In our opinion, increased transparency is one of the most important keys to resolve the privacy and data protection conundrum, and to ensure that the effective use of personal data aligns with data subjects' reasonable expectations. Such increased transparency should be applied in many different ways:

**Simplified and multi-layered privacy policies** – In order to counter the shortcomings of today’s online privacy policies, online service providers must be encouraged to draft multi-layered privacy policies. Such privacy policies would consist of two parts: a **concise summary** and a **detailed statement**.

The concise summary should then only contain information which is immediately relevant for the online service at hand. In order to reduce its length — and thus encourage users to actually read the document before actually using the associated service — all details and less relevant sections should be removed from the summary, and should only be included in the detailed statement.

For example, server log files are automatically generated by most web servers, as they contain useful information for website operators. From the perspective of the website visitors, the privacy impact of these log files is typically fairly limited. Provided that these log files are only kept for a few months (and are not used for privacy-impacting data mining purposes), we think that a concise summary should not mention that these logs are kept.

---

252 I.e., profiling data about a natural person that provides no hooks to actually identify the natural person associated with the profile.  
As another example, we think it is not necessary for a company to mention in the concise summary that the company uses the contact details submitted through a contact form, when these contact details are only used to answer questions.

It could also be considered to amend the Data Protection Directive by explicitly requiring data controllers to ensure that the "average customer" can understand the privacy policy in a fast and efficient process, taking into account the nature of the service offered.

**Integration of transparency in software** – Although previous attempts to integrate privacy configurations in software\(^{254}\) have not been successful, we think that the time has come to reconsider the development of privacy configuration software. Such software should allow its users to configure his/her privacy settings, and subsequently convey warnings when a service to be used is not in line with these predefined settings. Provided such software offers an attractive and user-friendly interface and apply the "lessons learnt" from previous (failed) attempts, we think there is a realistic possibility that users and developers will use such privacy features. Ideally, such privacy features should not only be offered for websites, but also for operating systems, downloadable software, as well as software in the cloud.

**Development of templates** – Privacy policy templates (per sector or per type of website) must be developed\(^ {255}\) that adhere to the simplified, multi-layered approach described above. Such templates could even be offered via automated tools (which, ideally, integrate with the above described privacy configuration software)\(^ {256}\), in order to allow online service providers to generate the privacy policies in an efficient way. Obviously, these templates should take care not to get trapped in the "boiler plate" issue described above: they must encourage their users to carefully complete the template, so that it becomes a useful document, instead of a purely formal document.

### 9.2.3. Increasing awareness

Data subjects — particularly consumers — should in the first place be made aware of the privacy impact of their behaviour in an online context. Indeed, it is often stated that the person who can do the most to protect one’s privacy over the long run, is perhaps each person himself\(^ {257}\). All stakeholders should therefore further invest\(^ {258}\) in educating citizens about the non-volatile nature of data posted on the Internet, the electronic footprints that are inherently left behind on the Internet, online social dangers (harassment, stalking and flaming), the use of privacy enhancing technologies, the hidden business model of “free” services offered on the Internet, the awareness that personal data is being traded\(^ {259}\), the importance of the respect for privacy, etc. This will allow data subjects to make informed decisions about which online services they want to use, and which personal data they want to upload to these services.

The Commission has recently recognized the necessity of adequate education of data subjects: "**Effective protection also supposes familiarity with the rights and the risks concerned (particularly on the\(^ {254}\) See the description of the P3P project on p. 42

255 Similarly, the Rand Study recommends (p. x) that "Data Protection Authorities, with guidance from the European Data Protection Supervisor (EDPS), should be encouraged to develop more accessible privacy policies e.g. comparable to the Creative Commons model for intellectual property rights licences"

256 Examples include. However, these “privacy policy generators” do not adhere to a multi-layered, simplified approach to draft privacy policies.

257 J. PALFREY and U. GASSER, o.c., p. 70

258 The European Commission has already started on the path with respect to social networks: social networking websites were urged on 10 October 2008 on a conference organised by the Council of Europe to warn users about the low level of protection given.

259 M. KUNEVA, o.c."
Internet). Information campaigns should be conducted, in particular to raise awareness among the most vulnerable" 260. The Commission has already taken initiative in this respect, in the context of the eYouGuide project. This project informs consumers of their rights online, and also focuses on data protection261.

In our opinion, this non-legal awareness training of citizens is perhaps even more important than fostering a better knowledge of the legal aspects of current data protection rules. In our experience, most citizens already seem aware of the most important data protection rights under national and EU privacy and data protection rules. Even so, on a secondary level, they should be made better aware of these rights, particularly with respect to access and correction rights.

Awareness training is particularly important for young people (so-called "digital natives"), who are growing up with online technology, are often said to adhere to a shifting sense of privacy protection, and encounter difficulties in making a sound rational decisions about their actions262.

Finally, we think that the very (Web 2.0) technologies that increase the exposure of personal data, can — almost paradoxically263 — help in limiting each in solving the data: wiki's, social community webpages as well as peer-to-peer learning tools can be used to spread knowledge about privacy and data protection. Some of these tools are already used today, although in an uncontrolled and disperse way264. Enhanced enforcement

Data breach notifications for all data controllers – Article 4 of the E-privacy Directive currently only requires providers of publicly available electronic communications services (i.e., mainly telecom operators) to inform subscribers of the risks and measures regarding a breach of the security of the network. In our opinion, the scope of this data breach notification duty should be enlarged, to include any type of data controller. Moreover, we would also require the data controller to inform the competent data protection authority of the breach. We would, however, restrict the notifications to breaches of important data, for example sensitive data265.

Our position in this respect is similar to the position of the European Parliament266 and the European Data Protection Supervisor (EDPS)267 in the current debate on the reform of the telecommunication package. While the European Parliament would like to broaden the scope of the notification duty to

260 Commission communication, An area of freedom, security and justice serving the citizen, COM (2009) 0262 final
261 See http://ec.europa.eu/information_society/eyouguide/keywords/personal_data/index_en.htm
262 J. PALFREY and U. GASSER, o.c., p. 63
263 This is more generally known as the "paradox of privacy": technology can both enhance and detract from privacy. See L. BYGRAVE, Data protection law. Approaching its rationale, logic and limits, Kluwer Law International, 2002, p. 102
264 See, for example, the public protest against the change in Facebook's terms & conditions (February 2009). When a blogger announced that Facebook had surreptitiously changed its terms & conditions, bloggers and social media around the world quickly picked up this news to protest against this change, inter alia by setting up a petition. As a result, Facebook backed down on the change within a few days, and even announced that it would revert to user feedback systems before introducing important changes to the website.
265 Whereby the notion of sensitive personal data, is preferably changed (see section 9.3.2)
include any undertaking operating on the Internet that provides services to consumers, the EDPS would broaden the scope to other actors as well, particularly online service providers that process sensitive personal data. Incidentally, it can also be mentioned that mandatory data breach notifications have already been introduced in most US states.

Clear rules on the law applicable to data protection breaches – There should be clear rules on which country’s tort laws apply when a citizen claims to be harmed by the unlawful processing of his personal data. This recommendation is at the borderline between the short and long term.

9.2.4. Abolishment of the notification duty

Taking into account that mandatory notifications to data protection authorities contribute very little to the transparency towards data subjects, while they do cause a clear administrative burden for data controllers, we recommend to abolish the notification duty for data controllers. This will free up time for data controllers to focus on real data protection compliance, instead of mere formal compliance by submitting a notification to a national data protection authority. In our opinion, the principles that lie at the basis of the notification duty (transparency, accountability) can be satisfied in other ways.

9.2.5. Further development and promotion of Privacy Enhancing Technologies

Privacy Enhancing Technologies (PETs) help in making breaches of data protection rules more difficult, or support detecting such breaches. From the perspective of the system developer, the idea behind PETs is to design systems in a way that minimises the collection and use of personal data and hinders unlawful forms of processing. This requires both organisational and technical solutions. Examples of PETs include software to encrypt data or communication, web browsers which offer a "privacy mode", cookie blocking software, minimal disclosure tokens and privacy configuration managers such as P3P.

In a recent communication, the Commission emphasized the need for further research in the field of privacy-aware technologies: "Compliance with the principles of data protection must also be ensured through the development of appropriate new technologies, through greater public/private sector cooperation, particularly in the field of research. The introduction of a European certification scheme for "privacy-aware" technologies, products and services must be examined."

Many PET concepts and tools exist, but they are not yet broadly used in practice. The European Commission therefore already adopted a Communication regarding Privacy Enhancing Technologies, to

---

268 As recently mentioned by EU Commissioner Vivane Reding, “Transparency and information will be the key new principles for dealing with breaches of data security.”, V. REDING, Securing personal data and fighting data breaches, EDPS-ENISA Seminar ‘Responding to Data Breaches’, 23 October 2009
269 See section 7.1.2
270 First report of the Commission, p. 16
271 First introduced by Apple's Safari, and later on adopted by other browsers such as Google Chome, Internet Explorer 8 and Firefox 3.5
272 Minimal disclosure tokens prevent unauthorised manipulations of protected identity information, both by third parties and by individuals themselves. Such tokens also allow individuals to see their personal data that is shared. See www.computerweekly.com/Articles/2008/06/30/231283/identity-assurance-for-the-uk.htm
273 Commission communication, An area of freedom, security and justice serving the citizen, COM (2009) 0262 final
support the development of PETs and their use by data controllers and consumers\(^{275}\). Such efforts should be sustained and accelerated. It should also be further investigated to which extent PETs can become technical standards in certain industry sectors, or with respect to the processing of certain types of personal data\(^{276}\).

### 9.2.6. Clarifying the definition of data controller

Taking into account the importance of the qualification as data controller and the difficulties to apply the current definition to the complex online reality\(^{277}\), we recommend to change the definition of article 2.d of the Data Protection Directive. The new definition should be predictable, flexible, apt for the online context. It should try to minimise situations with concurrent data controllers for the same type of processing, as we think it is more efficient for both data subjects and data protection authorities to have to deal with a single point of contact who is responsible for the entire data processing.

### 9.2.7. Rethinking the "household exception"

The new rules should solve the current issues associated with the "household exception", particularly the issue that large numbers of private users are unnecessarily exposed to data protection obligations.

On a more fundamental level, it should be further discussed whether the private use of personal data should be simply excluded from all data protection obligations. On the one hand, it may not be desirable to subject private users to burdensome data protection obligations. On the other hand, it should be recognised that – taking into account that even the smallest digital devices can store gigabytes of data, that data will be increasingly stored "in the cloud", and that data gathered by private users will often be highly sensitive – private storage of personal data does create various risks, which may be as important as the risks created by professional users.

We therefore recommend to clarify the scope of the current "household exception", and to consider subjecting private users to at least the most important data protection obligations (instead of simply exempting them from all obligations), to the extent they are relevant in a private context.

### 9.2.8. Narrowing down the interpretation of the "use of equipment"

As explained in section 4.3.2, the "use of equipment" criterion for applicability of the Data Protection Directive, is currently interpreted too widely, due to the fact that data protection authorities consider the storage of a cookie on web visitors' computer to be a "use of equipment".

We recommend to explicitly amend article 4.1.c of the Data Protection Directive, in order to mitigate this current extensive interpretation. For example, article 4.1.c could be changed to read as follows: "...makes use of equipment, automated or otherwise, that is under the control of the data controller or its data processors and is situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community". As cookies can be deleted at any moment by the data subject (so that they are not really "under the control" of the data controller), this small amendment seems sufficient to narrow down the scope article 4.1.c.

---

\(^{275}\) 2 May 2007

\(^{276}\) See below, standardisation

\(^{277}\) See section 4.6
9.2.9. Taking measures against unsolicited data aggregation

With respect to the issue of unsolicited data aggregation\textsuperscript{278}, it should be recognised that these types of services are already likely to breach the Data Protection Directive and the e-Privacy Directive.

Telephone operator BT had tested Phorm (behavioural advertising technology) in 2006 and 2007, without informing the customers involved\textsuperscript{279}. The e-Privacy Directive prohibits any type of interception of electronic communications and related traffic data without the consent of the individuals concerned. Use of Phorm without consent of the customers involved, is therefore prohibited under the e-Privacy Directive\textsuperscript{280}.

Considering the surreptitious and unsolicited nature of these activities, as well as their privacy-threatening features\textsuperscript{281}, we recommend to take strong action against these services.

It could also be envisaged to include an explicit prohibition in the Data Protection Directive, although care should be taken not to undermine the functioning of regular search engines (that offer functions that may in some respects be similar to real unsolicited data aggregation). The prohibition on unsolicited data aggregation could in this respect be similar to a prohibition on spam.

9.2.10. Clarifying the scope of article 15.1 of the Data Protection Directive

As explained in section 4.9, it is not clear whether, and when, article 15.1 of the Data Protection Directive (which holds that every person has the right not to be subject to an automated decision that produces legal effects concerning him, or significantly affects him) applies to profiling data.

We recommend to clarify that article 15.1 does not apply to abstract profiles\textsuperscript{282}, and to strictly limit the prohibited decisions to specific domains (for example, financial grants and job evaluations). From a data protection perspective, such restriction of scope prevents that the Data Protection Directive would hinder bona fide profiling applications\textsuperscript{283}. Of course, even in the event where abstract profiles are allowed, it must be ensured that the fundamental principle of non-discrimination is always guaranteed.

9.2.11. Self-regulation

General – Article 27 of the Data Protection Directive encourages the use of codes of conduct that are intended to contribute to the proper implementation of the national provisions adopted by the Member

\textsuperscript{278} See section 2.3.3
\textsuperscript{279} C. WILLIAMS, Brussels to sue UK over Phorm failures, The Register, 14 April 2009, available at www.theregister.co.uk/2009/04/14/eu_phorm_formal/page2.html
\textsuperscript{280} The European Commission recently launched an infringement proceeding against the UK, following complaints of internet users concerning this Phorm case. By limiting the principle confidentiality of electronic communications to international communication, the UK has implemented the e-Privacy Directive incorrectly. A letter of formal notice has been issued by the Commission on 14 April 2009. The UK failed to respond to the questions of the Commission within the proposed deadline (see www.theregister.co.uk/2008/08/12/eu_phorm_letter/)
\textsuperscript{281} particularly when new data processing technologies, such as face recognition, will be applied
\textsuperscript{282} assuming such profiles would qualify as personal data in the first place
\textsuperscript{283} This chapter limits its analysis of profiling and behavioural advertising to a privacy and data protection perspective, since a review of the "consumer acquis" is outside the scope of this study. In this respect, it is useful to further examine the effects of behavioural advertising on consumer's rights, for example in relation to unfair commercial practices, price discrimination and the blurring between advertising and editorial content. In this context, DG SANCO recently issued a Non-Paper (Data Collection, Targeting and Profiling of Consumers for Commercial Purposes in Online Environments, 5 March 2009) and organized a roundtable and Consumer Summit (March-April 2009)
States, taking account of the specific features of the various sectors. In our opinion, the possible benefits of this article have not yet been fully realised. It is therefore necessary to examine the advantages of self-regulation\textsuperscript{284}, as compared to a pure market model and a pure government enforcement model.

The advantages of self-regulation include the opportunity to make use of industry expertise. The industry itself is usually aware of the costs involved in complying with certain types of rules. Self-regulation can also lead to the creation and subsequent enforcement of norms of behaviour. The specificities of certain types of processing or sectors can be taken into account, whereas general legislative rules are often too vague since they must be applicable in very divergent circumstances. Areas of data protection that are subject to self-regulation may provide an incentive for the industry to enhance its reputation. Finally, technical standards can create network externalities, lower costs and increase competition\textsuperscript{285} (see our recommendations in Chapter 13 - self regulation).

**Limits of self-regulation** – The US self-regulatory examples described on page 46 demonstrate that self-regulatory efforts alone most likely cannot ensure the level of data protection envisaged by Europe. Also, the advantages and disadvantages of self-regulation should be carefully weighed so as to determine which combination of self-regulation and government enforcement will be most efficient, and at which level self-regulation should play a role (legislation, adjudication and/or enforcement).

**Examples** – We think that self regulation could be particularly useful in the following example domains:

- **Community sites** – Community sites have already engaged in self-regulation with respect to the safety of their young users (for example the engagement to apply privacy-safe default settings, to ensure that profiles of young people are not searchable, to prevent use of their services by underage users, etc.)\textsuperscript{286}. Such engagements could be extended to other user categories as well, for example with respect to the use of personal data for direct marketing purposes, data personal data access rights, permanent deletion of profiles, etc.

- **Behavioural advertising** – Through self-regulation, companies that are involved in behavioural advertising could engage to provide information towards consumers on how their behaviour is being monitored, which parties are involved, and how they can opt-out.

In the UK, a first step was recently taken by the Internet Advertising Bureau, which launched a set of self-regulatory Good Practice Principles for online behavioural advertising, which came into force on 4 September 2009. The Principles are based on notifying users about data collection, allowing them to choose whether or not to participate, and educating users on behavioural advertising\textsuperscript{287}. Incorporation of technology and privacy by design

\textsuperscript{284} It should be noted that self-regulation also implies certain risks. For example, they may encourage industry members act together to exercise market power, which is not likely to lead to a balance between their interests and those of data subjects. Similarly, closed standards and standards rely on the intellectual property rights of certain market players, may create antitrust risks.


\textsuperscript{286} The "Safer Social Networking Principles" have been adopted by a number of important community sites, including Facebook, Netlog and Google. A list of all signatories and self-declarations can be found at http://ec.europa.eu/information_society/activities/social_networking/eu_action/selfreg/index_en.htm#selfDecl

\textsuperscript{287} The signatories of the Good Practice Principles include several important behavioural advertising companies, including Google and Phorm, available at www.iabuk.net/en/1/behaviouraladvertisinggoodpractice.html
Recital 46 of the Data Protection Directive emphasises the importance of taking appropriate technical and organisational measures, both at the time of the design of the processing system, and at the time of the processing itself — particularly in order to maintain security and thereby to prevent an unauthorised processing. This principle could be further extended to the design of software and data processing systems (the so-called "privacy by design" principle), so that privacy rights are embedded right into the technology itself. The technology itself would then be configured from the ground up to take into account important data protection principles, such as the minimisation of the routine collection and use of personal data, the use of encryption and coded information whenever possible, etc.

In this respect, the Commission recently confirmed the need to stimulate and support the introduction of the "security and privacy by design" principle at an early stage in the development of RFID applications. The Commission therefore urged Member States, in collaboration with the industry, to inform and raise awareness among companies, in particular SMEs, of the potential benefits and risks associated with the use of RFID technology.

More specifically, RFID tags should be designed so as to enable citizens to disable ("kill") the tracking ability of the tags after purchase. In this respect, the Commission will launch a debate to further investigate the technical and legal aspects of the "right to silence of the chips", which expresses the idea that individuals should be able to disconnect from their networked environment at any time. EU Commissioner Viviane Reding maintains the same point of view, and recently stated "no European should carry a chip in one of their possessions without being informed precisely what they are used for, with the choice to remove or switch it off at any time." Similarly, with respect to software, attention for privacy should be built-in. Although this concept is rather new for software developers and may seem counter-intuitive in an IT context that is clearly targeted at maximal information processing, software engineering practices have shown that it is possible to convince developers to focus on aspects which may not seem to add immediate value to the software environment. Attention for privacy and data protection could therefore be compared to attention for software security, a virtue which has only really taken off in the last decade. Before this time, writing secure software was often considered an after-thought, or a feat which must only be added to software when specific issues would arise. Conversely, writing secure software and building secure systems that can withstand intrusion and hacking attempts, has now become a key part of the entire development process.

9.2.12. Adopting standards

Taking into account that the lack of standards supporting data protection legislation creates considerable uncertainty for both data controllers and data subjects, we strongly recommend to encourage the

---

288 Commission Recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification, 12 May 2009, C(2009) 3200 final, p. 8
289 Ibid.
293 As illustrated by the following quotes, found in G. McGRAW, Software security: building security in, 2006, Chapter 1: "The notion of software security risk has become common knowledge, yet developers, architects, and computer scientists have only recently begun to systematically study how to build secure software.", and "Security was the exclusive domain of guns, dogs, and concrete not too many years ago. Since the worldwide deluge that is the Information Age, all things security have changed radically. In tandem with the stunning growth of the Internet, the new field of computer security has taken root and grown like a weed"
adoption of data protection standards in the short term. Several advantages can be identified when standards – which are a kind of self-regulation – would be implemented in the field of data protection:

- standards create a level playing field between market players;
- standards offer a balanced representation of all interested parties, including end users or consumers;
- standards have an explicit status vis-à-vis the law; and
- standardisation has a specific toolset of enforcement mechanisms.

Within the EU context, the policy makers have, since many years, been using standardisation as one of the instruments to reach their policy objectives. The usefulness of standards has been recognized by the 29th International Data Protection and Privacy Commissioners’ Conference: “Standards are one way of applying technical and organizational specifications which can translate legal requirements into concrete practices.”

However, it should be noted that compliance with (even formally adopted) standards will not necessarily and automatically result in compliance with the Data Protection Directive (although compliance with formally adopted data protection standards would significantly facilitate compliance with the Directive). In order to achieve this automatic compliance result, the Data Protection Directive needs to be re-qualified into a “New Approach” Directive, which is one of our recommendations for the mid-term.

Examples – The use of standards can be envisaged for the following data protection related issues:

- content and structure of privacy policies;
- appropriate security measures for data controllers and data processors;
- standards for specific data protection tasks, such as the right to access and correction, as well as information obligations;
- some commentators propose to introduce a “digital territory” in order to counter the privacy-undermining effects of ambient intelligence. Such digital territory would introduce protective borders, for example in private or public bathrooms, where intelligent devices are not allowed to perform their tracking and monitoring activities. Although respect for the digital territories should also be enforced in law, standardisation can also play an important compliance role in this regard.
- standards for storage terms, per industry sector or per category of personal data.
- standard data export formats, when the right of data portability would be recognised.

Legal basis – In order to receive a formal legal status, standards should be adopted through the European Standardisation Organisations (CEN, CENELEC and ETSI), based on the legal framework of Directive 98/34 and Council Decision 87/95. It should be noted that, the ICT standardisation policy is currently under scrutiny by the European Commission.

---

294 See P. VAN EECKE, P PINTO and T. EGYEDI, EU Study on the specific policy needs for ICT standardisation, study commissioned by the European Commission, available at www.ictstandardisation.eu


296 See for example W3C’s Platform for Privacy Preferences, as discussed in detail in section 6.1


298 See section 9.3.3
**CEN initiatives** – In the context of the Initiative for Privacy Standardisation in Europe (IPSE), CEN has created a Workshop on Data Protection and Privacy (DPP), which contributes to resolving ICT technical compliance issues, taking into account EU data protection legislation\(^299\). The DPP Workshop will, *inter alia*, work on the privacy aspects of RFID standards, implementing the concept of “privacy and security by design”\(^300\).

### 9.2.13. Clear criteria with respect to the applicable law

The provisions with respect to the applicable law should be far less complex, and – as regards the applicable national law – data controllers should only be obliged to comply with one national data protection law.

In order to reach this goal, several definitions and concepts should be rephrased so as to minimise the possibility of divergences in interpretation and in some cases, limit their scope of application. Concepts and rules included in the Directive should also be adequate in respect of current and future technological evolutions.

**Applicable Member State law** – To determine the applicable law within the EU, a suggested approach would be the home country control principle, which implies that controllers are only subject to the national law of the Member State where they are established. To ensure no uncertainties can arise as to which national law applies, controllers that are established in different Member States, could – for example – be allowed to choose which of the possible national laws will apply (they would be required to notify their choice in the privacy policy). Furthermore, to the extent different entities of a certain corporate structure process the same personal data for the same purposes, they may need to be considered as one single entity for the transfer of such personal data between them.

**Applicability of EU data protection rules** – In order to determine whether the EU data protection rules apply to websites or online services operated by data controllers outside the EU, it could be envisaged to adopt a provision which holds that the EU rules only apply when the website or online service is targeted at EU citizens, or objectively used by a non-trivial amount of EU citizens. In our opinion, such provision would constitute a reasonable balance between the protection of EU citizens and legal certainty and flexibility for foreign businesses.

### 9.2.14. Adapting transfer prohibitions to today’s reality

As pointed out in section 4.4, one of the most important shortcomings of the current EU data protection rules is their failure to deal with the constant cross-border data flows. As a result, there is a significant discrepancy between the very strict legal requirements (which only allow transfers of personal data to third countries in specific circumstances), and the practical reality in the online context. In our opinion, various solutions to this discrepancy can be found to resolve this discrepancy, both in the medium and the long term.

**Optimising BCR procedure** – The BCR procedure must be further optimised and streamlined. In particular, the mutual recognition procedure for BCRs currently accepted by thirteen Member States must be further extended so as to include all Member States.

\(^{299}\) See [www.cen.eu/CENORM/Sectors/Sectors/ISSS/Activity/wsdp.asp](http://www.cen.eu/CENORM/Sectors/Sectors/ISSS/Activity/wsdp.asp)

\(^{300}\) Standardisation mandate issued by the Commission to the European Standardisation Organisations in the field of Information and Communication Technologies applied to RFID and systems (M 436), 8 December 2008
Create new safe harbors – In order to facilitate data transfers between the EU and the US, the US Department of Commerce has, in consultation with the European Commission, developed a “safe harbor” framework. It may be useful for the EU to encourage governments of other countries to also set up safe harbor systems. Similar to the US safe harbor, foreign companies could then voluntarily commit to compliance with the EU data protection principles. As a result, they can freely do business with EU companies, without a further need to conclude model clauses agreements or to fulfill other administrative formalities.

Solving the transfer paradox – In order to solve the data transfer paradox, and find a solution for the competitive disadvantage sustained by companies established in the EU, we recommend to adopt an exception that would allow personal data to be processed in the EU without a sufficient legal ground under the EU rules, when the personal data concerned was collected in accordance with the local laws of a third country. This exception should, of course, be without prejudice to the EU data protection rules when the personal data collected in third countries would be combined with personal data collected within the EU.

Extension of the “legal obligation” ground – We recommend to extend the scope of article 7.c of the Data Protection Direction, so that the necessity to process personal data for reasons of compliance with third-party legal obligations, is also accepted as a lawful ground for processing. We would, however, explicitly state that the data controller must not have voluntarily sought to become subject to the legal obligation that is invoked.

Gradual recognition of adequate protection – As an alternative to the current binary distinction between countries which do and countries which do not provide adequate protection, intermediary categories could be introduced (likely in the mid-term timeframe), depending on the type of processing and countries involved. For example, the USA could be considered as providing adequate protection for profiling data, pseudonymised data (encoded by a third party encoder), and data that does not allow direct identification.

Controller accountability – Also in the mid-term time frame, instead of regulating data transfers in the context of a state-to-state approach, data transfers could be regulated regardless of whether they occur in a European or international context. Such approach is especially relevant in a controller-processor context, where data controllers could be held accountable for the protection of personal data. This implies that it is up to the controller to verify whether the third party processor has the necessary policies and processor in place to ensure adequate safety of the data transferred.

With respect to controller-to-controller transfers outside the EU, such an approach which solely relies on the controller’s liability, is less desirable. Contrary to a controller-processor relationship, the receiving controller, established outside the EU, will not obliged to strictly comply with the other controller’s instructions and policies.

---

301 See p. 28

302 Another condition would, obviously, hold that the local laws of the third country allow this personal data to be processed in the EU in the way envisaged by the data controller.

303 A similar approach is maintained in Japan, where data transfers are regulated as such, without specifying additional conditions in case of transfers outside Japan (see section 7.2.4). Similarly, Canadian law provides that, regardless of where information is being processed (whether in Canada or abroad), the organization must take all reasonable steps to protect it from unauthorized uses and disclosures while it is in the hands of the third party processor (see www.priv.gc.ca/information/guide/2009/gt_dab_090127_e.cfm)
9.3. **Mid-term**


As pointed out above, we recommend to adopt data protection standards in the short term. However, in the mid-term, we recommend to take this concept of standardisation one step further.

It could be considered to re-qualify the Data Protection Directive as a so-called "New Approach" Directive. This way, it will be formalised that the practical and technical implementation of the principles set forth by the Directive is to be laid down in standards. As a consequence, compliance with formally adopted standards in the field of data protection will automatically result in compliance with the respective requirements of the Data Protection Directive.

The "New Approach" covers domains relating to the protection of health, safety and security. It entails a set of rules and principles governing the EU standards setting, which are laid down in the Council Resolution of May 1985 on a New Approach to technical harmonisation and standards and Directive 98/34/EC (the "Transparency Directive"). It upholds a clear separation between EU legislation and EU standardisation efforts.

The New Approach relies on four principles: (a) formal legislation should be limited to the essential requirements; (b) these essential requirements are further implemented by standards; (c) the standardisation efforts are entrusted to competent organisations; and (d) the adoption of standards remains voluntary (companies are not legally required to comply with the standards, but when they do, there is a presumption of conformity with the essential requirements).

In our opinion, the Data Protection Directive meets the fundamental criteria laid down by the Council Resolution in order to qualify as a "New Approach" Directive.

9.3.2. **Modifying the concept of sensitive data**

In light of the various problems associated with the current definition and interpretation of sensitive data (see section 4.7 above), we recommend to modify the definition.

Commentators have suggested to convert the current approach to sensitive data — which relies on a fixed number of categories of data that are always presumed to be "sensitive" — into either a *purpose*-based approach, or a *contextualised approach*. In the purpose-based approach, personal data is qualified as sensitive when the processing is intended to reveal sensitive data. A contextualised approach to sensitive data, on the other hand, means that personal data becomes sensitive according to its context.

Although different, both approaches have the advantage of better grasping the reality of whether certain types of data should receive a higher level of protection. Sensitivity is then no longer perceived as an *a priori* attribute, but only when the purpose or the circumstances of the processing call for higher protection.

---

304 (1) the area in question should not call for an exhaustive regulation; (2) the area should have "potential" for standardisation (the New Approach would not be suitable for areas that must be strictly regulated); (3) strict law-making in the area must not be well advanced; and (4) there must be sufficient indications of internal market barriers in the area.

305 However, data protection should also be considered a type of (non-physical) "safety". This may require legislative intervention.


307 SIMITIS, *Revisiting sensitive data*, 1999. This approach was also used by Germany.
9.3.3. Introduction of new data protection rights

In order to counter some of the issues identified for social websites, it could be envisaged to introduce two new rights in the Data Protection Directive:

**Right to be forgotten** – This would give every citizen the right to ask a data controller to remove personal data as from a specified period of time (for example, five years), even when the data was initially collected with the consent of the data subject and the data controller has reserved the right to keep using the data in the future\(^{308}\). Such "right to be forgotten" would be particularly useful for community sites\(^{309}\), where data subjects may regret in the future of having uploaded pictures and blogs today. The terms and conditions of these community sites currently do not allow data subjects to "forget". It is interesting to note that the "right to be forgotten" is already being considered in France\(^{310}\).

**Right of data portability** – Article 12 of the Data Protection Directive already grants data subjects the right to access their personal data, and to request communication "in an intelligible form" of the personal data that is being processed. However, article 12 does not require data controllers to send actual copies of the data: it suffices to communicate the data "in an intelligible form".

It could be considered to extend the scope of article 12 into a true "right of data portability", which would allow data subjects to request a copy of the personal data held by the data controller\(^{311}\). Industry standard file formats could be used when the personal data would be stored by the data controller in proprietary data structures.

9.3.4. Ensuring transparency for ambient intelligence

In order to counter the privacy undermining effects of ambient devices, standardized symbols and warning methods should be developed to indicate that certain places are monitored. Similar to warning signs for camera surveillance, citizens should be informed of the presence of the devices, the data which is collected, the data processing purposes and the data controller.

9.3.5. Entering into an international data protection treaty

In addition to the medium term recommendations to resolve the data transfer conundrum, we recommend to initiate discussions for an international data protection treaty, with a group of countries as large as possible. Provided this data protection treaty offers a reasonably high level of protection, it is consequently recommended that all parties to such treaty are recognized by the EU as ensuring an adequate level of protection. In this regard, it can be useful to analyse recent regional and global initiatives.

**Regional initiatives** – The Asia-Pacific Economic Cooperation (APEC)\(^{312}\) has recently adopted a Privacy Framework\(^{313}\) which sets out nine basic principles with respect to data protection, and enables...

---

\(^{308}\) The "fundamental right to forget" was one of the topics recently discussed during the Personal data use and protection Conference organised by the European Commission. For an overview of the presentations made regarding this subject, see http://ec.europa.eu/justice_home/news/events/news_events_en.html#dp_conference_2009

\(^{309}\) and perhaps also search engines

\(^{310}\) See www.senat.fr/leg/ppl09-093.html

\(^{311}\) See, for example, the Data Liberation Front initiative of Google: wwwdataliberation.org

\(^{312}\) Of which the 21 member economies include, inter alia, the United States, Russia and the People’s Republic of China, available at www.apec.org/apec/member_economies.html
regional data transfers to the benefit of consumers, business and governments. It focuses on both domestic and international implementation of privacy standards for APEC member economies and explores new ways of information sharing and cooperation across agencies and authorities to enable transfers of personal information across borders.\footnote{Available at www.apec.org/etc/medialib/apec_media_library/downloads/taskforce/ecsgr/pubsl/2005.Par.0001.File.v1.1}

Similarly, the Latin American Data Protection Network (RIPD)\footnote{Available at www.apec.org/apec/news__media/fact_sheets/apec_privacy_framework.html} adopted "A commitment to attain International Data Protection and Privacy Standards"\footnote{Available at www.agpd.es/portalweb/english_resources/regulations/common/pdfs/statement_vi_ripd_en.pdf} at its sixth meeting in May 2008. The statement recognizes that "the processing of personal data has multiplied exponentially in the midst of a globalised world" and that "global economic development entails a new thrust of international data flows that are processed in geographical environments with a variety of regulations providing different levels of guarantee for individuals". The statement therefore considers that giving an appropriate response to the protection of personal data makes it necessary to adopt international standards such as to provide individuals, regardless of where their data are processed, with certain guarantees.

Similar to other international legal instruments on data protection, the RIPD statement recognizes the Council of Europe's Convention 108\footnote{Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe, adopted 28 January 1981} as a benchmark in terms of guaranteeing adequate protection of personal data. The principles contained in the 1980 OECD Guidelines on the Protection of Privacy and Trans-Border Flows of Personal Data, which are very similar to those contained in Convention 108, have served as a basis for the APEC Privacy Framework.\footnote{APEC Privacy Framework, p. 3, n° 5}

Global initiatives – Even on a global international level, there seems to be a consensus as regards the need for global standards with respect to the protection of personal data. The 30th International Data Protection and Privacy Conference\footnote{www.privacyconference2008.org} organised in October 2008 by the French and German data protection authorities, was attended by participants from 60 countries. One of the resolutions adopted by the Conference, is the "Resolution on the urgent need for protecting privacy in a borderless world, and for reaching a Joint Proposal for setting International Standards on Privacy and Personal Data Protection". The Resolution refers to the Montreux declaration adopted at its 27th Conference, in which it appealed to the United Nations to prepare a legally binding instrument which clearly sets out in detail the rights to data protection and privacy as enforceable human rights.

As part of this Resolution, the Conference has also mandated the establishment of a working group, to draft and submit a Joint proposal for setting international standards on privacy and personal data protection. Part of the working group's tasks is to examine the role to be played by self-regulation, to formulate the essential guarantees for better and flexible international transfers of data and to elaborate

\footnote{Available at www.privacyconference2008.org/adopted_resolutions/STRASBOURG2008/resolution_international_standards_en.pdf}
a set of principles and rights which, while reflecting and complementing existing texts, aim to achieve the maximum degree of international acceptance ensuring a high level of protection\textsuperscript{322}.

Following the 30th International Conference, a group of data protection authorities, chaired by the Spanish Data Protection Authority, have commenced drafting these "International Standards on the Protection of Privacy with regard to the processing of Personal Data". It is expected that this global legal instrument will be approved at the 31st International Conference of Data Protection and Privacy Commissioners in November 2009\textsuperscript{323}, and will be submitted to the United Nations as the basis for a treaty\textsuperscript{324}.

**European Parliament** – A recent recommendation of the European Parliament\textsuperscript{325} on strengthening security and fundamental freedoms on the Internet identifies different issues originating from the widespread use of the Internet. The European Parliament recommends the Council to recognise that the global and open nature of the Internet requires global standards for data protection, security and freedom of speech, and to call on Member States and the Commission to take the initiative for the drawing up of such standards. In this context, the European Parliament also refers to, and welcomes, the Resolution adopted by the 30th International Conference as further described above\textsuperscript{326}.

**Evaluation** – There seems to be a worldwide consensus as regards the fact that an international data protection instrument is required to ensure privacy protection while at the same time allowing cross-border data flows. Also, there seems to be a certain level of consensus, as regards the basic principles for data protection, as included in the OECD Guidelines and Convention 108.

\textsuperscript{322} 30th International Conference of Data Protection and Privacy Commissioners, Resolution on the urgent need for protecting privacy in a borderless world, and for reaching a Joint Proposal for setting International Standards on Privacy and Personal Data Protection, p. 4

\textsuperscript{323} See www.privacyconference2009.org/privacyconf2009/index-ides-idweb.html


\textsuperscript{326} Ibid., recommendation ae
EU study on the

Legal analysis of a
Single Market for the Information Society

New rules for a new age?

5. Copyright and digital content

November 2009
## Table of contents

**Chapter 5 Copyright and digital content**

1. Introduction.................................................................................................................. 2
   1.1. Current trends — and their issues ........................................................................... 3
   1.2. The copyright infringements problem ...................................................................... 6
2. Overview of the current legal framework...................................................................... 8
   2.1. Overview of all EU legal instruments relating to digital content ......................... 8
   2.2. Most important legal provisions ........................................................................... 10
3. Key issues in the current EU legal instruments ........................................................... 14
   3.1. Gaps ...................................................................................................................... 14
   3.2. Ambiguities ......................................................................................................... 16
   3.3. Unbalanced provisions ....................................................................................... 17
   3.4. Obstacles for the Single Market .......................................................................... 20
   3.5. Issues relating to TPMs ...................................................................................... 21
   3.6. Relation to the eCommerce Directive ................................................................... 24
   3.7. Future-readiness and technological neutrality ..................................................... 25
4. Practical impact of current legal framework ............................................................... 31
   4.1. National Implementation of EU level legal instruments ......................................... 31
5. Practical example: Europeana.................................................................................... 39
   5.1. Introduction .......................................................................................................... 39
   5.2. Licence restrictions ............................................................................................. 40
   5.3. Orphan works ..................................................................................................... 41
   5.4. Consequences of format shifting ........................................................................ 42
   5.5. Public domain works .......................................................................................... 42
6. Conclusions .................................................................................................................. 43
7. Recommendations......................................................................................................... 44
   7.1. Responding to the changed role of users ............................................................... 44
   7.2. Meeting business requirements .......................................................................... 48
   7.3. Promoting the fair balance of rights between the interested parties .................... 53
   7.4. Dealing with TPMs ............................................................................................. 60
   7.5. Start a fundamental copyright debate .................................................................. 62

---

This study was commissioned by the European Commission's Information Society and Media Directorate-General, in response to the invitation to tender OJ 2007/S 202 244659 of 19/10/2007. The study does not, however, express the Commission's official views. The views expressed and all recommendations made are those of the authors.
Chapter 5
Copyright and digital content

1. Introduction

Rapid changes in technology, modifications of legal instruments and new business models have created "the perfect storm around intellectual property conceptions". The vast usage, exchange and distribution of digital content have created a new reality for the different interests of the content owner (rightholder) and of the user of the content to meet.

Different interests – Rightholders want to fully commercially exploit the value of their content, maintain their rights as much as possible, increase infringement detection possibilities, and enhance control over their work through the use of technological measures. Conversely, content users want to freely interact with the digital environment and make a profitable use of the digital content at a minimum cost by exploiting the individual qualities of a digital work. In the new digital era, these two interests are closely related, and in some occasions they merge with each other.

EU-level initiatives – In a 2007 Single Market Report, the European Commission highlighted the need to promote the free movement of knowledge and innovation as the “Fifth Freedom”. In the same vein, the European Parliament and the Council have stressed that there is an increasingly apparent demand for quality digital content in Europe with balanced access and users rights. The participation of all stakeholders in the knowledge-based economy is a strategic objective for the European Union. This is also in line with the Lisbon European Council, that set the transition to a knowledge-based economy as a new strategic goal for the European Union, by stipulating that it is important: "to become the most competitive and dynamic knowledge-based economy in the world, capable of sustainable economic growth with more and better jobs and greater social cohesion". The presidency conclusions further recommended to establish an "information society for all", in order to prepare the evolution to a competitive, dynamic and knowledge based economy. This shift to a knowledge-based economy will be a powerful engine for growth, competitiveness and jobs, capable of improving the quality of life and the environment. In addition, article 118 of the Lisbon Treaty stipulates that "in the context of the establishment and functioning of the internal market, the European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall establish measures for the creation of European intellectual property rights to provide uniform protection of intellectual property rights throughout the Union and for the setting up of centralised Union-wide authorisation, coordination and supervision arrangements."

Hence, in order to fully reach the goal of an information society for all, it is essential to make digital content more accessible, usable and exploitable for everyone in Europe. Furthermore, as the new knowledge-based economy requires the contribution of all parties, it is important to reconcile all interests and to carefully balance their rights and obligations in order to establish a harmonised regime of

---

1 Promoting innovation and economic growth: the special problem of digital intellectual property a report by the digital connections, Council of the committee for economic development, 2004, p. 14
3 Decision 456/2005/EC [OJ L 79/1/29-3-2005], consideration nr. 5
4 Presidency Conclusions, Lisbon European Council 23-24 March 2000, para. 5
5 ibid., para. 8
protection throughout the Single Market. This chapter therefore investigates today’s digital content challenges.

1.1. Current trends — and their issues

In order to better understand the situation described previously, current practical issues and trends must be further presented.

Within the new digital environment, Internet users and owners of personal digital devices (such as personal computers, CD-players, DVD-players, iPods, etc.) are now able to play the role of the creator, re-creator and distributor of the digital information\(^6\). Any user who obtains the right digital equipment — most of which are cheap and easy to obtain and to use in everyday life — can produce digital works. Although there is every reason to believe that this phenomenon is only in its infancy, it remains unclear to which extent this user-generated content will become prominent in the future\(^7\).

Furthermore, the distribution of information and entertainment is shifting from the physical to the digital environment, while at the same time there is also a move from tangible to intangible methods of content distribution\(^8\). The distribution has also become more direct: due to the penetration of digital devices, it is now possible to distribute content directly to the user. This also means that the role of typical offline intermediaries (administrators, publishing companies, music companies, etc.) tends to diminish.

For these reasons, the role of the user in the creation, modification and distribution of digital content has changed significantly. The penetration of digital culture has led to the conversion of the role of the consumer of the content to that of an interactive user of the pre-existing copyrighted materials. The user not only has the ability to tailor the content according to his desires and needs, but also the ability to choose the conditions under which he can receive this content. The interactivity of the content relates not only to the content itself, but also to all the conditions surrounding its consumption\(^9\). The user creative content phenomenon is showing considerable development: according to the i2010 Mid Term Review “User-created content experienced especially rapid take-up, confirming the Internet as a medium of two-way communication, but now on the richer level facilitated by broadband access. 24% of European citizens posted or participated in online fora in 2007, up from 18% in 2006, with Estonia the most active country at 44%.28”\(^10\).

Moreover, the new information era has promoted the individualisation of content. The multiplication of consumer’s choices has modified the business model: from “push” (where only the service provider determined the schedule) to “pull” (where the consumer’s choices regarding the content have been multiplied)\(^11\).

\(^6\) G. MAZZIOTTI, EU Digital Copyright Law and End User, Springer, 2008, p. 4

\(^7\) See European Internet Foundation, The digital world in 2025 - indicators for European Action, available at www.eifonline.org/site/download.cfm?SAVE=10859&LG=1, p. 22

\(^8\) Study on the implementation and effect in member states’ laws of the Directive 2001/29/ EC on the harmonisation of certain aspects of copyright and related rights in the information society, Institute for Information Law, final report, February 2007, p. 8


\(^10\) i2010 Mid Term Review, (COM/2008/199) p.36

\(^11\) Ibid.
From the business point of view, digitisation of content allows traditional business models to promote online transactions. Within this environment, new online business models are developed that promote the new digital content. These business models “are characterized by various elements such as the type of transport technology (downloading or streaming), the type of network used for distribution (open or proprietary), the type of DRM used, the level of interactivity etc.”

Companies tend to develop business models that are either exclusively offered online, or that are transferred from already existing commercial ventures, so as to increase the quantity of customers being addressed. Moreover, new business models appear that take advantage of consumers’ involvement in the creation and distribution of content, and that build upon user generated work in order to commercially exploit it.

Moreover, technological advances have made that copying has become a rather prevalent act. The fact that copying has been made simpler, has led to a change of mentality of the digital users. The general public can easier than ever before and in more cost effective ways, download, copy, store and share copies of works. The low threshold towards copying digital content may lead to what has been called as “home-pirating” or “soft-pirating”. In many instances this is considered by the users as a “safe” practice. These practices proliferate due to the lack of effective and financially efficient measures for mass protection against those actions, and the high costs and difficulties to detect and prosecute infringements. (Due to the importance of copyright infringements for the creative sector, this issue is further investigated in the next section.)

New concepts have appeared that try to meet the needs of the participants in the current knowledge based economy. Such a notion is that of "open content”, described by some authors as "a definitive work published in a format that explicitly allows copying and modifying of its information by anyone”, and by others as not for profit content, produced (often collectively) with the intentional purpose of making content available for further distribution and improvement by others at no cost.

An "open content licence" is a licence that enables copying and distribution of content without payment. The rights and obligations set forth by these licences varies. In some cases, the creation of derivative works by the grant of permission to re-use the licensed content may be more controlled, whereas in some other cases it might be completely free.

---

12 Study on the implementation and effect in Member States’ laws of the directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society, final report, Institute for Information Law, February 2007, p. 21

13 In some Member States, such as the Netherlands, the downloading of audiovisual works does indeed seem legal, to the extent it falls within the scope of the home copying exception. See Kamervragen met antwoord 2006-2007, nr. 2256, Tweede Kamer and Kamervragen met antwoord 2007-2008, nr. 1862, Tweede Kamer


15 Intellectual property guidelines, version 1.0, edited by Minerva EC Working Group, September 2008, p. 31

16 Some common restrictions include the following: (i) works which derive from an open content license must themselves be released under an open content license (this prevents a third party from making a commercial product on the basis of content he received for free); (ii) the open content shall not be used in a commercial application; (iii) a copy of the license must be attached to any derivative work (this ensures that further descendant works are covered by the same license); (iv) attribution of the source of the content must be attached to the content, and retained in later derivative (“descendant”) works. This attribution is often the only form of reward enjoyed by the original/previous creator, and is used by him as a method to develop reputation, employability, etc; (v) no warranty is provided (the work is provided on an ‘as is’ basis); (vi) the license cannot be modified. See Intellectual property guidelines, version 1.0, edited by Minerva EC Working Group, September 2008, p. 32
An example of an open content licence is the Creative Commons (CC) set of licences. These licences define a spectrum of possibilities, between full copyright (all rights reserved) and the public domain (no right reserved). These licences help the creator keep the copyright upon his work while at the same time allowing certain uses (the so called "some rights reserved copyright"). The goal of Creative Commons is to create an easy mechanism for rightholders to turn their work over to the public or exercise some but not all of their legal rights over the work.

Some stakeholders question whether licences such as Creative Commons would be able to fulfil the needs of a licensor and a licensee. According to one stakeholder, a licence alone is not enough: "what is crucial to remember (as it is not explicit in the information supporting the CC licensing scheme) is that the licence does not, in itself, provide any rights protection to the creator as it lacks any support infrastructure. Without any means of exercising control the creator is, in effect, giving away all rights (globally and in perpetuity) whether that is the intention or not. Legislation will not change this; consumer and creator education, involvement of existing models for individual and collective rights management, and creator-controlled open DRM systems could potentially be more effective” 17.

Related to that is, also, the notion of "open access", which consists of a publication model for cultural and academic publications through the Internet18. Much of the open access content is published under an open content-like licence.

In the same vein, as regards software, is the rise of open source software (OSS). According to the i2010 Mid Term Review "open source software is also expected to increase its contribution to the dynamics of the software market; [...] open source will have a significant impact on the European economy”19. Overall, the features that characterise open source software20 are the free access and use of software, the freedom to use the program for every purpose (commercial or not), the freedom to make and distribute copies, as well as the freedom to modify the program and distribute the modified program.

Different OSS licences exist, with differences relating mainly to the freedom that is provided to the licensee regarding the derivative works. In general, two types of licences can be distinguished: "permissive" licences that allow to use the software in any way the recipient chooses21, and "restrictive" licences (also called "copyleft licences") that are based on the principle of reciprocity, according to which the derivative work of the licensee must be licensed under the same licence22.

Although OSS licences are generally considered to be compatible with copyright law system, some important issues regarding copyright rules are raised. One such issue is that most of the OSS licences are worded under US law, which could be a source of legal uncertainty in Europe, since intellectual property regimes in Europe and the United States are different. According to the LEGALIST project's findings23 "more European modeled licenses should be considered so as to adapt OSS license terms to

17 Submission by the Authors’ Licensing & Collecting Society to the All Party Internet Group Inquiry into Digital Rights Management, 17th January 2006
18 Intellectual property guidelines, version 1.0, edited by Minerva EC Working Group, September 2008, p. 34
19 i2010 Midterm Review, (COM/2008/199) p. 27
20 Report in legal issues on Open Source Software, LEGALIST, Issue date: 07/06/2005, p. 15
21 Examples: the BSD, MIT and Apache licenses
22 Examples: the GNU Public License (GPL), European Union Public License (EUPL) and Mozilla Public License (MPL)
23 Legal Issues in Open Source Software, LEGALIST, Issue date: 07/06/2005, p. 32
the European law. Another important issue, particularly within business environments, is the possibility that source code under a restrictive licence would "contaminate" a company's proprietary source code, due to the reciprocal nature of restrictive licences and the wide interpretation given to derivative works. Although no case law is known in this regard, this issue causes a significant amount of companies to refrain from (re)using open source software.

1.2. The copyright infringements problem

1.2.1. The stakeholders' perception of copyright infringements in the digital environment

Reasons – Digital copyright infringements (often called "digital piracy") flourish due to the low cost of reproduction and distribution, the quality of digital copies (which is typically identical to the quality of the original work), increased availability of broadband technology, the availability of many new consumer devices that can process and store large amounts of digital data (pc's, netbooks, MP3 players, ebook readers, digital VCRs, ...), the ubiquitous availability of source materials, the limited amount of legal alternatives, and the many editing possibilities offered by modern software.

User perception – One of the most remarkable characteristics of the copyright infringement phenomenon is the fact that it is often not perceived as un-ethical. The mechanisms used in certain types of digital pirated content could indeed lead to the perception that "supplying digital piracy might not be an illicit or blameworthy activity, especially as a significant part of the exchanges of pirated digital products occur without profit motives which can be perceived as a socially acceptable 'sharing'". Studies have mentioned that consuming pirated digital content is considered as normal by many users, and treated differently than other infringements of the law: it "is not a massive criminal conspiracy, but rather the collective actions of millions otherwise law-abiding Internet users of all ages who have grown accustomed to the culture of free content that is the hallmark of the Internet".

Infringing users defend their conduit with varying arguments, such as:

24 Taking for example the European Union Public License. The European Commission approved the English, French and German versions of the EUPL (v.1.0) on 9 January 2007. By a second Decision of 9 January 2008, the European Commission validated the EUPL (v.1.0) in all the other official languages, in respect of the principle of linguistic diversity of the European Union, as recognised by Article 22 of the Charter of Fundamental Rights. By a third Decision of 9 January 2009, the European Commission adopted a revised version of the Licence while at the same time validated it in all the official languages (EUPL v.1.1). Available at http://ec.europa.eu/idabc/eupl

25 See Piracy of digital content, Chapter 2

26 Ibid, p. 13

27 Ibid, p. 49


29 Confronting Digital Piracy, Intellectual Property Protection in the Internet Era, Shane Ham and Robert D. Atkinson, Progressive Policy Institute, available at www.ppionline.org/documents/Digital_Copyright_1903.pdf, p. 2. According to the writers ‘the justification of this attitude can be found in more than one reason; Firstly because there is a strong belief among users according to which content provided by Internet is free while the same content is paid in the offline world. Secondly, there is another mistaken belief related mostly to consumer-oriented media products that ties the content and the media together allowing consumers to believe that media itself is the expensive item while content embodied is an unlimited resource that can be taken for free, leading users to a misconception at least as far as copyright is related. Finally, the factor of anonymity of the Internet fosters piracy culture as the reduced detection risks means that even those consumers that recognize the illegal character, will conduct copyright infringement’, p. 7

30 See J. GANTZ and J.B. ROCHESTER, Pirates of the digital millennium, p. 78-88
Digital infringements are more like "obtaining" instead of stealing, because no physical objects are actually taken away from their owners.

"Illegal downloading is a minor issue; declining CD sales are self-inflicted by the record industry, which responds too slowly to changing habits of users."

"Record companies rip off artists."

"Consumers or minors are never prosecuted, so can freely pirate."

"If they don't want me to download, then why do I have the software and hardware with which to do it?"

"It's mine. I bought it, and I can make copies for myself if I want to."

"Products are overpriced and sold by greedy megacorporations."

Rightholders perception – Contrary to the users, digital copyright infringements are considered as very severe from the online content industry, since they cause great injuries to the interests and profits of the online content industry. Business stakeholders emphasize that copyright infringements – and particularly the existence of peer-to-peer file sharing networks – constitute "the single most important obstacle to further online dissemination of works in Europe".

1.2.2. The treatment of digital copyright infringements

Different treatment – The 2009 OECD Document on digital copyright infringements notes that the lack of a common definition of "digital piracy" / digital copyright infringements results in a significantly different treatment in different jurisdictions, where different exceptions to the rightholder's rights apply (private, domestic use etc). Accordingly, what is in one jurisdiction considered illegal may be considered legitimate in another. There are also many differences from a procedural point of view: in some jurisdictions, copyright infringements are treated as a civil offense, while in others they are treated as a criminal offense.

Reasons – The "different speeds" at which Member States deal with copyright infringements is a result of the fundamental differences in civil and criminal procedure law, an area that is even less harmonised than substantive copyright law. This disparity of regulatory regimes in various European Member States has been characterised as an issue of primary importance by stakeholders.

Evolving nature – The treatment of digital copyright infringements seems to be a continuously evolving phenomenon. Legal actions have extended to three different dimensions. Initially, copyright industry mainly initiated legal battles against file sharing software packages (such as Napster, KaZaA and Grokster). Afterwards, legal actions were also taken against individual users who uploaded copyright

---

33 Interactive Content and convergence : implications for the information society, October 2006, p. 49
34 Copyright and Digital Media in a Post- Napster World: International Supplement, Berkman Centre for Internet and Society, January 2005, p. 34
35 Interactive Content and convergence : implications for the information society, October 2006, p. 49
material on a large scale\textsuperscript{36}. The current efforts seem to be focused on policy options, such as the "three strikes down" laws and initiatives that are being considered across the EU, particularly in France.

**Prosecution of individuals** – While prosecution of individuals for digital copyright infringements have gained much media attention in the United States, lawsuits have also emerged in across Europe, although to a lesser degree.

\begin{quote}
In Spain, for example, there was the case of Sharemula.com, a website which published hyperlinks that enabled users to download movies, music and software\textsuperscript{37}. The case was brought to Court by the Anti-piracy Federation in 2006. In 2007, a Madrid Court dismissed the case (against fifteen individuals), underlining that neither the site nor its administrators had infringed any law and that the site included legal content. In the appeal procedure, the provincial Court of Madrid rejected all allegations, concluding that indexing such hyperlinks cannot be viewed as copyright infringement\textsuperscript{38}.

In Denmark, the International Federation of the Phonographic Industry (IFPI) brought a case against a man who shared around 13 000 music files on Direct Connect. IFPI had tracked illegal activity via an IP address linked to the man. In 2008, the appeal court ruled that no other person than the man concerned could have used the IP address and ordered him to pay 160 000 kroner in damages, and to delete the music files he obtained illegally\textsuperscript{39}.
\end{quote}

However, due to the lack of common definition of digital copyright infringement that has been previously described, as well as the non-harmonised approach of its treatment by the different Member States, it is not clear how the different Courts within the Member States will construe the facts in each diverse case. In addition, it is not easy for rightholders – especially in cases of massive infringements like for instance in P2P platforms – to turn against every single individual infringer. The effort and the time necessary to prosecute individuals in different countries may be too high and too costly to be worth the attempt. It is also very problematic to enforce Court decisions against individuals. In addition, as also stated in section 7.3.1 below, we do not believe that the solution to battle copyright infringements resides in criminalizing and prosecuting individuals. All of the above require the co-operation of the Member States for the uniform treatment of digital copyright infringements within the Single Market at a more centralized level in order to effectively tackle with the issue at stake without targeting only individual users (see also the relevant recommendations in section 7.3.1 below).

2. **Overview of the current legal framework**

This section 2 offers a “helicopter view” of the most pivotal provisions and regimes that have the greatest impact on today’s digital content issues.

2.1. **Overview of all EU legal instruments relating to digital content**

**First generation** – Digital content, copyright issues and related rights in the European Union are governed by legislation both at the EU level and the national level\textsuperscript{40}. Harmonisation between Member

\textsuperscript{36} BERKMAN CENTRE FOR INTERNET AND SOCIETY, Copyright and Digital Media in a Post-Napster World: International Supplement, January 2005, p. 30

\textsuperscript{37} Spain: Indexing torrent files is not copyright infringement available at http://www.edri.org/edrigram/number6.18/link-torrents-not-infringement

\textsuperscript{38} Ibid.

\textsuperscript{39} See http://torrentfreak.com/ifpi-wins-danish-file-sharing-case-081021/

\textsuperscript{40} Copyright and digital media in a post-napster world: International Supplement, Berkman Center for Internet & Society and GartnerG2, January 2005, p. 9
States was conducted between 1991 and 1996 as a result of several EU Directives which aimed at a vertical standardisation. This bulk of Directives included the Computer Programs Directive\(^\text{41}\), the Rental Right Directive\(^\text{42}\), the Satellite and Cable Directive\(^\text{43}\), the Term Directive\(^\text{44}\), the Database Directive\(^\text{45}\), the Artists’ Resale Rights Directive\(^\text{46}\) and the E-Commerce Directive\(^\text{47}\), all of which constitute the first generation of copyright directives.

**Second generation** – The first of the second generation European Commission Copyright Directives (and the most important, until today) piece of EU legislation regarding digital media and content is the Copyright Directive\(^\text{48}\) which came into force on the 22 June 2001 requiring transposition to the member states by 22 December 2002. After the Copyright Directive, the so-called “Enforcement Directive” came into force in 2004\(^\text{49}\).

**Other EU legal instruments** – Other relevant acts (binding and non binding) to digital content include the Directive on the Reuse of Public Sector Information\(^\text{50}\), the Audiovisual Media Services Directive\(^\text{51}\), the Directive on Copyright, Satellite Broadcasting and Cable Retransmission\(^\text{52}\), the “Echerer” Report of the European Parliament on a Community framework for collecting societies for authors’ rights\(^\text{53}\), the Commission Recommendation on Collective Cross-Border Management of Copyright and Related Rights for Legitimate Online Music Services\(^\text{54}\), the (results of the) monitoring of the Commission Recommendation 2005/737/EC of 18 October 2005 on collective cross-border management of copyright and related rights for legitimate online music services\(^\text{55}\), the Green Paper on Copyright in the Knowledge

---


\(^{54}\) Commission Recommendation of 18 May 2005 on collective cross-border management of copyright and related rights for legitimate online music services O J L 278/54, 21.10.2005

2.2. **Most important legal provisions**

Within the list of EU legal instruments, the following legal provisions and legal instruments are most relevant to the topic of digital content.

**Copyright Directive** – The Copyright Directive includes content provisions, as well as communications and information technology rules. It also refers to issues of access and use of content. The objectives of the Copyright Directive were, firstly, to adapt legislation on copyright and related rights so as to reflect technological developments, and, secondly, to transpose into community law the main international obligations arising from the two treaties on copyright and related rights adopted from the World Intellectual Property Organization.

In addition, the Copyright Directive aimed at harmonising the different copyright regimes within the European Union that were an obstacle to the Single Market. This harmonisation was expected to "lead to legal certainty so as to create a Single Market within which the competition would flourish" and, at the same time, "to promote substantial investment in creativity and innovation including network infrastructure which in turn will lead to growth and competitiveness of the European Industry across industrial and cultural sectors which will consequently create new jobs." According to recital 31, the Directive equally aimed to achieve "a fair balance of the rights and interests between the different

---

56 Green Paper on Copyright in the Knowledge Economy, COM(2008) 466/3
58 (COM/2008/199)
64 A more detailed analysis of the most significant legal instruments will follow in the next subparagraph
67 Copyright Directive, recital 1
68 Copyright Directive, recital 4
categories of right-holders, as well as between the different categories of right-holders and users of protected subject matter must be safeguarded”.

The most significant rules of the Copyright Directive regarding the horizontal harmonisation of national laws are the standardisation of the fundamental exclusive rights, the introduction of an exhaustive list of copyright exceptions of optional character and the implementation of rules regarding technical protection measures.

**Enforcement Directive** – The Enforcement Directive was adopted to reduce the inconsistencies existing in the enforcement means of different Member States, which “hampered the proper function of the Single Market since it was difficult to ensure equivalent protection of intellectual property throughout the European Community”. Therefore, its main goals are “to bring into line the enforcement measures across European Union with the purpose of approximating legislative systems in order to ensure a high, equivalent and homogenous level of protection for intellectual property in the Single Market” and “to create a level playing field for the enforcement of IP rights in the Member States”. Additional goals are the promotion of innovation and business competitiveness, the safeguarding of employment in Europe, the prevention of tax losses and destabilisation of the markets, the insurance of consumer protection and the maintenance of public order.

The Directive established a general framework for the exchange of information between national authorities. At the same time, its objective was to strengthen the defence of the rights of the right-holders and to protect users from unfair litigation. Also, it introduced the measures, the procedures and the remedies necessary to ensure the enforcement of intellectual property rights within the Single Market, and aimed at adopting effective means for presenting, obtaining and preserving evidence. Furthermore, it established provisional measures for the immediate termination of infringements, as well as procedures to prevent further infringements of intellectual property rights. At the same time, this Directive determined the damages and the corrective measures that could be enforced in case of an infringement.

**Satellite Broadcasting and Cable Retransmission Directive** – Recital 21 explains that the main objective of this Directive is “to ensure that protection for authors, performers, producers of phonograms and broadcasting organizations is accorded in all Member States and that this protection is not subject to a statutory licence system”. Moreover, in recital 33 it is stressed that “whereas minimum rules should be laid down in order to establish and guarantee free and uninterrupted cross-border broadcasting by...”

---

69 Copyright Directive, recital 31
70 reproduction right, right of communication to the public, right of making available to the public and distribution right
71 However, only one of the exceptions is mandatory (article 5 par.1 of the Copyright Directive); member states were free to adopt all or none of the rest of the exceptions included in this exhaustive list (article 5 pars 2-5 of the Copyright Directive)
73 Directive 2004/48/EC, o.c., recital 10
77 Ibid.
78 Ibid.
79 Enforcement Directive, article 1
80 Enforcement Directive, recital 20
81 Enforcement Directive, recital 22 and 24
satellite and simultaneous, unaltered cable retransmission of programmes broadcast from other Member States, on an essentially contractual basis”. Among the most important provisions regarding the function of the licensing methods are the extension of applicability of collective agreements to individual rightholders not represented by a collecting society under certain conditions (for broadcasting by satellite), the compulsory collective management of cable retransmission rights, the equal treatment for those rightholders that have not transferred the management of their rights to a collecting society compared to those represented by collecting societies, the legal presumption for the constitutional protection of the ownership, as well as the introduction of mediation system of general acceptance for the disagreement resolution.

Cross-border copyright management of music services – The 2005 Commission "Recommendation on collective cross-border management of copyright and related rights for legitimate online music services" 82 has a major policy impact, although it is not binding. As the online environment is multi-territorial by nature, the purpose of this sector-specific Recommendation was to create a licensing policy that would correspond to the ubiquity of the online world 83, in order to enhance legal certainty and to foster the development of legitimate online services.

More specifically, this Recommendation aims to develop effective structures for cross-border management of rights, by abolishing local factor hurdles (such as the residence or the nationality of the rightholder or the manager). According to the Recommendation, minimum protection provisions of rightholders should be incorporated either in contracts or in statutory membership rules in all categories of rights. In addition, the Single Market should be promoted by adopting rules that exclude discrimination on the grounds of residence, nationality and category of rightholder. Market fragmentation should be cured by modifying licensing structures in the online music sector. These objectives are to be achieved by promoting a regulatory environment that suits to the management of copyright and related rights for the provision of legitimate online music services at the Community level 84. Member States were invited to take the steps necessary to facilitate the growth of legitimate online services in the Community.

Green Paper on Copyright in the Knowledge Economy – The purpose of this (non-binding) green paper is to foster a debate on how knowledge for research, science and education can best be disseminated in the online environment 85. The Green Paper stipulates that a high level of copyright protection is pivotal for the proliferation of intellectual creation, since it provides the rightholders with a reward for their efforts and it promotes creativity and innovation. However, at the same time, it is recognised that due to the emergence of new ways of delivering digital content “it is necessary to allow consumers and researchers to access protected content” 86. In addition, it is underlined that some stakeholders claim that income is not distributed fairly between the different categories of rightholders despite the introduction of exclusive rights in the Copyright Directive. It also points out that the way that the exhaustive list of exceptions was drafted in the Copyright Directive led to different implementations of the provisions stipulated in the Directive. Finally, the Green Paper calls the stakeholders to comment on the issues raised by the document, taking into account the basic question whether a fair balance is

---

82 Commission Recommendation of 18 October 2005 on collective cross- border management of copyright and related rights for legitimate online music services, O J L 276/54, 21.10.2005
83 Recital 6
84 Paragraph 2 of the Recommendation
85 Green Paper on Copyright in the Knowledge Economy COM(2008) 466/3 p. 3
86 Ibid p. 4
currently achieved between the different categories of right-holders and users. Following the aforementioned Green Paper, a 2009 Communication from the Commission regarding "Copyright in the Knowledge Economy" was published. In this document it was stressed that during the Public Consultation on the Green Paper "[...] two divergent views emerged. Libraries, archives and universities favor the 'public interest' by advocating a more permissive copyright system. Publishers, collecting societies and other right holders argue that the best way to improve the dissemination of knowledge and provide users with increased and effective access to works is through licensing agreements". Apart form highlighting the problem, the Communication proceeded into presenting future steps to deal with the problems of the libraries and archives, of the orphan works, of teaching and research, of persons with disabilities and of the user- created content. This document concluded by mentioning that "[...] copyright policy must be geared toward meeting the challenges of the internet-based knowledge economy. Different interests have to be carefully balanced".

Creative Content Online in the Single Market – This Communication aimed at launching further actions to support the development of innovative business models and the deployment of cross-border delivery of diverse online creative content services. According to the Communication, the notion of creative content online is twofold: from the consumers' side, creative content online is equivalent to new ways to access and influence content available online. From the side of the companies, however, it equals to the possibility to offer new services and to develop new markets.

e-Content Plus Program – Decision 456/2005/EC established the e-Content Plus Program, and underscored the important values set by the European Union in relation to the new digital content environment (in line with the Lisbon strategic goals previously mentioned). This Program was created to fund the development of new concepts and tools, in order to make digital content in Europe more accessible, usable and exploitable — taking into account the importance of the characteristics of digital content (accessibility, re-usability, exploitability) to the new knowledge-based economy.

The Decision held that "the shift to the digital based economy, prompted by new goods and services, will be a powerful engine for growth and competitiveness". At the same time, it recognised that "the demand for quality digital content in Europe with balanced access and user rights, by a broad community be they citizens in society, students, researchers, SMEs and other business users, or people with special needs wishing to augment their knowledge, or 're-users' wishing to exploit digital content resources to create services, is increasingly apparent". In addition, it was stated that "access, use and distribution of digital content would be enhanced by improving interoperability at the service level". Although the e-

---

87 The full list of the relevant responses can be found at http://circa.europa.eu/Public/irc/markt/markt_consultations/library?l=/copyright_neighbouring/consultation__copyright&vm=detailed&sb=Title.
88 COM (2009) 532 final, p. 4
89 COM (2009) 532 final, p. 10
91 COM (2007) 836 on Creative Content Online in the Single market, 3/01/2008, p. 3
92 Ibid., p. 2
94 Ibid., recital 3
95 Ibid., recital 5
96 Ibid., recital 8
Content Plus Program has expired on December 31st 2008, the actions to make digital content in Europe more accessible, usable and exploitable will be continued.

**ICT Policy Support Program** – The Information and Communications Technologies (ICT) Policy Support Program, one of three specific programs implemented through Decision no 1639/2006 establishing a competitiveness and Innovation Framework Program (2007-2013) was adopted to stimulate innovation and competitiveness, and to accelerate the development of a sustainable information society. It supports activities to enhance innovation and implementation of ICT based services and it promotes the exploitation of digital content by citizens, governments and businesses.

**International legal instruments** – In addition to EU-level legislation, there is a set of international treaties that establish standards for copyright protection, such as the Berne Convention for the Protection of Literary and Artistic Rights, the Rome Convention for the protection of Performers, Producers of Phonograms and Broadcasting Organizations, the Universal Copyright Convention and the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty.

The treaties have been used by national Courts to interpret national law. However, Courts have used many diverse ways to interpret the local transposition of the legislative provisions. In section 4.1.3 below, an indicative reference in some important and interesting cases is made to depict how the relevant provisions have been construed by the Courts in different Member States, and to delineate how significant Court decisions are for the establishment of the Single Market for digital content.

3. **Key issues in the current EU legal instruments**

3.1. **Gaps**

**Lack of a single standard of originality** – Although the Copyright Directive was aimed at harmonising the range of exclusive rights for digital works, it did not adopt a common definition of the standard of originality for the work under protection. Hence, Member States are free to uphold their own regime of originality standards for copyright protection in the information society under the copyright systems that they traditionally follow. In practice, this means that a work that may be protected under copyright law in one Member State may not be protected in another Member State. This lack of common originality standards in relation to the digital content could create obstacles in the function of the Single Market, since it leads to discrepancies between the legal regimes of the different Member States.

The Europeana project (see also the detailed discussion below) constitutes a practical example of the consequences of the lack of a single standard of originality. As part of this project, objects in the public domain are digitised, in order to make them available on the Europeana website. However, in some Member States, when public domain items are digitised, the digitising company could claim a new copyright originated from the digitisation, even when no creative efforts are employed during the digitisation process.

97 O J L 310/15 9.11.2006
98 ICT PSP work programme 2009, p. 4
102 Ibid.
Applicable law & competent court – The Copyright Directive does not deal with the topic of choice of law or with the competent court. This creates legal uncertainty, as it is not always predictable in advance which law or court shall apply, which in turn could impede cross border investments from the rightholder.

For example, in case of a copyright infringement in the offline environment, the applicable law is the law of the country for which protection is sought under Article 5 (2) of the Berne Convention. However, in an online context, the applicable law is either the law of the country where the unauthorised uploading ("copying") of the work takes place, or the law of the country where the work is accessed or downloaded without prior authorisation from the rightholder.\(^{104}\)

Absence of segmentation-preventing measures outside online music\(^{105}\) – The lack of a harmonised method of copyright management throughout the Member States can lead to segmentation of the Single Market. However, this issue has only been contemplated in relation to online music. The (non-binding) Commission Recommendation\(^{106}\) of 2005 aims to provide guidelines to cure market fragmentation, by introducing a modification of licensing structures in the online music sector. In addition, Member States were invited to take the steps necessary to facilitate the growth of legitimate online services in the Community, by promoting a better regulatory environment. However, these provisions only apply to online music, and do not extend to other types of digital copyrighted content disseminated online, and are not mandatory.

**Practical example: online licensing across Europe.** An major social community platform wanted to secure the necessary rights from the major Belgian musical rightholders association (SABAM), for using musical tracks on its website. However, during the contractual discussions with SABAM, it became clear that – although SABAM has mutual agreements with many similar organisations in other Member States and presents itself as a "one stop shop" – SABAM can only clear rights for service providers established in Belgium. Consequently, the social community platform needs to negotiate separately with each rightholder association of each Member State. This constitutes an important impediment for a platform that simultaneously targets most European Member States.

Exhaustion principle applying only to physical media – Article 4 of the Copyright Directive stipulates that the exhaustion principle applies to physical media ("original of a work or copies") incorporating the protected work. Recitals 28 and 29 further explain that "the first sale principle of the original of a work or copies thereof by the right-holder or with his consent in the Community, exhausts the right to control the release in the Community of a work incorporated in a tangible tool". This wording limits the principle of exhaustion to tangible goods only, excluding on-line services and intangible goods that incorporate digital content.

Getting legal certainty to reuse content – Copyright emerges without any formalities: although some countries used to require rightholders to register their works in order to receive protection, these formalities have been abolished. In the offline world, "the abolishment of formalities (meaning registration or any mark of the created content) before the development of digital technologies was considered as a positive step since it removed a burden from those who wanted to create content by eliminating requirements for work protection"\(^{107}\).

---

\(^{104}\) P. TORREMANS, *Private International Law aspects of IP - Internet Disputes*, p. 245

\(^{105}\) G. MAZZIOTTI, o.c., p. 68

\(^{106}\) Commission Recommendation of 18 October 2005 on collective cross-border management of copyright and related rights for legitimate online music services, o.c., p. 54

\(^{107}\) G. MAZZIOTTI, o.c., p.53
Even so, the lack of formalities often makes it difficult for someone who wants to use an existing work to find the rightholder and to obtain the permission required.

For example, if someone would like to reuse a picture on a random website, it will often not be clear who is the rightholder of this picture (see also analysis on the orphan work issue in section 3.7.5 below). Due to the ever-increasing amount of copying and reuse of content on the Internet, it is even difficult on photo and video sharing websites that explicitly attribute ownership (such as Flickr, YouTube or stock.xchng) to receive certainty that content is really owned by the alleged rightholder, and whether such person's permission suffices for reuse.

This “gap” in the current legal rules could lead to the limitation of creativity, since those willing to develop digital content may find it difficult to build upon previous works that are not registered or recorded in any repository (see also the discussion in section 7.2.5 below).

3.2. Ambiguities

Some of the general terms used in the Directives are drafted in a rather general language, are vague and are open to different interpretations. The vagueness of these expressions prevents clear understanding of the actual rights and the content of the rights. This issue is further aggravated due to the fact that the market is reluctant to seek clarification of the legal situation through Courts because of the cost and the time included in a Court decision.

Independent economic significance – One characteristic example is the criterion of "no independent economic significance". The Copyright Directive does not include any specific guidelines on what constitutes "independent economic significance", which creates ambiguity, in particular when combined with the broad scope of the reproduction right.

Lawful use – Another example is the expression "lawful use" in article 5.1.b, which is open to diverse interpretations because the lawfulness of the use rests in criteria found outside of article 5.1 itself. According to recital 33 of the Copyright Directive, a use should be considered lawful where it is authorised by the right-holder or not restricted by law. However, this explanation still leaves a margin of uncertainty since it is not clear whether it refers to copyright limitations or to any limitation of the restrictions imposed by the copyright regime. Furthermore, the two criteria used in recital 33 may in some cases contradict each other. The use of the word "or" instead of the word "and" could lead to the interpretation that the will of the right-holder is equal to the provisions set by law.

Adequate legal protection – Yet another example of ambiguous wording is found in articles 6.1 and 6.2 of the Copyright Directive. Here, the ambiguity resides in what constitutes "adequate legal protection", who is entitled to invoke it, when does a device have only a limited commercially significant purpose or

---

108 This issue is further discussed in section 7.2.5
111 article 5.1 of the Copyright Directive
112 Study on the implementation and effect in Member States’ laws of the Directive 2001/29EC on the harmonisation of certain aspects of copyright and related rights in the information society, final report, Institute for Information Law, February 2007, p. 50
114 Study on the implementation and effect in Member States’ laws of the directive 2001/29/EC, o.c., p. 48
115 Ibid., p. 76
use other than to circumvent, etc. According to article 6.3 of the Copyright Directive, all the measures mentioned are deemed "effective technological measures" without any further prerequisites.

**Scope of private copying exception** – Member States are not allowed to adopt exceptions that could allow private copying by commercial enterprises or legal entities, even if there is no commercial purpose included. It is not clear, however, whether the private copying exception should be limited to copies made by the beneficiary himself; article 5.2.b does not clearly indicate whether Member States can allow the third parties to actually produce the digital copies. A legal entity may thus rely on the private copying exception provided that its service constitutes some form of agency.

### 3.3. Unbalanced provisions

**Lack of harmonised exceptions and limitations** – Article 5 of the Copyright Directive provides ample discretionary margin to the Member States to decide if and how to implement the exceptions and limitations set forth. The lack of homogeneity throughout limitations and exceptions of article 5 is a result of two factors: the optional character of the exceptions, and the actual way that Member States have implemented those exceptions and limitations into their national laws. In the 2008 Green Paper it was mentioned that "the approach chosen by the drafters has left Member States a great deal of flexibility in implementing the exceptions contained in the Directive.

The disparities in the legislation of Member States could lead to the adoption of standard terms and conditions with dubious legal validity throughout the Single Market. This is a highly controversial issue, since there exist many different opinions in relation to whether it is necessary or not to alter the existing status of the limitations and exceptions regime established in the Copyright Directive (see also the discussion below).

**Different sector specific approaches for the private use exceptions** – Article 5.2 of the Copyright Directive introduces an exhaustive list of exceptions to the reproduction right that can be implemented by Member States. This list of exceptions is not obligatory, so that Member States can choose whether to implement or not any (or none) of them.

The Database Directive and Computer Programme Directive take a different approach. Article 6.1 of the Database Directive lays down that "(t)he performance by the lawful user of a database or of a copy thereof of any of the acts listed in Article 5 which is necessary for the purposes of access to the contents of the databases and normal use of the contents by the lawful user shall not require the authorization of the author of the database. Where the lawful user is authorized to use only part of the database, this provision shall apply only to that part". In addition, article 5.2 of the Computer Programme Directive.

---

116 Ibid., p. 112
117 Copyright law and consumer protection, European Consumer Law Group, February 2005, p. 11
119 "firstly, the aforementioned article uses a language that is not binding for the member states (‘may provide for exceptions and limitations’) and secondly it omits to lay down strict rules that member states are expected to transpose into their legal system”.
120 Study on the implementation and effect in Member States’ laws of the directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society, final report, Institute for Information Law, February 2007, p. 53
121 Green Paper on Copyright in the Knowledge Economy COM(2008) 466/3 , p. 5
permits a person that is entitled to use a computer program to make a back-up copy, so far as it is necessary for that use. Hence, in the provisions set in the Computer Programme Directive and the Database Directive, these acts are not considered as "exceptions" to copyright, but instead as rights of the user that cannot be circumvented by contract. Moreover, the provisions of the Computer Programme and the Database Directives are mandatory for all Member States.

**Broadness of reproduction rights** – The reproduction rights included in the Copyright Directive have been criticised as being overly broad and overlapping with the right of communication to the public.\(^{123}\)

> Nevertheless, the reproduction right and the right of communication to the public are strictly separated in most contracting processes. For example, in order to license online music, most online forms of dissemination require the simultaneous clearance of both rights. This significantly complicates the licensing process.\(^{124}\)

The broad scope of the reproduction right practically extends to all parties involved in the dissemination and use of the online digital content. This way, the right of reproduction covers any use of a work or other subject matter, even where "similar acts of use in the analogue world (such as receiving a television signal or reading a book) would fall well outside the scope of what intellectual property aims to protect".\(^{125}\)

The exception introduced by article 5.1 of the Copyright Directive has set some limitations to the reproduction right, by imposing an obligatory exception for transient and incidental reproduction acts. However, this exception does not alleviate the overlap of the reproduction right with the right of communication to the public and the right of making available to the public.

The extensive scope of the reproduction rights expands liability for copyright infringement to more parties, so that – compared to analogue works – more authorisation actions are required for the use of digital content.\(^{126}\) This could prevent parties in the Single Market from engaging in acts in the online environment, while the same acts would not be restricted in the offline environment. As a result, business ventures dealing with digital content will require more time and money to acquire all necessary permissions.

**Broadness of the scope of the Enforcement Directive** – The IP enforcement regime of the Enforcement Directive is broad, covering even minor, unintentional and non-commercial infringements. Its broadness stems from the fact that it applies to any infringement of IP rights as provided by community law and national law of the Member States.\(^{127}\) Article 2 of the Enforcement Directive stipulates that " [...] this directive shall apply [...] to any infringement of intellectual property right as provided for by Community law or/and by the national law of the Member State concerned". This article has been criticised for the lack of distinction between infringements on a commercial scale and

---

\(^{123}\) Study on the implementation and effect in Member States' laws of the directive 2001/29/EC, o.c., p. 24


\(^{125}\) Ibid.

\(^{126}\) Study on the implementation and effect in Member States' laws of the directive 2001/29/EC, o.c., p. 39

\(^{127}\) Copyright and Digital media in a post – Napster world: International Supplement, Berkman Center for Internet and Society and GartnerG2, January 2005, p. 11
infringements on a personal scale\textsuperscript{128}, and for the “absence of guidance on the scope of intellectual property rights that enforcement measures are to be directed towards”\textsuperscript{129}.

The lack of distinction between commercial and private scale infringement has particularly raised concerns among consumers. These concerns are based on the opinion that the Enforcement Directive treats all infringements with similar seriousness, while in reality the infringements may significantly differ\textsuperscript{130}. As a result, some critics state that civil liberties in Europe were attacked by “a legal instrument treating average consumers who accidentally infringe copyright with the same toughness as it does for commercial counterfeiters”\textsuperscript{131}. Some have even proposed \textsuperscript{132} that the scope of the Enforcement Directive should be limited to intentional commercial infringements only\textsuperscript{133}.

The Enforcement Directive has therefore been criticised by some members of the market for rendering the business environment unfriendly for certain ventures, such as phone companies and internet access providers. Contrary to the eCommerce Directive, which limits the liability of some intermediaries, the Enforcement Directive enables judicial authorities to order the disclosure of information on the origin and distribution of infringing content\textsuperscript{134}, as well as to order interlocutory injunction against them\textsuperscript{135}, including seizure of equipment used for the distribution\textsuperscript{136}. As a result, the question arises to which extent the Enforcement Directive can be reconciled with the intent to promote innovation and investment in the online Single Market.

Also internet access providers are concerned about the permission granted by the Enforcement Directive to confiscate and destroy their equipment and servers without a previous Court hearing for the allegedly infringing activity of their customers\textsuperscript{137}. Thus, as identified by them, “a hostile business environment is created where threat of liability is likely to impede further investment on digital content sector”.

\textsuperscript{128} Only some articles are limited to “commercial scale” infringements: articles 6.2, 8.1 and 9.2 (see recital 14)
\textsuperscript{130} Compare, for example, a teenager who illegally downloads a work and a large company that repeatedly downloads copyrighted material.
\textsuperscript{131} EU passes dangerous IP Law, Despite MEP's Conflict of Interest "Midnight Knocks" by Recording Industry Executives Get Go-Ahead, available at http://ipjustice.org/ CODE/release20040309_en.shtml
\textsuperscript{132} IP Justice is an international civil liberties organisation that promotes balanced intellectual property laws, available at www.ipjustice.org
\textsuperscript{133} Top 8 reasons to reject the EU IP Rights Enforcement Directive, available at http://ipjustice.org/ CODE/release20040302_en.shtml
\textsuperscript{137} EU passes Dangerous IP Law, Despite MEP's Conflict of interest "Midnight Knocks" by Recording Industry Executives get Go-Ahead, o.c.
3.4. **Obstacles for the Single Market**

The different rules that have been adopted by the Member States constitute as an obstacle to the further development of cross border services within the Single Market. The level of knowledge necessary for the conclusion of one simple agreement per territory is in many cases too high to make the effort for commercial ventures within the Single Market worthwhile. The lack of actual harmonisation creates the requirement of extensive legal research before entering into a market or service, which in turn raises procedural and transactional costs for the interested parties. However, territorial restrictions are often also the deliberate result of commercial decisions by rightholders and providers of audiovisual media services (even though authors often grant worldwide rights to their publishers, collecting societies or producers).\(^{138}\)

This lack of harmonisation, combined with the uncertainty regarding the scope of limitations, obliges parties to negotiate the terms of use of the protected work with every rightholder and in every territory (which in practice favours the strongest contractual party). Enterprises that are willing to undertake cross-country business ventures need costly and time consuming expert services in order to enter into agreements outside of their territory. For example, in the field of online music, the public performance rights (right to make available) are licensed on a national basis.\(^{139}\)

As acknowledged by Commissioner Reding, *“Europe’s content sector is suffering under its regulatory fragmentation, under its lack of clear, consumer-friendly rules for accessing copyright-protected online content, and serious disagreements between stakeholders about fundamental issues such as levies and private copying”*.\(^{140}\) It is therefore not surprising that the European Commission has made the online single market the key priority for the post-i2010 era.

This is particularly burdensome for SMEs and universities,\(^{141}\) which often cannot afford such costly services. Consequently, SMEs could be impeded from entering into contractual agreements in a different territory since they lack the legal expertise to bargain with a stronger contractual party (in case of a B2B transaction). Nevertheless, according to some stakeholders, the overall harmonisation conducted so far is sufficient,\(^{142}\) so that attention should be concentrated to the implementation and enforcement of the already developed framework.

The variety of exceptions and limitations has particularly raised concerns about the use of DRMs across the Single Market. Due to the different implementations adopted in each Member State, a rightholder who wishes to commercially exploit his digital work in the online environment would be obliged to program these protection technologies in such a way so as to meet the requirements set in every different local legal regime. Hence, those rightholders that are not able to undertake the cost necessary for a country-by-country analysis are obliged to opt for one of the following: to adopt standard

---

139 Ibid., p. 6  
141 See the Communication from the Commission regarding Copyright in the Knowledge Economy, COM (2009) 532 final, page 7: “[Libraries and universities] contend that trans-national licensing within the EU is difficult or impossible. Libraries and universities assert that it would be more practical and efficient to have one central organisation to grant a wide range of online rights with respect to digital material.”  
142 Ibid.
terms and conditions drafted according to their local laws, regardless the risk of being illegal in another Member State or to transact on line only with the local users, or to completely avoid on line transactions.

3.5. Issues relating to TPMs

Lack of guidelines – Due to the ease with which digital works can be copied, rightholders not only rely on the law itself to prevent illegal copying, but also rely on technological protection measures (“TPMs”), such as Digital Rights Management (“DRM”), to prevent/restrict unauthorised acts. However, the Copyright Directive does not provide specific guidelines for the implementation of TPMs. For that reason "there is a great variety to the scope of protection afforded to them in each Member State". Also, "since art. 6.1 of the Directive 2001/29/EC lays down that Member States should provide adequate legal protection without further indicating the nature of this protection, this permits a variety of legislative solutions to be adopted from each Member State ranging from civil to criminal law".

Lack of explicit distinction between access control and copy control – In the online world, digital copyrighted works are usually governed by the terms of a licensing agreement. In addition, they can be protected by technological protection measures (“TPMs”), which are measures designed to prevent/restrict acts that are not authorised by rightholders. The use of TPMs is encouraged by the Copyright Directive, as it confers a new right to the rightholders: the control of access to their digital work through TPMs.

Both methods are used to define permissible uses, and to prohibit users from reproducing works and communicating them to the public. It has been observed that “right-holders of the content seem to be satisfied by their complete control of the use of the copyrighted work which practically leads to the abolishment of the reasonable expectations of the consumers regarding certain acts (for example the number of the permitted downloads and the right to make a back up of the file)".

The Copyright Directive does not distinguish between "access control" and "copy control", granting equal legal treatment to both "methods" of control. The most important consequence of this lack of distinction is that rightholders using TPMs are both entitled to control access to their digital work, and to control the copies of the work. In other words, access control is equivalent to copy control. Copyright protection is therefore extended beyond the protection bestowed to analogue works.

Possible circumvention of copyright provisions by TPMs – Article 6 of the Copyright Directive distinguishes between a rightholder's ability to "control" use and the user's right to "gain access". The rightholder is allowed to restrict access to the work, based not on copyright law itself, but on the technology (particularly TPMs) and the contractual freedom. HEIDE has pointed out that "the reliance on this access control power is not reliance on any legal mechanism and in so relying on a different 'rights structure' does not require adherence to any exception limitations that is required under that legal structure […] where copyright law is not preferred, there can be no reliance upon its exceptions." 

---

143 Study on the implementation and effect in Member States’ laws of the directive 2001/29/EC, o.c., p. 97
144 Ibid.
145 Study on the implementation and effect in Member States’ laws of the Copyright Directive, o.c., p. 168
146 Study on the implementation and effect in Member States’ laws of the Copyright Directive, o.c., p. 169
148 Ibid.
150 Ibid.
other words, the attention of the legal protection is shifting from the copyrighted work to the technology that protects it.

In addition, the Copyright Directive does not create a clear link between the notion of "lawful use" and the beneficiary of the copyright exceptions. The intention of article 6.4 is to secure that the beneficiaries of certain exceptions and limitations will be actually at the legal position to exercise those rights. However, the fact that the Member States are not obliged to implement the exceptions of article 5 of the Directive in their national laws (all but one) reduces the practical impact of article 6.4, since no such rights may exist. Hence, article 6.4 only creates obligations when Member States decide to provide the exceptions and limitations in their national law. Thus it has been commented that "by not providing the discretionary exceptions and limitations of art 5 (2) (3) of the Directive, Member States can easily prevent the objective of the provision from being established".

Moreover, copyright exceptions can be contracted out. According to some authors "the all lawful uses of article 5 of the [Copyright Directive] can be restricted by the application of DRMs which ban access to the copyrighted material to unauthorized users regardless of the lawfulness of their purpose". Article 6.4 of the Copyright Directive holds that where TPMs control access and use of copyrighted work, only those users that have legal access to the protected work can exercise copyright exceptions. Hence, it has been observed that "through the use of technological measures and licenses, rightholders can easily prohibit acts that are not restricted by law".

In this way, it seems that restrictions to lawful uses through contractual consent and access control technologies could, in some cases, be "legitimised". This was also pointed out by the Study on the Implementation and Effect of the Enforcement Directive: "a rule of precedence has been established between contractual arrangements and the application of technological protection measures". Some arguments also claim that the interpretation of article 6.4 create a two-track policy "which has practically silenced the lawful use of copyrighted works in an online environment in many countries".

**TPM exceptions do not apply to online services under "agreed" contractual terms** – Member States must ensure that the various exceptions for beneficiaries that are set forth in article 5 of the Copyright Directive are respected, even when TPMs are applied by rightholders. However, according to article 6.4 of the Copyright Directive this should not be ensured for "works or other subject matter made available to the public on agreed contractual terms in such a way that members of the public may access them from a place and at a time individually chosen by them".

---

151 G. MAZZIOTTI, EU Digital Copyright and the end user, Springer, 2008, p. 86
152 W. BASLER, "Technological Protection Measures in the United States, the European Union and Germany: How much fair use do we need in the 'Digital World'", Virginia Journal of Law and Technology, fall 2003, vol 8, no 13, p.16
154 G. MAZZIOTTI, EU Digital Copyright and the end user, Springer, 2008, p.87
155 EU Digital Copyright and the end user, o.c., p.87
156 Study on the implementation and effect in Member States’ laws of the directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society, final report, Institute for Information Law, February 2007, p. 152
158 e.g., using protected works for private use, teaching or scientific research
159 Article 6.4
This wording creates ambiguity for interactive and on-demand digital services. Although the majority of these services are offered under a non-negotiated licence\textsuperscript{160}, nevertheless they could still fall under the definition of "agreed contractual terms" because the user usually has to accept the terms before using the content (e.g., by clicking on an "I accept" button). In this way, the provision of article 6.4 could leave out of protection most of the online digital work, allowing TPMs to abolish the exceptions and limitations in article 5 of the Copyright Directive.

This discrepancy could lead to the development of a dual analogue v. digital system. Some narrators have pointed out that "as soon as more and more material becomes available through internet (online distribution), technical measures will permit exceptions of great importance to be abandoned"\textsuperscript{161}. Contractual terms set by the rightholder could thus force the user to abandon his lawful uses of digital works, while this is not allowed in the analogue environment. This inequality between the analogue and the digital environment could impede the dissemination of digital content within the Single Marketplace.

**Reasons for applying TPMs** – Articles 6.1 and 6.2 of the Copyright Directive do not differentiate between the reasons for applying TPMs and the reasons for circumventing them. This could raise concerns as regards the fair balance between the interests of the user and the interests of the rightholder. According to the study on the implementation and effect of the Copyright Directive, this results in the situation where any act of circumvention is prohibited\textsuperscript{162}. Furthermore, TPMs are also used for reasons others than copyright protection, e.g. to protect market share, limit consumers to specific devices, etc. Although the anti-circumvention measures should have been restricted to copyright infringements, nevertheless their protection extends also to TPMs that are not used to protect copyrighted material.

**Circumvention for legitimate purposes** – Acts of circumvention done for legitimate purposes are not protected, so that "the protection conferred by art. 6 of the Directive 2001/29 seems to extend to non-restricted acts too"\textsuperscript{163}. This could also lead to efforts of distortion of competition by limiting the permitted consumer choices in device and content. In this regard, the European Consumer Law Group has declared that "although TPMs consist legitimate means to protect copyrighted works and enforce the relative intellectual property rules, nevertheless this should not happen at all cost"\textsuperscript{164}.

**TPMs and personal data protection** – TPMs have the ability to gather a great deal of data regarding the persons that purchase digital content, by tracing what a person reads, listens, his/her viewing habits, etc. Moreover, TPMs have the ability to "impose" on the user the obligation to give his consent to gathering his personal information, in order to allow him to view, use or in any other way utilise the protected work. The use of TPM technologies can therefore conflict with a user's data protection rights and privacy rights, by tracing the use of the protected work and monitoring a user's behaviour\textsuperscript{165}.

---

\textsuperscript{160} Study on the implementation and effect in Member States' laws of the directive 2001/29/EC, o.c., p. 126
\textsuperscript{161} G. MAZZIOTTI, EU Digital Copyright and the end user, Springer, 2008, p. 98
\textsuperscript{162} Study on the implementation and effect in Member States' laws of the directive 2001/29/EC, o.c., p. 114
\textsuperscript{163} Study on the implementation and effect in Member States' laws of the directive 2001/29/EC, o.c., p. 100
\textsuperscript{164} Copyright Law and Consumer Protection, o.c., p. 21
\textsuperscript{165} Giuseppe Mazziotti, EU Digital Copyright Law and End-User, Springer, 2008, p. 92
\textsuperscript{166} www.nytimes.com/2009/07/18/technology/companies/18amazon.html
Recital 57 of the Copyright Directive lays down that “these technical means, in their technical functions, should incorporate privacy safeguards in accordance with Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data”. However, the wording used in the recital only encourages – and does not mandate – the use of privacy enhancing technologies (PETs). The use of the word “should” (instead of “shall” or “must”) leaves the effective protection of personal data to the rightholders that employ DRMs. Furthermore, the reference to the data protection issues is only included in the recitals of the Copyright Directive, which demonstrates that the Copyright Directive omits to directly address the use of PETs. Therefore, “the effective availability and use of DRM technology may raise privacy concerns”.

Persons with disabilities – As pointed out by the Communication from the Commission on Copyright in the Knowledge Economy, TPMs are an additional obstacle towards making content available to persons with disabilities (only 5% of books published in Europe are converted into accessible formats), because they prevent the conversion into accessible formats of legally acquired works by organisations or individuals.

Adequate information – Another issue related to TPMs is that consumers fear that they are not always capable of knowing their possibilities “especially regarding to what they can or cannot do with their digital hardware and content”. They claim that in many instances they are not properly informed about the specific characteristics of a device and/or a work and for that reason their choice does not meet their expectations. They identify themselves as being the weaker party in a transaction since “they do not dispose any choice as to whether to accept or refuse the restrictive terms of use even if they are regarded as unfair”. In addition, although common use of information in the analogue world is permitted (such as sharing a CD with friends), these kind of activities are no longer permitted in the digital world.

3.6. Relation to the eCommerce Directive

The role of online intermediaries’ provider is not always clear. It is not clear to which extent the provisions of article 8.3 of the Copyright Directive conflicts with the prohibition of a general monitoring obligation set forth in articles 15 of the eCommerce Directive. This issue is being discussed in depth in section 4.6 of Chapter 6 (liability of online intermediaries).

---

168 Ibid.
169 Giuseppe Mazziotti, o.c., p. 34
171 Accommodating the needs of iConsumers: Making sure they get their money’s worth of digital entertainment, Guilbault L., 19 June 2008, Springer
172 Ibid.
173 Ibid.
3.7. Future-readiness and technological neutrality

3.7.1. Few exceptions fit properly in the digital environment

Even though the final text of the Copyright Directive includes a number of optional limitations, only a small number of those limitations were designed to fit properly in the digital environment (as it was then perceived): the private use exception\(^\text{175}\), the exception for acts of reproduction for libraries\(^\text{176}\), and the exception for research/private study terminals of publicly accessible establishments\(^\text{177 178}\). Still, even those exceptions have received criticism that they are not fit (or not fit anymore) with the current developments of the digital world.

Conversely, there are multiple exceptions and limitations in the Copyright Directive\(^\text{179}\) that are not relevant to the Single Market or/and do not foster the deployment of the dissemination of the digital content\(^\text{180}\). In this regards, the aim set by the Copyright Directive (namely to adopt rules relevant to digital content technological development), is not completely reached, since only a limited number of (optional) exceptions addresses the multiple challenges of the digital era as they were then identified.

Consequently, stakeholders have expressed the view "that the rights granted under the [Copyright Directive] do not actually initiate or promote the establishment of new innovative business models but that they contribute to the legitimization of the business models that were already in the market previous to the 2001 Directive"\(^\text{181}\). They claim that the Copyright Directive did not add much to the promotion of innovative business models and that this Directive was neutral as far as the establishment of new business models is concerned.

3.7.2. Future-readiness of exclusive rights, limitations and exceptions

While some legal provisions are sufficiently flexible to be adapted to future challenges, other provisions are less future-ready and raise concerns in relation to their ability to respond to the new technological challenges.

For example, the right of communication to the public\(^\text{182}\) is worded in such a way that it does not directly target specific technologies. The same is true for the right of making available to the public\(^\text{183}\). The criteria set forth in this article are technology neutral, while the requirement of access from a place and at a time individually chosen by the user covers shifting technological methods and the portability of

\(^{175}\) article 5.2.b
\(^{176}\) article 5.2.c
\(^{177}\) article 5.3.n
\(^{178}\) Study on the implementation and effect in Member States’ laws of the directive 2001/29/EC, o.c., p. 44
\(^{179}\) Such as those in articles 5.2.e, 5.3.e, 5.3.g, 5.3.h, 5.3.i and 5.3.j
\(^{180}\) Study on the implementation and effect in Member States’ laws of the directive 2001/29/EC, o.c., p. 46
\(^{181}\) Study on the implementation and effect in Member States’ laws of the directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society, final report, Institute for Information Law, February 2007, p. 73
\(^{182}\) article 3.1 Copyright Directive
\(^{183}\) article 3.2 Copyright Directive
the means used (pc, mobile phone etc). This way, this right does not discriminate against one or another type of technology used\textsuperscript{184}.

Conversely, the right of reproduction is not technologically neutral in its current wording. The provisions of article 5.1 Copyright Directive seem to have been written having in mind a specific technology\textsuperscript{185}, namely the one that allows internet access providers to operate. Most of the limitations and exceptions of the Copyright Directive are generally phrased in such a broad way that this could reassure their technological neutrality\textsuperscript{186}. However the exhaustive character of the list of exceptions and limitations contained in the Copyright Directive may pose some obstacles to the future readiness of the provisions stipulated in this Directive\textsuperscript{187}. By prohibiting other exceptions or/and limitations, new trends and technological developments that require those new exceptions will not be covered: "the exhaustive quality of the (exceptions and limitations') list raises questions [...] (since) Member States cannot anticipate the fast sociological and especially technological developments and revise exceptions accordingly. Consequently, great opportunities are lost on both sides (both right holders and users) as no flexibility is left to Member States"\textsuperscript{188}. Moreover many arguments have been raised by different stakeholders on whether some of these exceptions and limitations reflect the current situation of the digital environment and whether they are still able to cope with the advances of specific domains. The proponents of these arguments propose for an amendment of the exceptions and limitations regime of the Copyright Directive by altering or/and providing more clarifications to some of the exceptions and limitations. However, others are fully satisfied with the status quo created by the Copyright Directive (for further discussion on the exceptions and limitations see below).

\subsection*{3.7.3. Different sector specific rules?}

According to a 2006 Study \textsuperscript{189} "the role of information has been transformed to a sui generis commodity that led to the augmentation of the need for vast exchange of information and for more people to access the information. This fact means that so far as it is commercially viable and consumer desirable, content producers should be able to make distribution deals without excessive technical, legislative and regulatory obstacles". In order to accomplish this goal and to meet the objective to establish the transfer of knowledge as the "Fifth Freedom", it is necessary to guarantee the movement of knowledge within the Single Market for all types of information. It has been supported however by some stakeholders that the present set of legal rules does not sufficiently cover the needs of all types of information flow, so that different sector specific rules may be necessary for different categories of information.

\begin{quote}
Hence, for example, arguments were raised asking for "a partially distinct set of rules for scientific research, fostering wide and efficient dissemination, e.g. by securing competitive market conditions and
\end{quote}

\begin{itemize}
\item Study on the implementation and effect in Member States' laws of the directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society, final report, Institute for Information Law, February 2007, p. 75
\item Ibid.
\item This, however, does not apply to the exception in article 5.2.a (which specifically mentions reproductions on paper "or any similar medium") and in article 5.3.n, which refers to communication or making available "by dedicated terminals".
\item This has been identified as the lack of flexibility of the exhaustive exceptions and limitations lists to take account of technological developments and to foster innovation, available at http://ec.europa.eu/internal_market/copyright/docs/studies/ett2005imd195recast_report_2006.pdf - p. 7 as found in Google's Contribution to the European Commission public consultation on "Copyright in the Knowledge Society, p. 6
\item Green Paper Common Position Interdisciplinary Centre for Law and ICT – K.U.Leuven, p. 2
\item Interactive content and convergence: Implications for the Information Society, A study for the European Commission, (DG Information Society and Media, Final Report 2006), p. 27
\end{itemize}
thereby encouraging innovative dissemination models. Copyright law as part of these market conditions should provide for a wide array of limitations to copyright, keeping market entry barriers low for new providers and their technologies and avoiding that scientific knowledge becomes “privatised” by publishers”\(^\text{190}\).

The discussion on sector specific rules is closely related to the discussion on whether it is necessary or not to change the exceptions and limitations regime of the Copyright Directive. Sector specific rules may constitute an interesting alternative when no consensus can be reached among the different stakeholders on the modification of the current exceptions and limitations regime.

For example libraries and archives might request for a more updated legislation since it is felt that “the current exception, which only allows online dissemination of digitised content on the premises of the institution (“on site”) obviously hinders these organisations to fulfil their role in the 21st century information society”\(^\text{191}\).

The Commission has already adopted certain sector specific non mandatory rules and initiatives to provide guidance in particular subject-matters that are of high importance.

For instance, *digitisation of scientific work and material of cultural heritage* is considered as a very important issue since it will enable access and use of works through users’ personal computer. The idea of improving visibility of collections held by museums, archives and other institutions has been promoted by the Commission through the Digital Library Initiative (DLI) and other projects such as the Lund Digitisation Action Plan and The European Library\(^\text{192}\).

Part of the discussion regarding digital content refers to the *digitization of European Cultural Heritage*, meaning the digitisation and online accessibility of cultural material and digital preservation. Due to its importance, the Commission has proceeded to the Communication on the digitisation and online accessibility of cultural material and digital preservation\(^\text{193}\). As mentioned in recital 3 “the development of digitised material from libraries, archives and museums should be encouraged. The online accessibility of the material will make it possible for citizens throughout Europe to access and use it for leisure, studies or work. It will give Europe’s diverse and multilingual heritage a clear profile on the Internet. Moreover, the digitised material can be re-used in industries such as tourism and the education industry, as well as in new creative efforts. Member States are recommended to adopt national strategies for long term preservation and access to digital material.”

Moreover, the Commission issued the Communication on *scientific information in the digital age: access, dissemination and preservation*\(^\text{194}\), which stated: “this Communication’s objective is to signal the importance of and launch a policy process on (a) access to and dissemination of scientific information and (b) strategies for the preservation of scientific information across the Union”. For this reason the Communication announces a series of measures at the European level. This document also identifies issues and challenges of organisational, legal, technical and financial nature.

### 3.7.4. Is all content (still) equal in the digital era?

Under the current copyright rules, all copyrighted content is protected in the same way: even trivial original work is protected under copyright law. However, the ubiquity of the Internet and the increased dissemination of digital content have enhanced the content creation by internet users, and new tools have been developed that allow creating or reusing digital work easier and more cost effectively than ever before.

---

\(^{190}\) Comments by the MAX PLANCK INSTITUTE FOR INTELLECTUAL PROPERTY, COMPETITION AND TAX LAW, p. 4

\(^{191}\) Green Paper Common Position Interdisciplinary Centre for Law and ICT – K.U.Leuven, p. 3


\(^{193}\) C (2006) 3808 FINAL, 24.08.2006

\(^{194}\) Communication from the Commission to the European Parliament, the council and the European Economic and social committee on scientific information in the digital age:access, disseminationand preservation COM (2007) 56 FINAL 14.2.2007
Value-differentiated content – Most stakeholders will likely agree that not all user-created content holds the same value: there is very valuable content (with clear present or future commercial value, such as for example music and films), less valuable content and low-value content (such as for instance an SMS messages, messages sent in a social network, etc.). The question arises whether all this content should be treated the same way, particularly because the author does not always have the same intentions regarding the exploitation of his/her work. It could therefore be argued that the current legal regime, which obliges all digital user-created content to be treated in the same way regardless of its value and regardless of the intentions of the author, is not ready to meet these new trends195.

Collaborative content – A related issue is that copyrighted material is increasingly created in a collaborative way (e.g., wikis, open content such as Wikipedia, open source software, etc.). In such cases, it is difficult to identify the actual rightholders. Moreover, under the current legal rules of most Member States, dealing with co-ownership of intellectual property rights is a legal labyrinth. Not only does the "default regime" for co-ownership differ significantly among Member States, the legal rules on co-ownership of intellectual property rights are also not extensively developed in most Member States (they rely on a mix of general co-ownership rules and specific rules for some types of intellectual property rights).

3.7.5. Feasibility of clearing rights

The problem of locating the rightholders – According to the 2008 Green Paper on Copyright in the Knowledge Based Economy196 within the current legal framework "the obligation to clear rights before any transformative content can be made available can be perceived as a barrier to innovation in that it blocks new, potentially valuable works from being disseminated"197. The problem of locating the rightholder(s) of a work in order to ask for the permission to use or re-use it is very intense in the digital world, where in many instances it is not easy to identify the rightholders, due to various factors such as for instance the ubiquity of the Internet, the frequent use of pseudonyms, the anonymity of the users etc.

This is further aggravated due to the "orphan works" issue that arises when data on the author/rightholder(s) is simply missing or outdated, which is particularly problematic when a work has multiple authors. In these cases, it can be very costly and time consuming to find or to identify the rightholders in order to grant permission to exploit their work. In addition, users that use an orphan work are never sure whether they will be held liable for copyright infringement198.

The significance of this problem must not be underestimated. For example, as a result of the decay that is inherent to the physical properties of early twentieth century film, half of the movies made before 1950 cannot be recovered199. By sustaining a lack of incentive to initiate conservation efforts, the legal uncertainty with regard to orphan works may lead to the irretrievably loss of parts of our cultural heritage. It can be argued that solving the problem of orphan works would be beneficial for all stakeholders involved. Authors could use older works to create new value, rightholders may benefit from remuneration from a new source and more valuable content would be made available to consumers200.

195 For further discussion on this, matter see section 7.2.5 below
196 Green Paper on Copyright in the Knowledge Economy, COM(2008) 466/3 p. 19
197 Ibid.
198 Green Paper on Copyright in the Knowledge Economy, COM(2008) 466/3 p. 10
EU initiatives – In light of the above, the Commission adopted the (non-binding) Commission Recommendation of 24 August 2006 on the digitisation and online accessibility of cultural content and digital preservation, 2006/585/EC, L236/28, encouraging Member States to create mechanisms to facilitate the use of orphan works and to promote the availability of lists of known orphan works. Furthermore, a High Level Expert Group on Digital Libraries adopted a "Final Report on Digital Preservation, Orphan Works and Out of Print Works", and a (non-binding) memorandum of understanding on orphan works was signed by representatives of libraries, archives and rightholders.

The Digital Library Initiative – In the context of the i2010 Digital Libraries Initiative, an overall solution for the issue of orphan works was proposed. The aim of this proposal is to provide cultural institutions with the possibility to identify the digitisation status of a work, to gain access to it and to enable digitalization it if this has not already been done.

The proposal identifies three key issues in this respect:

- The establishment of sector-specific criteria for diligent search for rightholders to copyright works. By harmonising the search criteria throughout the Member States, searches in various Member States could be made subject to the principle of mutual recognition.
- The creation of one or more databases of orphan works. This would allow interested parties to make an assessment of the copyright restrictions resting on a particular work without having to re-initiate a thorough search for rightholders, and would consequently maximise the potential use and distribution of orphan works; and
- The development of a rights clearance mechanism to issue a licence to use an orphan work. Following a diligent search in accordance with the agreed upon criteria, and on the condition that no rightholder has been identified, such a mechanism should provide for the provision of non-exclusive licences to the work.

With regard to the rights clearance mechanism, various approaches could be adopted. The three main solutions that should be considered by the Member States are:

- The creation of an extended collective licensing mechanism. Such a mechanism would allow one or more institutions to grant licences that apply automatically to all rightholders in a given field, even if unknown or untraceable. In view of the pronounced presence of collective copyright organisations, this option is feasible in the European context. This is contrary to the United States, where collective copyright organisations are of less significance. In Denmark, Finland, Sweden and Hungary, such a system – although not specifically created to deal with the issue of orphan works – is already being used in this respect.

---


- **The grant of a non-exclusive licence by an independent body.** An alternative approach would be to allow an independent body to issue a non-exclusive licence after conducting a diligent search for the rightholders. This approach has been recommended by the Copyright Subgroup of the i2010 Digital Libraries High Level Expert Group. Under this setup, one or more “rights clearance centres” would be able to grant orphan works licences. For this purpose, Member States should encourage rightholders to vest licence-granting authority in such clearance centres. Licensing policies, criteria and fees should also be discussed with rightholders representatives, such as collective copyright organisations.

- **Creation of an exception to copyright.** In the UK Gowers Review of Intellectual Property, it was recommended to deal with the issue of orphan works through an amendment of the Copyright Directive. This would entail amending the Directive to include an exception which permits the use of genuine orphan works, provided the user has performed a reasonable search and, where possible, gives attribution. However, such an exception is currently contrary to the permissible exceptions set forth in the Copyright Directive, which are at present incompatible with a commercial orphan works exception.

Regardless of the option chosen, national solutions will need to take into account issues of mutual recognition in Member States to achieve the necessary cross-border effects. In accordance with the second key principle identified by the i2010 Digital Libraries Copyright Subgroup's, such efforts can for example be supported by creating databases, shared at European level, of declared orphan works. To simplify such centralisation efforts, it could be considered to encourage Member States to adopt harmonised solutions to the problem of orphan works in their national legislation.

**Communication from the Commission on “Copyright in the knowledge Economy”** – Despite the aforementioned initiatives, up until now, only limited progress has been made by the Member States on this point. The issue of orphan works published on line in blogs, social networks, portals, etc. remains uncovered, which could hamper the proliferation of user created content and create obstacles to novel digital ventures.

In its 2009 Communication on Copyright in the Knowledge Economy, the Commission indicated that the issue of orphan works will be examined in an impact assessment, in order to find possible approaches to facilitate the digitisation and dissemination of orphan works (e.g., legally binding stand-alone instruments on the clearance and mutual recognition of orphan works; an exception to the Copyright Directive, or guidance on cross-border mutual recognition of orphan works).

**The ARROW project** – ARROW (Accessible Registries of Rights Information and Orphan Works) is a project undertaken by a Consortium of European National Libraries, publishers and collective management organisations also representing writers through their main European associations and national organisations, which is funded under the eContentplus program dealing with copyright issues.

---

206 Gowers Review of Intellectual Property, 71
207 COM (2008) 513, p. 15
208 Two initiatives that can be mentioned in this respect are MILE and ARROW. Both projects aim to centralise information relating to orphan works.
209 COM (2009) 532 final, p. 5
210 COM (2009) 440 Final, p. 5
212 www.arrow-net.eu
such as orphan works. As described on its official web site, ARROW targets at supporting EC’s Digital Library Project by finding ways to identify rightholders, rights and clarify the status of the rights specifically by determining whether it is orphan or out of print\textsuperscript{213}. This project will enable obtaining information on practical copyright issues such as the rightholders, the rights concerned and their administration as well as information regarding where permission to use these rights can be found\textsuperscript{214}. This project aims also at achieving interoperability of the sources of information held by several copyright players.

4. Practical impact of current legal framework

4.1. National Implementation of EU level legal instruments

4.1.1. Discretionary margin allowed by articles 5.2 to 5.5 Copyright Directive

Articles 5.2 to 5.5 of the Copyright Directive contain an exhaustive list of limitations and exceptions to the reproduction right. This limited list was intended to enhance harmonisation and legal certainty throughout the Single Market. However, the exceptions and limitations contained in this list are only optional: Member States can choose whether or not to implement them. Moreover, these exceptions and limitations are expressed in a very broad way\textsuperscript{215}. Therefore, Member States have a significant discretionary margin in deciding how to implement those provisions in national law. This has resulted in a variety of implementations. Below are some indicative examples of how the countries have made use of this discretionary margin.

Private copying – Member States are allowed to adopt their own copyright limitations regarding private copying. Article 5.2.b of the Copyright Directive lays down that they may provide for exceptions and limitation “in respect of reproductions on any medium made by a natural person for private use and for ends that are neither directly nor indirectly commercial, on condition that the right holders receive fair compensation which takes account of the application or non-application of technological measures referred to in Article 6 to the work or subject matter concerned”. However, only a few Member States have implemented article 5.2.b as such\textsuperscript{216}. Hence, while article 5.2.b is reflected in all Member States, its regulatory framework and the details of its scope vary\textsuperscript{217}. For instance in the United Kingdom and in Ireland, copying for private uses is generally considered as copyright infringement, while in Belgium and Portugal private copying is immunised against contractual overrides\textsuperscript{218}. In the Czech Republic and in Poland the existing laws did not change, so that a general exception applying to acts of private copying remains in place subject to the condition that the purpose must be for personal use\textsuperscript{219}. The scope of permissible uses is more extensive in Austria and Germany, but the production of digital copies for uses

\textsuperscript{213} Ibid.

\textsuperscript{214} Ibid.

\textsuperscript{215} Study on the implementation and effect in Member States’ laws of the directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society, final report, Institute for Information Law, February 2007, p. 4,p. 39

\textsuperscript{216} The implementation of the Directive 2001/29/EC in the Member States, part II, February 2007, Queen Mary Intellectual Property Research Institute, p. 16

\textsuperscript{217} Ibid, p. 17


\textsuperscript{219} The implementation of the Directive 2001/29/EC in the Member States, part II, February 2007, Queen Mary Intellectual Property Research Institute, p. 17
exceeding the private use is subject to specific requirements. A very important deviation in the German implementation concerns the treatment of digital copies made for personal rather than purely private purposes where "the German implementation has drawn a distinction on the basis of the traditional regulation of copying for 'other own uses'"\textsuperscript{220}. Thus, legal entities are enabled to exploit personal use restrictions for copies made for example for scientific purposes\textsuperscript{221}.

As to the issue of copies made by third parties, there is uncertainty regarding the extent that a beneficiary may employ third parties to facilitate private copying in his behalf\textsuperscript{222}. As a result, Member States that have not addressed this issue will find difficulty in distinguishing between agency type situations and situations where legal entities have made copies with remuneration\textsuperscript{223}. More specifically in Hungary there is an expressed prohibition on third party copying, in Italy services of reproductions of sound and video recording are illegal, while in Germany a third party may be involved for non-commercial services if the copy is made for private purposes\textsuperscript{224}.

Moreover it has been identified that the Copyright Directive does not address the question of whether private copying exemptions can be contractually overridden\textsuperscript{225}. This issue is also closely related to the variety in the national implementation, which has also resulted from the complexity of the rules of the Directive regarding DRM and their interplay with the freedom to make private copies\textsuperscript{226}.

\textbf{Illustration for teaching purposes} – One characteristic example of the different implementation of the limitations in the Member States, is article 5.3.a regarding "illustration for teaching purposes". This exception refers to the "use for the sole purpose of illustration for teaching or scientific research, as long as the source, including the author's name, is indicated, unless this turns out to be impossible and to the extent justified by the non-commercial purpose to be achieved". Only Cyprus, France, Latvia, Luxembourg, Malta, the Netherlands and Spain reflect article 5.3.a in a single provision, though not all those Member States concurrently permit uses consisting communication to the public\textsuperscript{227}. Slovakia and Slovenia lack specific provisions dealing with educational and scientific research purposes\textsuperscript{228}. Furthermore; even between those countries that have either implement 5.3.a or adopted a similar provision, deviations can be found\textsuperscript{229}. Moreover, not all Member States extend article 5.3.a to acts of communication to the public\textsuperscript{230}. In Belgium, for example, a specific provision to cover the communication to the public for purposes of illustration for teaching or research by officially recognised establishments was adopted, whilst less restrictive requirements apply with regard to reproductions made for such purpose. In both cases, however, a levy is payable\textsuperscript{231}. Hence, while in some Member States communication to the public for educational and research purposes is subject to fair compensation like in

\begin{thebibliography}{99}
\item \textsuperscript{220} Ibid., p. 18
\item \textsuperscript{221} Ibid., p. 18
\item \textsuperscript{222} Ibid., p. 19
\item \textsuperscript{223} Ibid.
\item \textsuperscript{224} Ibid.
\item \textsuperscript{225} N. HELBERGER and P.B. HUGENHOLTZ, \textit{Ibid.}, p.1065
\item \textsuperscript{226} Ibid.
\item \textsuperscript{227} The implementation of the Directive 2001/29/EC in the Member States, part II, February 2007, Queen Mary Intellectual Property Research Institute, p. 32
\item \textsuperscript{228} Ibid.
\item \textsuperscript{229} Ibid.
\item \textsuperscript{230} The implementation of the Directive 2001/29/EC in the Member States, part II, February 2007, Queen Mary Intellectual Property Research Institute, p. 34
\item \textsuperscript{231} Ibid.
\end{thebibliography}
France (since 2009), in others like Spain communication to the public is restricted only to school teaching.\textsuperscript{232}

**Exception for publicly accessible libraries** – Article 5.2.c of the Copyright Directive (exception to the reproduction right for publicly accessible libraries, educational establishments and museums) is also a good example of the implementation differences that exist in the Member States\textsuperscript{233}. In some Member States, this exception has been transposed as a limitation used by libraries or archives for all types of works and for purposes of restoration and preservation of the material, while in other Member States it was restricted in specific types of material only by limited institutions. In other Member States, however, these limitations were not incorporated at all in national legislation\textsuperscript{234}.  

**Dedicated terminals** – Another example is article 5.3.n of the Copyright Directive, for communicating or making available a work "by dedicated terminals" for the purpose of research or private study, in publicly accessible libraries and the like. The discretionary margin allowed to the Member States has resulted in a situation where some countries\textsuperscript{235} did not implement the provision, some others did adopt the provision\textsuperscript{236} whereas others\textsuperscript{237} implemented it in such a way so as to be partially covered by communication to small groups of researchers. According to the Green Paper on copyright in the knowledge economy\textsuperscript{238}, the exception does not cover electronic delivery of materials to end users. Other commentators do not seem to agree with this point of view\textsuperscript{239}.

### 4.1.2. Other implementation issues

**TPMs** – A further example on how Member States deal with the discretionary margin allowed by the Copyright Directive, is the implementation of article 6 Copyright Directive regarding TPMs. Whilst most of the countries have implemented this article, Cyprus has not implemented article 6.1, and Austria has not transposed subsection 4. Although France has implemented the article, it has used nonetheless different wording than the one included in the Directive, using complex definitions for the acts of circumvention, the permitted circumvention for research purposes and the allowance of devices manufactured for circumvention which have other purposes. On the other hand, Greece and Malta have implemented article 6 as it is\textsuperscript{240}.

**The Information right** – The exercise of the information right in the Enforcement Directive has been difficult in some cases, due to the discrepancies of the national legal regimes of different Member States.

\textsuperscript{232} More on the implementation of the Directive 2001/29/EC can be found in the "Study on the implementation and effect in Member States' laws of the directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society", Institute for Information Law, February 2007, p. 63

\textsuperscript{233} Study on the implementation and effect of the Copyright Directive, o.c., p. 78

\textsuperscript{234} Ibid.

\textsuperscript{235} among which Austria, Ireland, Latvia, Sweden and the United Kingdom

\textsuperscript{236} among which Belgium, Italy and Luxembourg

\textsuperscript{237} such as Germany

\textsuperscript{238} p. 7: "This exception would arguably not cover the electronic delivery of documents to end users at a distance. As regards electronic delivery of materials to end users, recital 40 of the Directive states that the exception for libraries and archives should not cover "uses made in the context of online delivery of protected works or other subject matter."

\textsuperscript{239} They argue that online delivery is possible, provided that appropriate technological measures are applied to achieve truly restricted availability. See L. GUIBAULT, "The nature and scope of limitations and exceptions to copyright and neighbouring rights with regard to general interest missions for the transmission of knowledge: prospects for their adaptation to the digital environment", available at http://unesdoc.unesco.org/images/0013/001396/139671e.pdf, p. 23.

\textsuperscript{240} The implementation of the Directive 2001/29/EC in the Member States, o.c., p. 95–101
For example, in many Member States, internet addresses ("IP addresses") qualify as personal data\textsuperscript{241}. Therefore their collection must abide by the rules of the data protection law, according to which personal data can be revealed only in criminal cases involving serious crimes (such as a felony). However, the processing of personal data – even in cases of copyright infringement – is problematic\textsuperscript{242} in several Member States, including Greece and Italy. In some Member States, rightholders cannot obtain the identity of a user through civil proceedings, as this information can only be disclosed to the police or to the Court in criminal actions\textsuperscript{243}.

**The use of the three steps test** – As pointed out above, incidents of digital copyright infringements have exponentially increased, while at the same time technological measures allow the monitoring of access and use of copyrighted content. This has resulted in a disturbed balance of interest between the parties involved.

When investigating how the balance can be restored, it is sometimes said to be useful to rely upon the "three steps test", which aims to prevent copyright limitations from encroaching upon rightholders' rights\textsuperscript{244}. At the same time, the three steps test is considered as a crucial attempt to harmonise the exceptions and limitations between the diverse implementations of the different Member States\textsuperscript{245}.

Nonetheless, in the Study on the Implementation of the Directive 2001/29\textsuperscript{246}, it was observed that "the test is perceived as a matter of legislative compliance with international prerequisites rather than a rule of interpretation of domestic law; it remains however blurred whether the test only constitutes a guideline for legislative action or for interpretation of exceptions by national judges". In practice, the "three step test" is indeed used in most Member States as a norm to be applied by the Courts in the interpretation of the limitations on copyright recognised in the national copyright laws\textsuperscript{247}. It functions as a control mechanism to reassure the balance between the rights and limitations of copyright\textsuperscript{248}.

It has also been suggested, however, that the direct enforceability of the test by the Courts is problematic in so far as it equals to a quantitative assessment of the three factors\textsuperscript{249} that – according to article 5.5 and in line with the Berne Convention and the TRIPS Agreement – should be met cumulatively. In addition it has been also commented that the test cannot be used effectively if there are no directions determining where the line between grants and reservations of copyright should be drawn. Hence this lack of guidelines has resulted in different interpretations within the Courts of different Member States.

\footnotesize{\textsuperscript{241} See also Chapter 4 - privacy and data protection  
\textsuperscript{243} Ibid.  
\textsuperscript{244} M.R.F SENFTLEBEN, *Copyright, limitations and three step test*, Kluwer Law International, p. 5  
\textsuperscript{245} G. MAZZIOTTI, *EU Digital Copyright Law and the End-User*, Springer, 2008, p. 84  
\textsuperscript{247} Study on the implementation and effect in Member States ‘ laws of Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society, Institute for Information Law, 2007, p. 71  
\textsuperscript{248} Copyright, limitations and three step test, Martin R.F Senftleben, Kluwer Law International, p. 5  
\textsuperscript{249} EU Digital Copyright Law and the End-User, Giuseppe Mazziotti, Springer, 2008, p. 303}
4.1.3. **Case law and legal doctrine**

*In this section, some indicative cases are presented as examples of how different jurisdictions have ruled in some important issues related to digital content trends that have recently risen.*

**a) District Court of Munich**

This case concerns the first court case in the EU regarding open source Software, and concerned the alleged violation of the GNU General Public License (GPL). The case was presented before the District Court of Munich [250, 251].

**Background** – The plaintiff was a member of the "netfilter/iptables" open source project, and asserted a claim for injunctive relief against the defendant, a German company selling network products. The plaintiff made the source code of the "netfilter/iptables" software available under the GPL licence, so that the software could be downloaded, used and further improved by anyone. However, according to the term of the GPL licence, any further distribution of the software (whether or not modified) should again be accompanied by the source code. Although the defendant had used the software in its network products, the website of the defendant did not include any reference to the fact that the "netfilter/iptables" software was used, and did not make available the source code [252].

**Decision** – On the 2nd of April 2004, the District Court of Munich upheld a temporary injunction, according to which "the defendant was enjoined from distributing and/or copying and/or making available to the public the software netfilter/iptables without at the same time in accordance with the license conditions of the GNU General Public License, Version 2 (GPL) – making reference to the licensing under the GPL and attaching the license text of the GPL as well as making available the source code of the software "netfilter/iptables free of any license fee" [253].

**Evaluation** – The ruling of the Court was accepted with great enthusiasm by all the members of the open source community. It was considered "the first sign of case law regarding the development of non proprietary software and various forms of content which is based on the circulation of licenses that tend to weaken standard copyright" [254].

Even so, the decision has also been criticised. This criticism was targeted at "the strict approach of the decision to the German methodology and the lack of the US approach, as this issue was deemed to have deep legal roots to the US Law and the US Open Source Mentality" [255]. Moreover it has been argued that the Munich ruling could possibly be opposed to the principle of exhaustion. Prof. HOEREN has commented that the Court was ignorant of what is called the "opinio communis" [256]: "if the GPL licence is considered binding in cases of transfer of software to a third party, this could be considered as a possible violation of the principle of exhaustion which applies to the first sale of the copy in the Community with the consent of the right holder" [257]. According to the GPL licence, contrary to what is set

---

250 District Court of Munich I, Judgement of 19/05/2004 – file reference: 21 0 6123/04 (Open Source – effectiveness of GPL)

251 Harald Welte vs S. Deutschland Gmbh, District Court of Munich, available at [www.jbb.de/judgment_dc_munich_gpl.pdf](http://www.jbb.de/judgment_dc_munich_gpl.pdf)

252 Ibid.

253 Ibid.

254 Introduction to GPL and Creative Commons, Ahlert Christian available at [www.oii.ox.ac.uk/resources/feedback/OIIFB_GPL1_20040903.pdf](http://www.oii.ox.ac.uk/resources/feedback/OIIFB_GPL1_20040903.pdf)

255 T. HOEREN, "The first- ever ruling on the legal validity of GPL- A critique of the case", available at [www.oii.ox.ac.uk/resources/feedback/OIIFB_GPL3_20040903.pdf](http://www.oii.ox.ac.uk/resources/feedback/OIIFB_GPL3_20040903.pdf)

256 Ibid.

257 Ibid.
by the European Software Directive, once the author has “sold” a copy of the work with his/her consent he/she still retains his/her exclusive distribution right regarding that work. German law does not allow to override this exception with a contract.

Nevertheless, this case is of crucial importance. First, because it ruled for the first time that open source licences are valid, and second because – although it was a clear judicial decision in favour of the validity of open source licensing – it held that not all terms included in the licence may be valid.

b) Peppermint’s case
Another interesting case is the so called “Peppermint’s case”, regarding the conflict between personal data and IP infringement.

**Background** – In this case, a German music label (Peppermint Jam Records GmbH), had sent 3,636 notices of copyright infringement to alleged Italian copyright infringers. With these notices, Peppermint informed the alleged infringers that they were suspected of illegally uploading copyrighted songs. These notices also included a request drafted by an Italian law firm, asking from the infringers to stop their illegal actions and, additionally, to remove from their computers all songs that belonged to the music label. In addition, they invited the alleged infringers to deposit an amount of 300 Euros to the account of the law firm, in order to avoid being subject to civil and criminal lawsuit brought against them. At the same time, a draft agreement was attached to the notice to be signed and returned to the Italian law firm.

The proceedings before the Court of Rome begun when Peppermint sued an Italian internet access provider in order to obtain the names and addresses of the users that had allegedly shared the files whose copyright belonged to Peppermint. This claim was supported by a report that indicated that copyrighted songs from Peppermint were offered by file-sharing programs through the Internet.

There were a number of other similar proceedings brought by Peppermint and a Polish videogame publisher, Techland.

**Decision** – On the basis of the evidence provided in this report, the Court of Rome issued an interim decision ordering the access provider to provide Peppermint with the personal details of its customers. The legal basis for the decision of the Court of Rome was section 156ter of the Italian Copyright Law, according to which a party is entitled to ask a Court to order the other party to communicate information in its possession. In addition, the Court decided that it is possible for the rightholder of copyright to start civil actions against any person deemed to have been involved in the infringement if the infringer is unknown. For that reason, it ordered the ISP to disclose the personal data of its clients. While the Rome Court initially sided with the rightholders, in a later injunction proceeding, after intervention by the Data Protection Authority, the Court reversed its ruling and denied the rightholders’ requests. This eventually led to the March 2008 rule by the Authority that held that “*the use of such software violated the Italian Privacy Code and the EU Privacy Directive and as such the resulting names could not be disclosed*.”

---


259. Ibid.


261. L. LIGUORI, Peppermint’s Case, o.c.

262. International Intellectual Property Alliance (IIPA) 2009 Special 301: Italy.p.218
Evaluation – This case triggered discussions as to whether the activities of Peppermint and Logistep (the company that drafted the report) to gather data of internet users were compatible with the Italian Data Protection Law²⁶³.

c) Mulholland Drive case
This case concerned the legal nature of the private copying exception as opposed to the restrictive power of digital anti-copying devices²⁶⁴.

Background – Legal action was initiated by a French user who wanted to make a private analogue copy of a copy-protected DVD film distributed in France. The DVD had no indication informing users that it could only be used on specific devices. The user’s claim was that he wanted to copy this film from the DVD to a VHS format, so that he would be able to watch it at his parents’ home where no DVD player was available. The user argued that the copy-protection device installed on the digital medium impeded this purpose²⁶⁵. The French consumer union “UFC-Que Choisir” joined the French user’s claim, declaring that the right of private copying of the user was violated. The plaintiffs claimed that under French law “holders of copyright and related rights cannot prohibit copies or reproductions that are strictly reserved to a private use by the copier and are not used collectively”²⁶⁶.

Decisions – The Paris High Court ruled that the existence of an exception of private copy was by nature detrimental to the normal exploitation of films²⁶⁷. The Paris Court of Appeal on 22 April 2005, however, declared that the private copying regime did not constitute a consumer’s right, but rather an exception to the rightholders’ monopoly²⁶⁸. Next, the Supreme Court held that technical measures implemented to protect the exclusive right of reproduction should always be construed as prevailing upon private exceptions, even if the enforcement of such exceptions takes preference over the protection of technical measures²⁶⁹. The new decision of the Court of Appeal in Paris in April 2007 laid down that the right to private copying cannot forbid the application of DRMs. Nevertheless, private copying can be considered as an argument for defence in counterfeiting cases²⁷⁰ ²⁷¹. In this context, the Court decided that the private copy of a work is not a right but “a legal exception to the principle of copying the entire work without the consent of the copyright holder”²⁷² and as such an exception can not be considered a basis of a legal action.

Evaluation – The history of this case shows that international copyright treaties (like the Berne Convention) and the European Directives are of direct applicability in France and prevail over internal law in the hierarchy of rules: the private copying rule found in the French Intellectual Property Code “has to comply with higher international laws”²⁷³.” The decision of the Supreme Court portrayed that the

²⁶³ Ibid.
²⁶⁵ G. MAZZIOTTI, EU digital copyright law and the end-user, 2008 Springer, p.201
²⁶⁶ Translation based on Giuseppe Mazziotti, o.c., p.202
²⁶⁷ Case law available at www.legalis.net/breves-article.php3?id_article=722
²⁶⁸ www.legalis.net/jurisprudence-decision.php3?id_article=1909
²⁶⁹ G. MAZZIOTTI, EU digital copyright law and the end-user, 2008 Springer, p.206
²⁷⁰ Private copy explained by Court of Appeal in Paris available at www.edri.org/edrigram/number5.7/private-copy-france
²⁷¹ Case law available at www.legalis.net/jurisprudence-decision.php3?id_article=1909
²⁷² As found in Private copy explained by Court of Appeal in Paris, available at www.edri.org/edrigram/number5.7/private-copy-france
²⁷³ www.europeanbusinesslawyers.com/cache/article/file/Mulholland_Drive.doc
adoption of a normal exploitation regarding markets for copyrighted digital works might have the negative consequence of outlawing all types of digital private reproductions of copy-protected content, regardless of whether these reproductions are carried out by analogue or digital means.\textsuperscript{274}

Although this case was brought to Court before the implementation of the Copyright Directive Directive in France, it has highlighted the issue that technological measures can prevent permitted acts from lawful users. This issue has become even more obvious with the implementation of the Copyright Directive.

d) The Pirate Bay case

**Background** – Between 1 July 2005 and 31 May 2006, the Pirate Bay website offered "BitTorrent" files to facilitate the peer-to-peer exchange of data.

In January 2008, the Swedish District Prosecutor indicted four persons for complicity in breach of the Copyright Act (1960:729), since, "jointly and in collusion with each other and another person, they had been responsible for the operation of the file-sharing service [called] The Pirate Bay".\textsuperscript{275} According to the Prosecutor, through this website they aided and abetted other individuals who made recordings and software available to the general public via the Internet, as well as computer software and computer games. In addition, the Prosecutor claimed that these persons aided and abetted others in the production of copies of the recordings and of the computer software. According to the Prosecutor, the acts of "aiding and abetting" referred to the fact that the defendants, through the file-sharing service, provided others with the opportunity to upload torrent files to the service, provided others with a database linked to a catalogue of torrent files, provided others with the opportunity to search for and download torrent files, and also provided the functionality with the assistance of which individuals wishing to share files with each other could contact each other through the file-sharing service's tracker function.

The Prosecutor also claimed that the defendants were guilty of preparation for breach of the Copyright Act, during the period 1 July 2005 to 31 May 2006, in that, in connection with the operation and through the functionality of the file-sharing service, they received and stored the BitTorrent files in a specially prepared database with associated catalogue. These files were specifically intended to be used as an aid in breach of the Copyright Act.\textsuperscript{276}

**Decision** – The verdict of the Swedish court in the Pirate Bay trial was given on 17 April 2009, with the four defendants found guilty of complicity in breach of the Copyright Act. The Court sentenced each to one year in prison and to pay together about 2.7 million euro in damages.\textsuperscript{277} However, the defendants have expressed their intention to appeal to the decision.

\begin{quote}
This case also contains an interesting application of the special liability regime (set forth in the eCommerce Directive, and discussed in detail in Chapter 6). According to the Swedish court, the Pirate Bay does qualify as a "hosting provider" (article 14 of the eCommerce Directive), as it offered server space to third parties to store BitTorrent files. However, the court ruled that the Pirate Bay was not actually protected by the special liability regime, because hosting providers are only protected to the extent that they have no actual knowledge of the illegal information on their systems, and take down any illegal information as soon as they gain actual knowledge. According to the court, "It must have been...
\end{quote}

\textsuperscript{274} G. MAZZIOTTI, o.c., p.208

\textsuperscript{275} STOCKHOLM DISTRICT COURT, Division 5, Unit 52, VERDICT B 13301-06, 17 April 2009, handed down in Stockholm, Case no B 13301-06, www.ifpi.org, p.15

\textsuperscript{276} Ibid.

\textsuperscript{277} The Pirate Bay Decision : www.edri.org/edri-gram/number7.8/the-pirate-bay-court-decision

Following this decision, the music industry has decided to use all possible legal means against Pirate Bay, and already initiated legal action in Denmark, Netherlands, Norway and Sweden. As a result, the Pirate Bay's services were unaccessible in August 24th 2009, because its hosting provider was obliged by a Swedish Court order to disconnect the website from the Internet at the threat of significant daily penalties (even so, The Pirate Bay had prepared a backup solution and came back online soon). Meanwhile, in Ireland, internet access provider Eircom has cut off access to The Pirate Bay as from 1 September 2009. In Norway, the hearing between the movie and music industry and access provider Telenor to block the Pirate Bay will take place on October 2009. In the Netherlands, the anti-piracy organisation BREIN obtained a default judgement to block The Pirate Bay.

Evaluation – This case concerns the issue of criminal complicity in copyright infringement specifically by individuals who are alleged to have provided a file-sharing service within a computer network. Additionally, it concerns the liability of those involved to pay damages under the terms of the Copyright Act. Furthermore, it is of crucial legal importance not only because it practically describes the way that copyrighted works were made available to the public through the use of the file-sharing technology, but also because there is a belief that the verdict may have implications for all file-sharing platforms starting a "legal battle" between them and the recording industry. At the same time, it is one of the most indicative examples of the copyright infringements phenomenon and it has an important societal influence. Protests attended by a number of people in big European cities against the decision indicated once more that everyday users do not consider the phenomenon of copyright infringements as an unethical activity.

5. Practical example: Europeana

5.1. Introduction

In November 2008, the online library Europeana was made available to the public. The aim of the platform, which is operated by the European Digital Library Foundation, is to gather Europe's cultural and scientific resources and to make those resources accessible through the Internet. Today, the Europeana project, which was initiated by the European Commission and is funded by the Commission and the Member States, gathers 4,6 million digital items on its website. More than 1,000 cultural institutions, such as libraries, museums and universities, have contributed content and more than 150 institutions are part of Europeana's partner network. The collection consists of a broad set of objects,
such as pictures of museum objects, paintings, newspapers, radio broadcasts and films. The policy target is to gather 10 million objects on the platform by 2010\textsuperscript{286}.

Europeana is an unprecedented effort to digitise Europe’s cultural and scientific heritage. However, the progress of Europeana has also brought to light a number of significant challenges and problems with regard to the process of digitising and distributing content on a Europe-wide scale. These issues currently limit the potential of Europeana and constitute a barrier to the dissemination of its contents. Also, the problems identified within the framework of Europeana are not unique to this project, and retain their relevance in relation to the wider subject of digitising and distributing content online. In view of the increasing importance of digital content models, addressing these issues is crucial for the further development of a European legal framework that balances the interests of rightholders and the public at large. As pointed out by Commissioner Reding in a recent speech:\textsuperscript{287}

“Let us be very clear: if we do not reform our European copyright rules on orphan works and libraries swiftly, digitisation and the development of attractive content offers will not take place in Europe, but on the other side of the Atlantic. Only a modern set of consumer-friendly rules will enable Europe’s content to play a strong part in the digitisation efforts that has already started all around the globe.”

This section 5 therefore applies the issues identified in the previous sections to the Europeana project, and delves further into some of the specific problems encountered within the framework of the project.

### 5.2. Licence restrictions

At present, much of the material accessible through Europeana is in the public domain, \textit{i.e.} free from intellectual property rights (in particular copyright). However, Europeana explicitly aims to also include copyrighted material, which is necessary if the platform is also to provide access to contemporary information of cultural and scientific importance\textsuperscript{288}. A significant issue in this respect is the variety in licence conditions applicable to copyrighted works. This is exemplified by the (provisional) terms of use of Europeana, which state that:

“All third-party material presented within this website are subject to individual Intellectual Property Rights (IPR) conditions and licences. Providing details of such IPR and licensing is the responsibility of third-party sources and should be either presented within this website or available from the originating sources of the third party material”\textsuperscript{289}.

Licence agreements often contain restrictions with regard to the cross-border distribution of the content, thus excluding the possibility to distribute the digitised content on a Europe-wide basis. For example, one Europeana contributor had to withdraw a number of photographs from Europeana, because the applicable licence agreement prohibited distribution outside of France\textsuperscript{290}. While it is technically possible to restrict access to content based on the geographic location of the end-user\textsuperscript{291}, such an approach

\textsuperscript{286} COM (2009) 440 Final, p. 4
\textsuperscript{287} V. REDING, EU Commissioner for Telecoms and Media Digital Europe - Europe’s Fast Track to Economic Recovery, The Ludwig Erhard Lecture 2009 Lisbon Council, Brussels, 9 July 2009
\textsuperscript{288} COM (2009) 440 Final, p. 5
\textsuperscript{289} www.europeana.eu/portal/termsofservice.html
\textsuperscript{290} COM (2009) 440 Final, p. 5
\textsuperscript{291} Such approach is followed by several services that distribute audiovisual content online, such as the BBC iPlayer and the video player on Fox.com
contradicts with the goal of Europeana to make Europe’s cultural and scientific resources accessible for all 292.

In part, the fragmentation of the right to disseminate content within certain territories is the result of financial considerations. For rightholders, it may be more financially interesting to restrict the scope of a licence to one country, allowing them to re-license the content in other countries and to receive royalties in each separate country. However, such licensing policies are hard to reconcile with the ubiquity of the online environment293. In this context, the encouragement of the adoption of multi-territorial licensing agreements is crucial in creating a balance between rightholders interests and public benefit. In addition, the legal uncertainty that exists with regard to the current legal framework may prove to be an additional barrier for the conclusion of pan-European licence agreements. The gaps and ambiguities identified in this report may prove useful in this respect294.

5.3. Orphan works

A second problem faced by Europeana is the inclusion of orphan works, i.e. copyrighted works of which the rightholders cannot be identified (see section 3.7.5 above). As a result, actions such as the digitisation, reproduction and dissemination of orphan works are not allowed, because they require the consent of the rightholders295. In addition, any commercial interest in these works is undermined by the concomitant legal uncertainty.

In the United States, the topic of orphan works has received significant attention in the context of the Google books settlement296. Through the Library Project, which is part of the larger Google Books project, Google has scanned thousands of books from university and civic libraries. A large number of these books are in-copyright, but are out of print or actual orphan works. Regardless of intellectual property concerns, Google has scanned these books and made them available in snippets. This has led to a claim from the US Authors Guild, which in turn has led to the proposed settlement. Under the settlement, Google would be released from liability for scanning, searching and displaying books, in exchange for 63% of the advertising revenues arising from Google Books297. More significantly, the deal would allow Google to continue making available out-of-print and orphan works, while holding a share of the revenues in trust for the rightholders. A new entity, the “Book Rights Registry”, would be responsible for passing along payments to authors and publisher. The settlement process was put on hold as a result of the significant number of objections that has been raised, including by the US Department of Justice298. However, lately, a Federal Judge gave the parties time to negotiate a new deal addressing some objections that were filed form implicated groups299. Judge Chin mentioned that it made no sense to hold a hearing on the settlement when there are indications that the parties are still negotiating changes in it300.

292 www.europeana.eu/portal/aboutus.html
293 See Section 5.2
294 See Section 3.1 and 3.2.
295 See Section 3.7.5
296 See Proposed Settlement, Authors Guild v. Google Inc., No. 05 CV 8136 (S.D.N.Y. filed Oct. 28, 2008)
297 J. GRIMMELMANN, “How to Fix the Google Book Search Settlement”, JILL, vol. 12, nr. 10, p. 11
298 The decision to postpone the planned fairness hearing is available at http://thepublicindex.org/docs/case_order/20090924.pdf
300 Ibid.
5.4. Consequences of format shifting

A third issue is the uncertainty about whether the digitisation of public domain works creates new intellectual property rights. This question results from the fact that some Europeana contributors claim rights on materials in their collection that are in the public domain, but have been converted to a digital format. Such claims take the form of watermarks and charging for downloading the works or viewing them in a higher resolution.\(^\text{301}\)

From a legal point of view, the question is whether a digitised work can be regarded as an "original" work. Although article 2 of the Berne Convention does not explicitly mention it, the criterion against which the copyrightability of literary and artistic works needs to be checked is "originality".\(^\text{302}\) As noted above, no common definition of the standard of originality has been adopted by Copyright Directive.\(^\text{303}\) As a result, each Member State is free to uphold its own regime of originality standards for copyright protection, which may result in discrepancies. In particular, these standards may vary in function of the type of work that is digitised.\(^\text{304}\)

Despite the dissimilarities in interpretation throughout the Member States, the notion of originality usually requires some form of intellectual, creative or personal input.\(^\text{305}\) Therefore, simple, straightforward digital reproductions of a work may not achieve the required standard of originality.

In addition, marking digitised public domain works as original, threatens to nullify much of the benefits of the making physical works in the public domain easily accessible in a digital form. The Commission has also stressed the importance of keeping public domain works within the public domain after a format shift.\(^\text{306}\) However, it is clear that fair compensation mechanisms which take into account the nature of the digitised work should be put in place to incentivise the digitisation of public domain works. Therefore, it should be considered which public or private funding mechanisms can be put in place to compensate institutions for their efforts in this respect, without connecting such compensation with the establishment of new intellectual property rights.

5.5. Public domain works

A fourth factor limiting the content available on Europeana is the difference between European and United States copyright legislation with regard to what constitutes a public domain work. Both in Europe and the US, the duration of copyright protection is set at 70 years after the death of the author.\(^\text{307}\) After this period, copyright expires and works fall into the public domain. However, in the US, works that were published before 1923 are in the public domain, regardless of the date of decease of their author. The

---

\(^{301}\) COM (2009) 440, p. 7


\(^{303}\) See Section 3.1

\(^{304}\) As noted in COM (2009) 440, p. 7, the difference in digitisation cost of various types of work (such as books and three-dimensional objects) subject to copyright, may influence the decision of what constitutes originality.

\(^{305}\) For an overview of the interpretation of the notion in various Member States, see G. KARNELL, European originality: A Copyright Chimera, available at www.cenneth.com/sisl/pdf/42-5.pdf, p. 76 - 77


\(^{307}\) In Europe the term was harmonised by Council Directive 93/98/EEC of 29 October 1993 harmonising the term of protection of copyright and certain related rights, OJ no. L290 of 24 November 1993, pp. 9–13. In the Unites States, the extension was established by the Copyright Term Extension Act (CTEA) of 1998. The Act can be consulted at www.copyright.gov/legislation/s505.pdf
result is that European copyrighted works from before 1923 can be digitised and made available to consumers in the US, while they may not be available in Europe.\textsuperscript{308}

In its 2009 Communication on Europeana, the Commission has stated that solutions involving rightsholders and cultural institutions should be considered to redress this situation.\textsuperscript{309}

- A first possible solution is creating registries for orphan works and out of print works. While this approach would allow stakeholders to obtain a better view on the copyright restrictions applicable to a particular work, and possibly to allow the use of the work under one of the rights clearance mechanisms mentioned above, it would not remedy the discrepancy between the US and Europe created by the 1923 US cut-off date.

- The second suggestion entails implementing a similar cut-off date in Europe, following which a lower threshold for diligent search may be applied. However, as mentioned above, compliance with the standards of diligent search will only result in the provision of a licence if no rightholder has been identified. Consequently, where a rightholder is identified for a work created before 1923, Europe will still have a more limited number of works in its public domain. Therefore, in order to remove the existing disparity, Europe should consider adopting a cut-off date following the example of the United States.

6. Conclusions

1. Over the years, many Community legal instruments and policy documents have been enacted in the field of copyright. The most important legal instruments are the Copyright Directive and the Enforcement Directive.

2. While the Copyright Directive and Enforcement Directive take into account some broad characteristics of the online environment, many specific characteristics are not considered. For example, the Copyright Directive contains a long list of exceptions and limitations to the exclusive rights of authors, but few of these exceptions and limitations fit properly in the digital environment, and many are not technologically neutral.

3. Furthermore, the general terms used in the Copyright Directive are drafted in a rather general language and are vague and are open to different interpretations. For example, the exception on temporary acts of reproduction does not specify what qualifies as an act without "economic significance" (article 5 Copyright Directive). Similarly, it is unclear what constitutes "adequate legal protection" in article 6 Copyright Directive.

4. In addition, there are some gaps in both legal instruments, such as the lack of a single standard of originality, the absence of segmentation-preventing measures outside online music and the lack of a uniform criterion to determine the applicable law and the competent court.

5. Due to the diverging implementations of the EU-level instruments and the lack of a harmonised method of copyright management, there is significant market fragmentation. The difficulty to get legal certainty on the reuse of content and on clearing rights also contributes to this issue. Several Commission initiatives (such as the Commission Recommendation of 2005, the Green Paper on Copyright in the Knowledge Economy and the Communication on Creative Content Online in the Single Market) try to alleviate these concerns, but have not yet solved them.

6. Another important issue is the lack of a harmonised set of mandatory exceptions and limitations to the exclusive rights of authors. As a result, Member States can decide if and how to implement the

\textsuperscript{308} COM (2009) 440, p. 6
\textsuperscript{309} COM (2009) 440, p. 6
exceptions and limitations. The list of exceptions also exhibits many ambiguities and leaves ample discretionary room to Member States. Consequently, the exceptions and limitations have become a cluttered chaos on the Member States level.

7. **Technological protection measures** (TPMs) also entail many legal issues. The Copyright Directive legally protects TPMs – which shifts the focus of the legal protection from the copyrighted work to the technology that protects it – but does not provide specific guidelines on the implementation of TPMs. In addition, the Copyright Directive does not allow circumvention of TPMs not even if it is made for legitimate purposes. Further, the use of TPM technologies could conflict with a user's data protection and privacy rights.

8. Furthermore, the Copyright Directive and Enforcement Directive are unbalanced. The reproduction rights are overly broad and overlap with the right of communication to the public. Also, the IP enforcement regime of the Enforcement Directive is broad covering even minor and unintentional infringing acts.

9. As a result, the current legal instruments in the field of copyright are insufficient. They do not satisfy rightholders (which face a fragmented and pirated market) and do not satisfy users either (who face a list of ambiguities and a limited list of exceptions that does not take into account their daily concerns). A fundamental reform has become necessary.

7. **Recommendations**

7.1. **Responding to the changed role of users**

7.1.1. **New provisions to cover the "user created content" phenomenon?**

**Definition** – "There is a significant difference between user created content and existing content that is simply uploaded by users and is typically protected by copyright"\(^{310}\). In a recent OECD study, user created content (UCC) is defined as content that is made publicly available over the Internet, which reflects a certain amount of creative effort, and is created outside of professional routines and practices\(^{311}\). In this definition, no distinction is made between original or derivative works. The only criterion is that this works stems out from the effort of a person (natural or legal) outside of the course of its trade.

This definition reflects also the beliefs of those that support the proliferation of the UCC phenomenon that argue that "non-commercial users have different incentives to create, use, and to share than established professional content holders; [...] these incentives should be preserved due to their social and cultural impact"\(^{312}\). In the i2010 Mid Term Review it has been observed that "user created content experienced especially rapid take up, confirming the Internet as a medium of two way communication"\(^{313}\).

**New exception?** – Some have recommended to create an exception "for creative transformative or derivative works within the parameters of the Berne Conventions three step test"\(^{314}\). Furthermore the

\(^{310}\) Green Paper on Copyright in the Knowledge Economy, COM(2008) 466/3 p. 19
\(^{312}\) Ibid. p. 82
\(^{313}\) i2010 Mid Term Review, (COM/2008/199). p. 36
\(^{314}\) Gowers Review of Intellectual Property 2006, o.c., p. 6
have also been recommendations to introduce a limited private copying exception for format shifting without any accompanying levies for consumers. In the Gowers Review in UK it is suggested to amend the Copyright Directive so as "to allow for an exception for creative, transformative or derivative works within the parameters of the Berne 'Three Step Test'". According to some commentators, the exception adopted in relation to the user generated content must be made mandatory.

However, at the same time, there are others who claim that there is no need to adopt any new rules in relation to the UCC and who argue that there is no evidence that "further or different rules are necessary". According to some business players: "the current copyright system of protection and limitations can accommodate the new generation of creators that are utilizing new digital technologies". In the same vein it has been also supported that there is "no justification for new exceptions as the market is developing and will continue to develop on the basis of agreement between the parties, based on copyright and facilitated through licensing". This argument is further elaborated by suggesting that there is no need to change the law since the already existing exceptions and limitations can be "combined with systems like creative commons, and machine to machine readable permissions such as ACAP" to provide a sufficient environment for the proliferation of the UCC.

In the 2009 Communication on Copyright in the Knowledge Economy, it has been noted that: "[…] the Commission intends to further investigate the specific needs of non-professionals that rely on protected works to create their own works. The Commission will further consult on solutions for easier, more affordable and user-friendly rights clearance for amateur users."

**Our position** – While we appreciate the concerns of the rightholders, at the same time we welcome the suggestion of the aforementioned Communication to further investigate the user created phenomenon. It is our belief that the current legal framework is not sufficiently adapted to the concept of user generated content, if only because the current exceptions and limitations in the Copyright Directive are not mandatory. We think that it is now the time to provide the definition of the user created content to distinguish it from any other forms of generated content in order to further elaborate whether to attribute to those exercising it some lawful uses.

One idea could be to create new exceptions and/or statutory rights for "real" user generated content (i.e., content that reflects a certain amount of creative effort, and is created outside the professional context). User generated content has been the basis of many success stories in the online environment (such as YouTube, Wikipedia and DailyMotion) and promises to be the model of the future. In the context of the reform of the Copyright Directive, we therefore highly recommend to consider such new exception or statutory right according to the definition provided to describe the phenomenon.

---

315 Ibid.
316 Gower's Review on Intellectual Property, 2006, o.c., p. 72
317 ASSOCIAZIONE ITALIANA BIBLIOTHECHE, Comments to the Green Paper on Copyright in the Knowledge Economy at the European Commission, p. 3
318 Penguin Group, Comments to the Green Paper on Copyright in the Knowledge Economy at the European Commission, p. 3
319 Microsoft, Comments to the Green Paper on Copyright in the Knowledge Economy at the European Commission, p. 2
320 European Coordination of Independent Producers (CEPI), Comments to the Green Paper on Copyright in the Knowledge Economy at the European Commission, p. 3
321 Automated Content Access Protocol (ACAP), available at www.the-acap.org, as found in European Coordination of Independent Producers (CEPI), Comments to the Green Paper on Copyright in the Knowledge Economy at the European Commission, p. 9
For example, it could be stated that users (iConsumers) must have the right to reuse (digital) content, to the extent that this reuse is not intended to harm the rights of rightholders. On the basis of this right, a user would be allowed to reuse small fragments of commercial music and/or movie when publishing a new home video on a video sharing platform, provided there is indeed a create effort. The user would not be allowed, however, to publish the entire commercial track or the entire movie on the video sharing platform.

AVMS issues — Another important issue for user generate content emanates from the new Audiovisual Media Services Directive. This Directive only applies to service providers that exercise "editorial responsibility" over audiovisual content, which is defined as "the exercise of effective control both over the selection of the programmes and over their organisation". It is not clear to which extent a video platform with user generated content (such as YouTube) falls within the scope of this definition, as it is difficult to argue that such platforms exercise "editorial control" over the millions of videos uploaded to its platform (they typically only remove illegal content on request). Instead, it could be argued that "the community" exercises this control. However, the Directive does not take into account such decentralised organisations, and only focuses on traditional, centralised control hierarchies. As the Directive is not yet implemented in all Member States, it is too early to tell how this will be dealt with in practice.

7.1.2. Dealing with consumers

Many of the controversies between consumers and businesses within the digital content market result from "the consumers' wish to make best and most profitable use of digital generated work and on the other hand the interest of the industry to exercise control over the content's use and distribution to secure a viable business model". The challenge is to reconcile the conflicting interests and to find a balanced solution that satisfies both parties' reasonable and fair interests.

The current copyright legal instruments do not sufficiently take into account consumers, since general copyright law had been mainly designed to regulate the relationship between authors / rightholders and intermediaries (publishers). In the current legal instruments, consumers of digital content are generally treated in the same ways as users of analogue content. A challenge of the digital environment is therefore to address the complex roles of consumers and users of digital content.

Dealing with "active & passive consumers" — A first recommendation is dealing with the active consumer (further called the "iConsumer"). Indeed, the role of the consumer has changed in the new digital era: nowadays, digital technologies empower consumers to undertake actions that were until previously performed only by professional suppliers. Consumers write blogs, consume media, remix content, and create new content (e.g., as "citizen journalists" on their blogs).

Hence, new statutory provisions must be adopted that allow the iConsumer to undertake some minimum actions on the content. At the same time "passive consumers", i.e. consumers that do not actively create new content, must be more effectively protected too.

Both active and passive consumers should be able to take advantage of all the basic consumers' rights such as: the right to "technical neutrality"; the right to receive information regarding the technological protection measures used; the right to fair contract terms; the right to redress when products/works are of unsatisfactory quality; the right of interoperability of content and devices; the right of privacy

323 Ibid.
324 The word "prosumer" (which describes the current active user of digital content) stems from the combination of the words "professional" and "consumer". See A. TOFFLER, The Third Wave, 1980, as found in N. HELBERGER, o.c.
protection, as well as the right not to be criminalised. Additionally, we are in favor of adopting Codes of Conduct or/and minimum contractual clauses that would apply to all standard form contracts (i.e., non-negotiated contracts), since the former type of contracts broadly governs the majority of transactions taking place in the online environment.

Moreover, it could be envisaged to adopt a "black list" of unfair clauses, according to which a term in a non-negotiated contract would be deemed unfair if it departed from the provisions of copyright law. Another suggestion is to issue a sector specific list of "grey contractual clauses" that are considered as unfair under provisions of unfair contracts terms, acting as a presumption of unfairness. In the 2007 European Parliament Resolution on consumer confidence in the digital environment, it has been supported that "the application of the regime on unfair contract terms should be reinforced in the field of end-user licence agreements and should include technical contract terms." In this vein, the same document supports that the aim should be to increase consumer confidence in the digital environment.

In addition, in order for the protection to be expanded to more stakeholders (e.g. SMEs), a provision in the general contract law of Member States could be introduced to grant professionals too the right to benefit from a protective measure against the use of restrictive terms.

In Greece for example, in the general consumer protection law (that implements Directive 93/13/EC into national law), a consumer is defined not only as a natural person but also as a legal person that acts outside of the course of its business. This way SMEs and any other enterprise acting outside of their everyday trade could fall under consumer protection regime. This would also be in line with the OECD definition of user created content that does not distinguish natural or legal persons as long as they act outside of "professional routines and practices". Hence, their trust and legal security could be enhanced so as to participate with greater anticipation in the knowledge based economy.

Enlarge private use exception – The private use exception is difficult to apply to the context of the Internet, where publishing activities can easily reach a global audience. For that reason such activities might not fall under the notion of private use since the Internet by definition is not a private but rather a public tool. In addition it has been argued that the private use exception might fail to pass the "three step test" because the act of copying might not fall under “certain special cases” since over the Internet copying is the rule and not the exception. We therefore encourage to enlarge the private use exception, so that it also covers internet publishing activities undertaken by consumers.

326 L. GUIBAULT, Wrapping information in contract: how does it affect public domain?, p.2
327 L. GUIBAULT, Accommodating the needs of i-Consumers: Making sure they get their money’s worth of digital entertainment, p.10, available at www.ivir.nl/publications/guibault/Lucie_Guibault_Accomodating_The_Needs_Of_iConsumers.pdf
328 Ibid. It should be noted, however, that these rules currently only apply to consumers (not to legal persons or enterprises)
329 European Parliament resolution of 21 June 2007 on consumer confidence in the digital environment (2006/2048(INI)), 2006/2048 (INI), recital 38
330 Ibid, recital 10 (4)
331 Ibid.
7.2. **Meeting business requirements**

7.2.1. **Resolving the issue of rights management**

In the online world, the principle of territorial exploitation of copyright creates obstacles to an Internal Market in rights management, due to the fact that when exploitation extends to more than one Member States, different rules apply. The variety of rules applies both to individual management of rights as well as to collective management. As was clearly mentioned in the 2004 Communication for the Management of Copyright and Related Rights in the Internal Market, a lack of common rules regarding the governance of collecting societies may potentially be detrimental to both users and rightholders as it may expose them through different conditions applying in various Member States as well as to a lack of transparency and legal certainty.

7.2.2. **Promoting multi-territorial licensing agreements**

In order to foster investments, contractual copyright provisions should guarantee business players a sufficient degree of legal certainty. This could, for example, be achieved through predetermined contractual terms, which lead to less time and money spent during the preparatory stage of an transaction. Indeed, as it has also been suggested previously, "so far as it is commercially viable and consumer desirable, content producers should be able to make distribution deals without excessive technical, legislative and regulatory obstacles".

At the same time, commercial players need licensing policies that correspond to the ubiquity of the online environment. It would therefore be appropriate to further encourage the adoption of multi-territorial licensing in order to increase legal certainty of commercial users and foster the development of legitimate online services.

An example could be taken from the rules adopted in the Commission Recommendation of 18 May 2008 on collective cross border management of copyright and related rights for legitimate online music services. According to this Recommendation, there should be no difference in the treatment of rightholders by rights managers on the basis of the Member State of residence or nationality: rightholders should be able to properly license their works throughout the territory of the European Union. In addition, it has been supported that multi territory licences should follow the general rule that different types of licences and practices apply to different types of content.

As was mentioned in the 2004 Communication on the Management of Copyright and Related Rights in the Internal Market, an option to the issue of community wide licensing could be to adopt the model chosen for the satellite broadcasting sector under the Directive 93/83/EEC for the rights of communication to the public and making available to the public. According to article 1(2)(b) of this Directive:

---

333 Ibid.
336 Creative content online in Single market, as above, p.6 (COM 2007) 836
Directive, the relevant act of communication to the public “occurs solely in the Member State where, under the control and responsibility of the broadcasting organisation, the programme-carrying signals are introduced into an uninterrupted chain of communication leading to satellite and down towards the earth” 339. However, in the same Communication it has been also stressed that if this model is applied to copyright and related rights without limiting the contractual freedom of the parties, as was done under Directive 93/83/EEC, it does not necessarily yield the desired result of multi-territorial licensing, as it only determines the applicable law and does not by itself result in extending the license to the area.

7.2.3. Fostering security in the relationship between rightholders and collective rights managers

In most Member States, there is only one collecting society for each group of rightholders in each territory in respect of the collective management of their rights. For this reason, it is necessary that the principles of good governance, non-discrimination, transparency and accountability of the collecting society are followed and respected 340. As was underlined in the 2004 Communication, these principles should apply to the acquisition of rights, the conditions of membership, of representation and to the position of the rightholders within the society 341.

Several interesting ideas to counter the currently fragmented Internal Market can also be found in Directive 93/83/EEC 342. This Directive sets forth several important provisions on licensing, some of which could be used as an example for general copyright licensing issues. If adopted under a technological neutral wording, they could be used as the basis to deal with important licensing problems of digital content. They could be also used as a useful tool to confront the lack of actual harmonization of the rules on collecting societies.

This position is also shared by the European Commission: in a recent speech 343, Commissioner Reding stated, with respect to the issue of fragmented licensing: "We had a similar problem when commercial satellite TV started more than 30 years ago. As right clearance for this per se cross-border service became increasingly complex, Europe developed the Cable and Satellite Directive and introduced a simplified system of rights clearance for the whole of Europe. I believe it is now time to develop similar solutions for the evolving world of online content."

A first useful element is the extension of a collective agreement between a collecting society and broadcasting organisations concerning a given category of works, to other rightholders of the same category which are not represented by the collective society 344. This could facilitate licensing mechanisms by extending their positive achievements to more rightholders. The underlying idea is to avoid a situation where rightholders of broadcasts programs not represented by a collecting society would be enabled to individually enforce their rights thus creating interruptions in retransmitted programs. This reasoning too could be used as a general rule to be followed in other licensing models as well 345 346.

340 Ibid.
341 Ibid. p.19
342 Official Journal L 248, 06/10/1993, p. 15-21
344 Articles 3 and 9 of the Directive
345 T. DREIER and P.B. HUGENHOLTZ, Concise European Copyright Law, p. 280
Another useful element is art. 11 of this Directive, which introduces the establishment of a mediation system when an agreement of an authorization of the cable retransmission of a broadcast is not reached. This can be considered as a measure to facilitate contractual solutions further introduced to avoid deadlocks of contractual procedures.

A third element is that the relationship between rightholders and collective rights managers, whether based on contract or statutory membership rules, should include a minimum protection for rightholders with respect to all categories of rights that are necessary for the provision of legitimate online services.

**Relation between collecting societies and the end users** – The fact that collecting societies usually have a wide repertoire and dispose an exclusive mandate for the administration of rights in relation to each field of activity brings them in a stronger position if compared to users. As a response to users' complaints regarding the tariffs and the licensing conditions, we endorse the 2004 Communication’s suggestion that societies should be obliged to publish their tariffs and grant a license on reasonable conditions. Additionally, it is important for the users to be able to contest the tariffs through different methods (courts, mediation tribunals, public authorities)\(^\text{347}\).

As it was stated in the aforementioned Communication, "for both the off-line and on-line exploitation of intellectual property, more common ground on several features of collective management is required"\(^\text{348}\).

In any case more efficiency and transparency should be achieved in the field of collective management.

### 7.2.4. Adopting codes of conduct

Copyright protection bestowed to the rightholder is regulated both by the legal provisions and the terms and conditions of the licensing agreements between the parties. In a digital context, those contracts are typically standard contracts that contain clauses that are predefined by the rightholder and refer to an unidentified number of recipients/users. Accordingly, users are "obliged" to accept the terms without previously negotiating with the rightholder ("take it or leave it").

**Promoting codes of conduct** – The European Commission and the Member States should encourage the creation of codes of conduct (or of standard (sector-specific) licensing clauses) tailored to the needs of both the rightholders and the users in those market sectors that these codes are required by the stakeholders. Such codes of conduct can address issues such as transparency and fairness of contractual terms, and they could act as an incentive for all stakeholders to voluntarily comply with contractual terms regarding digital content.

Moreover, codes of conduct can increase trust between the sector specific digital content players. The creation of codes of conduct and of standard terms would bring together all stakeholders to discuss and to decide on the most crucial issues and problems related to the protection of digital content.

**Viability** – Obviously, the success of such measures depends on the active involvement of all stakeholders in the creation of the codes of conducts. However, stakeholders in the private sector will often be incentivised to develop codes of conduct, as they generally consider self-regulation to be more

---


\(^{348}\) Ibid. p. 19
efficient, more convenient and better adapted to their needs, while at the same time reducing enforcement costs.\textsuperscript{349}

In this vein, some business stakeholders have explicitly expressed the opinion that it is necessary to permit the market to self-regulate. During the public consultation of the Communication on "Creative Content Online in the Single Market" in July 2006 among the comments received, emerged the argument that "there exist an absence of Commission's premature intervention with legislation in a nascent and fast evolving market, raising questions on the necessity of adapting legislation instead of permitting market models evolve themselves\textsuperscript{350}". In line with the above, there were also contributions calling the Commission to encourage cooperation between industry, right-holders and consumers\textsuperscript{351}.

As analysed above, it is perceived that the law has in several occasions adopted generic legal notions that are not always easy to construe. It has been also commented that some stakeholders feel that certain of the provisions adopted by the Copyright Directive are not suitable to meet their current needs. For this reason, sector-specific codes of conduct with precise updated provisions that tackle the current needs and requirements of each different category of digital content, could be more suitable and could provide an effective solution to tackle with the different sector specific problems that appear.

**Common acceptance** – In order to achieve maximum acceptance of the codes of conduct, it is necessary that all the sector-specific stakeholders agree on the basic rules set out in those codes, and feel secure and able to participate in the digital content chain: "creating a secure environment through contractual agreements that incorporate shared values of the contracting parties is the way to promote self enforcement into the contract\textsuperscript{352}". Fairness of the contract is likely to lead to voluntary compliance which could be the most fruitful long term practice for the protection of copyright throughout the Single Market.

They could, for example, agree on issues such as pre-contractual information required in relation to the technical features of the products and services, the compatibility and the playability of files devices, the issue of on line contracting on copyrighted material, issues of multi-territorial licensing, etc. For instance, some players in the market have already expressed their willingness to enter into a dialogue with other stakeholders on the basis of the points raised by the Communication on Creative Content Online in the Single Market\textsuperscript{353}.

### 7.2.5. Promoting the adoption of registration formalities for digital content copyright?

**Issue** – The user-created content phenomenon and the orphan work issue greatly influence business players. For example, due to the lack of formalities to receive copyright protection, it is complicated for someone who wants to use an existing work to find the rightholder and to obtain the permissions required\textsuperscript{354}. This could cripple creativity, since those willing to develop digital content may find it difficult

---


\textsuperscript{350} On Creative Content Online in the Single market, 3/01/2008, p.3 (COM (2007) 836)

\textsuperscript{351} Ibid.

\textsuperscript{352} Promoting innovation and economic growth: the special problem of digital intellectual property a report by the digital connections council of the committee for economic development, 2004, p. 74


\textsuperscript{354} See section 3.7.5 above
to build upon previous works that are not registered or recorded in any repository\textsuperscript{355}. For that reason there have been some arguments claiming that new ways to license copyright or new technologies to facilitate licensing could be explored in order to provide solutions for this matter.

Repository – According to the 2007 OECD study: "this could, for example, involve the creation of clearing houses/centres for the attribution of rights to UCC and other creators"\textsuperscript{356}. In line with the above, Prof. LESSIG uses the example of the decentralised domain name system to propose a similar system which could be created for the registration and renewal of copyrights. This idea – which would require an amendment of the TRIPS treaty and the Berne Convention – resides in creating a "repository" where only work that is considered by its author(s) as valuable would be registered and as such protected by economic copyright rules, whereas work that is not registered would be free content (governed by the rule of freedom of access at no cost) where only moral right rules would apply (or even not)\textsuperscript{357}. In a similar vein, the Gowers Review in Great Britain has suggested that the local Patent Office should establish a voluntary register of copyright either on its own, or through partnerships with database holders\textsuperscript{358}.

Hence, according to these proposals, by introducing these formalities much of the uncertainty found in the digital content could be overcome. It would enable those who wish to create and/or re-use content by using digitally accessed works to identify whether the content is free or not, to locate the rightholder, to assert those rights and to renew the declaration of rights when necessary\textsuperscript{359}.

Evaluation – The 2007 OECD study stresses that these kind of suggestions "rely on drawing a dividing line between commercial and non-commercial work which may however be difficult to establish taking into account the diversity of UCC services and related business models. Moreover, the suggested benefits from such new approaches would have to be weighed very carefully against their costs, including, for example, to the established commercial content industry which produces significant economic value"\textsuperscript{360}. The copyright system as it is in force today in most of the counties worldwide (where no formalities are required) has been established following International Treaties and international consensus on the matter. More specifically, art. 5 par. 2 section a) of the Berne Convention lays down that "the enjoyment and the exercise of these rights shall not be subject to any formality"\textsuperscript{361}. It is thus understood how fundamental the principle of lack of formalities regarding the protection of the work under copyright is and how the existence of a repository would be equal to a well structured formality. Hence, we realise that this suggestion can only be implemented in the long term. Nonetheless, this seems like an interesting idea for further discussion, provided that a proper balance is achieved.

Alternative – In addition, or as an alternative to, the idea to install a repository for copyrighted works, we recommend to include an exception where the use of an orphan work would not lead to copyright infringement when a diligent, good faith search has been conducted to find the rightholder (see the detailed analysis above). When the rightholder of the alleged orphan work would then show up, only a fair and reasonable compensation would be necessary.

\begin{thebibliography}{9}
\bibitem{356} Participative Web and User Created Content, OECD 2007, p. 82
\bibitem{357} L. LESSIG, \textit{Free culture}, o.c., p. 286 - 291
\bibitem{358} Gowers Review of Intellectual Property 2006, o.c., p. 6
\bibitem{359} L. LESSIG, \textit{Free culture}, o.c., p. 286 - 291
\bibitem{360} Participative Web and User Created Content, OECD 2007, p. 82
\end{thebibliography}
7.2.6. **Clarifying the role of online intermediaries**

The role of intermediaries should be clarified, in particular with respect to the possibility to issue injunctions. We refer to our recommendations in Chapter 6 (liability of online intermediaries) for more information on this subject.

7.2.7. **Adoption of effective enforcement measures**

Enforcement mechanisms are of paramount importance for the success of the Single Market\(^{362}\). Although some progress to reach that goal has been made by the Enforcement Directive, however several issues remain unresolved.

One of the most important challenges is to define which law applies in case of a copyright infringement. It should be envisaged to adopt measures that indicate the application of a single law to all acts of infringement. Although there are no clear answer to this matter, the legal doctrine has mentioned some points of attachment that could be useful for further discussions\(^{363}\):

- the normal rule should be that the law applicable in an infringement issue should be the law of the country in which the server that hosts the infringing content is located
- if the application of the normal rule does not meet the minimum standards laid down by the Berne Convention and TRIPs, the law of the country where the operator of the website with the infringing content has its residence or principal place of business can be used;
- in other cases, the law of the forum can be applied; provided it meets the minimum standards of the Berne Convention and TRIPs Agreement.

7.3. **Promoting the fair balance of rights between the interested parties**

As it has been stated in the 2009 Communication on "Copyright in the Knowledge Economy", the dawn of the online culture of sharing and swapping, data mining and interactive learning, has exposed a difference of views between those who wish to move toward a more permissive system of copyright and those who wish to preserve the status quo. The challenge is to reconcile these interests\(^ {364}\). In addition, according to the Corrigendum to the Directive 2004/48/EC "the demand for quality digital content in Europe with balanced access and user rights, by a broad community be they citizens in society, students, researchers, SMEs and other business users, or people with special needs wishing to augment their knowledge, or 're-users' wishing to exploit digital content resources to create services, is increasingly apparent"\(^ {365}\). Hence, the fair balance of interests and rights between the distinct participants to the digital content environment is a necessity that has to be reached. For that reason, among others, the following important issues must be considered.

7.3.1. **Dealing with copyright infringements**

The topic of digital copyright infringements is very difficult to deal with, as it touches the very core of the digital copyright debate.


\(^{363}\) Ibid, p. 245

\(^{364}\) COM (2009) 532 final, p.4

Distinction between different types of infringements – A clear distinction should be made between consumer-level copyright infringements and commercial-scale copyright infringements. Recital 14 of the Enforcement Directive already contains a first step in this direction, by distinguishing between commercial and non-commercial acts of infringement: "acts carried out on a commercial scale are those carried out for direct or indirect economic or commercial advantage; this would normally exclude acts carried out by end-consumers acting in good faith".

Countering consumer-level copyright infringements – While consumer-level copyright infringements are widespread (particularly among minors/digital natives), sincere caution must be taken into account when adopting measures, because many of these infringements do not have any profit motivation, as they are conducted by private users for personal use. We are convinced that the long-term solution towards consumer-level infringements does not lie only with the adoption of legal instruments, but should also be found in a combination of education and user awareness, making available legal content (in part by adopting new business models), and balanced DRM measures.

This aligns with the Digital Britain report, which stated that "The civil infringement of taking someone else’s intellectual property or passing it on to others through file-sharing without any compensating payment is, in plain English, wrong. However, the Government also believes, and the evidence suggests, that most people, given a reasonable choice, would much prefer not to do wrong or break the law. The objective of the Government’s policy is therefore three-fold. Firstly, to provide a framework that encourages the growth of legal markets for downloading that are inexpensive, convenient and easily accessible to consumers."

The Commission must encourage the creation of policies and business models that aim at "discouraging piracy and increasing incentives to purchase content – while maintaining the balances inherent in copyright law". In this vein, the adoption of Codes of Conduct and of standard licensing clauses based on principles such as fairness, transparency and fair balance of the parties’ rights could be a useful tool. This way all parties would know and accept their rights and obligations in advance and would interact within a secure and trustworthy environment. We believe it is better to rely on consumers’ acceptability of the rights and obligations set in specific licensing agreements than drafting unilateral licenses with strict rules that would be impossible to enforce and to impose to non-complying users.

At the same time, we do not believe that new legal provisions should be undertaken to attack consumer-level copyright infringements with civil and/or criminal sanctions that could undermine the fundamental human rights. This was also recognised by the ECJ in the Promusicae v. Telefonica case for privacy issues.

---


368 Case C- 275/06, Productores de Musica de Espana (Promusicae) v. Telefonica de Espana SAU

369 Promusicae made an application to the Commercial Court No 5 of Madrid for preliminary measures against Telefonica asking for an order of disclosure of identities and physical addresses of several customers that were found to illegally exchange copyrighted materials through peer-to-peer software. The Court referred to the ECJ for a preliminary ruling asking "whether Community law, in particular Directives 2000/31, 2001/29 and 2004/48, read also in the light of Articles 17 and 47 of the Charter, must be interpreted as requiring Member States to lay down, in order to ensure effective protection of copyright, an obligation to communicate personal data in the context of civil proceedings" (nr. 41). The ECJ answered that "the Member States must, when transposing the directives mentioned above, take care to rely on an interpretation of the directives which allows a fair balance to be struck between the various fundamental rights protected by the Community legal order. Further, when implementing the measures transposing those directives, the authorities and courts of the Member States must not only interpret their national law in a manner consistent with those directives but also..."
Furthermore, the controversial relationship between anti-infringement measures and the right to freedom of speech has also been repeatedly pointed out. While copyright is considered as one of the means to secure freedom of expression at the same time, it is also considered as antithetical to the freedom of expression since it prevents all but the rightholder from expressing information in the form protected under copyright law. Therefore, an equilibrium must be reached so that copyright will be used in a way that will reward the labor of the author, but at the same time promote the freedom of expression and the progress of science, respect the user's privacy and personal data and cultivate creativity of digital content.

In addition, any legal provisions against consumer privacy that do not restore the fair balance between rightholders and users would strengthen the ongoing "copyright war" on consumers — particularly minors. As pointed out by Prof. LESSIG:

"Thus we must keep in mind the other values or objectives that might also be affected by this war. We must make sure this war doesn't cost more than it is worth. We must be sure it is winnable, or winnable at a price we're willing to pay. I believe we should not be waging this war. I believe so not because I think copyright is unimportant. Instead, I believe in peace because the costs of this war wildly exceed any benefit, at least when you consider changes to the current regime of copyright that could end this war while promising artists and authors the protection that any copyright system is intended to provide. (...)"

In a world in which technology begs all of us to create and spread creative work differently from how it was created and spread before, what kind of moral platform will sustain our kids, when their ordinary behavior is deemed criminal? Who will they become? What other crimes will to them seem natural?"

At the same time we consider that the direct attack of consumer pirates is not efficient for the rightholders too since it is very costly and time consuming to turn against individuals that reside in different Member States. Additionally Court decisions are not easy to enforce against individual users. For all these reasons, we reject the increasing trend to thwart consumer privacy by directly attacking consumers.

**Countering commercial-level infringements** – Commercial-level infringements, on the other hand, should be tackled from an entirely different perspective. The current legal instruments must be reinforced to better tackle these infringements. Under the current legal framework, it is still too difficult and too costly for rightholders to fight these types of infringements, and it is too easy for these "pirates" to get away with their activities. We therefore strongly recommend the Commission to encourage Member States to take these infringements very seriously, to increase cross-border cooperation and to strengthen current criminal and civil sanctions. In this vein, the most recent legislative initiative was a proposal for a

---

370 T. LOVERDOU, Copyright and freedom of expression : confluences and conflicts – a general overview abstract
371 Ibid.
372 L. LESSIG, Remix – Making Art and Commerce Thrive in the Hybrid Economy, 2008 (preface)
Directive\textsuperscript{373} that would fill the gap created by the implementation of the Enforcement Directive. Although the latter Directive provided measures, procedures and civil and administrative remedies, it lacked the penalties to make enforcement procedure complete. The new proposal for a Directive regarding criminal measures stipulates in article 3 that Member States must consider all intentional infringements of intellectual property rights on a commercial scale as criminal offences. Although this proposal has been criticised for being too vague and too wide, it promised to be an important instrument against the worst infringements. However, the proposal has not yet been adopted.

Furthermore, we recommend that data protection legislation should be adapted in such a way that alleged privacy and data protection infringements can no longer be invoked by commercial copyright infringers as a procedural defense to escape their responsibility. The further refinement and adoption of the Directive regarding criminal measures (see section 1.2.2) should therefore be undertaken.

Care should be taken, however, to not confuse real commercial-level infringements with new online business models, for which the legality lies within a "grey area". If those new business models would be treated as a type of commercial-level infringements, the further uptake of online service provision may become endangered. Therefore, the threshold towards qualification as commercial-level infringements should be sufficiently high.

7.3.2. Correct adjustment of the interpretation of the "three step test"

\textbf{Issue} – The "three step test" and its interpretation have been the object for discussions in legal circles. As argued above (section 4.1.2), the test suffers from a lack of direction as to where the line between grants and reservations of copyright should be drawn.

\textbf{Solution} – The correct adjustment of the test seems to be the only way to balance the confronting interests of excessive rightholders protection on the one hand, and infringements that are exercised under the pretext of new privileges granted to content users on the other hand. As it has been pointed out "a proportionate balance between grants and reservations can serve as a reference point for the application of the three step test". To achieve this, a solution could be to "work on transitory measures to improve the understanding of the three step test to ensure that exceptions have broadly similar impact at national level and are interpreted with sufficient permissiveness to promote innovation"\textsuperscript{374}. Some commentators argue that the European legislator should provide some guidance regarding the proposed role of the court in the interpretation of the test as well as in the function of the test itself as an interpretative tool\textsuperscript{375} \textsuperscript{376}. According to those arguments, "clarification would probably equal to flexibility in the application of the 'three step test' by avoiding a narrow interpretation of the first and second steps while making the third step which enables balancing of the interest of the owners and of public policy, a focal point of the interpretation"\textsuperscript{377}.

\textsuperscript{373} Amended proposal for a Directive of the European Parliament and of the council on criminal measures aimed at ensuring the enforcement of intellectual property rights, (COM (2006)168, final)

\textsuperscript{374} GOOGLE, Comments to the Green Paper on Copyright in the Knowledge Economy at the European Commission, p. 8

\textsuperscript{375} Study on the implementation and effect in Member States ‘ laws of Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society, Institute for Information Law, 2007, p. 73

\textsuperscript{376} Some stakeholders even urge the Commission to introduce "a further step to the three-step principle". According to this opinion "the fourth step should be that the legitimate interests of the right holder should not be detrimental to the world-wide progress of knowledge and to the information needs of the public": AIB, Comments to the Green paper on copyright in the knowledge economy of the European Commission, p. 4

\textsuperscript{377} Ibid.
7.3.3. Adoption of mechanisms to deal with orphan works

**Issue** – Orphan works, i.e. copyrighted works of which the rightholders cannot be identified, cannot be digitised, reproduced or disseminated, because these actions require the consent of the rightholders.

**Solution** – Sector-specific criteria for diligent search should be established in the Member States to enable tracing of rightholders. Such searches should be made subject to the principle of mutual recognition. Databases of orphan works should be created to allow interested parties to easily assess the copyright restrictions resting on a particular work. In addition, a rights clearance mechanism should be developed to allow for the grant of non-exclusive licences of orphan works.

The rights clearance mechanism could take the form of an extended collective licensing mechanism, an independent body responsible for granting the licences or a copyright exception permitting the use of genuine orphan works.

Regardless of the option chosen, national solutions will need to take into account issues of mutual recognition in Member States to achieve the necessary cross-border effects. Such efforts can be supported by creating databases, shared at European level, of declared orphan works. To simplify such centralisation efforts, it could be considered to encourage Member States to adopt harmonised solutions to the problem of orphan works in their national legislation.

7.3.4. Modifying the exceptions and limitations of the Copyright Directive

As it has been analysed previously in section 3.3, the optional character of article 5 of the Copyright Directive creates difficulties in the Single Market. It should be recognised, however, that this is a highly controversial subject since a lot of different views exist between the various stakeholders.

a) On the one hand, there are those stakeholders that argue to modify the current exceptions and limitations system.

From the consumer's perspective it has been proposed that "(copyright exceptions) should at least become mandatory in order to shield them from contractual overrides"\(^{378}\), while the lawful uses should be "fortified" in such a way that the rightholders would not be able to circumvent the rights or/and exceptions to the reproduction right. The mandatory list of exceptions and limitations would then become obligatory for all Member States, in order to enhance harmonisation and legal certainty within the Single Market and to set the requirements for a more business-friendly environment.

Some professional organisations also plead to modify the current exceptions systems. For example, the Italian Association of Bibliothèques, (Associazione Italiana Biblioteche) supports that "the full balance of interests of equal importance, the full harmonization of national laws, as well as the fundamental purpose of the Directive, namely the affirmation of an open and competitive European market, will be realized only when the exceptions will become mandatory, and they will be clarified and/or enlarged to prevent misunderstandings or narrower implementations"\(^{379}\). It has also been argued that "it is important not to construe the protection of copyright and promotion of copyright exceptions as contradictory objectives, or the interests of sectors relying on exceptions as opposed to the interest of sectors relying on protection. On the contrary, these are complementary objectives and interests that are both fostering the development of knowledge and creation and their dissemination"\(^{380}\). In addition, some stakeholders

---

\(^{378}\) G. MAZZIOTTI, o.c., p. 88

\(^{379}\) ASSOCIAZIONE ITALIANA BIBLIOTHECHE, Comments to the Green Paper on Copyright in the Knowledge Economy at the European Commission, p. 3

\(^{380}\) GOOGLE, Comments to the Green Paper on Copyright in the Knowledge Economy at the European Commission, p. 3
claim that due to the non-mandatory approach of the limitations and the exceptions "the [Copyright Directive] has failed to open the Internal Market to copyright products as was intended".\footnote{FOBID, Comments to the Green Paper on Copyright in the Knowledge Economy at the European Commission, p. 6}

At the same time others argue that: "there is an integral link between limitations and exceptions and fundamental human rights as expressed in the United Nation’s Universal Declaration of Human Rights".\footnote{Green Paper – Copyright in the Knowledge Economy Response of the Conference of European National Librarians (CENL), p. 6} Hence, they recommend that the fundamental human rights that are expressed by some of the limitations and exceptions\footnote{for example in articles 5.2.b, 5.3.a, 5.3.b, 5.3.c and 5.3.d} should be mandatory.

Some stakeholders attack the fact that the list of exceptions and limitations is exhaustive, since they are of the opinion that "it keeps the exceptions firmly in the twentieth century by limiting those available to provisions that have been found useful in the past".\footnote{Ibid. p. 2} Hence, according to this argument, the exhaustive character of the list could hamper future developments by forbidding the adoption of new limitations that could abide by the new technological trends. For that reason, it has been also proposed that the law can introduce "an obligatory, non-limited list of exceptions, leaving Member States the possibility to add 'national' exceptions which they deem necessary and which can be reconciled with the 'three step test'. That way, the rights of users and of right holders are both kept in balance".\footnote{INTERDISCIPLINARY CENTRE FOR LAW AND ICT (K.U.Leuven), Comments to the Green Paper on Copyright in the Knowledge Economy at the European Commission, p. 3} In the same vein, another proposal recommends that "Member States ought to be free to add exceptions which comply with the 'Three Step Test'".\footnote{UNIVERSITY OF LODZ, Comments to the Green Paper on Copyright in the Knowledge Economy at the European Commission, p. 4}

Other commentators argue that the current exceptions should be replaced by subjective rights, which would even be enforceable through court action. Speaking of "rights" instead of "exceptions" would place more emphasis on the fact that, in order to be effectively protected against access and usage restrictions, uses covered by copyright exceptions should be completely and effectively enforceable.\footnote{MAZZIOTTI, o.c., p. 288}

b) On the other hand there are others that claim that there is no need for any change to take place, as the current system created by the Copyright Directive is satisfactory.

For instance, there are those who argue that "restrictions should not be introduced to benefit economic interests regardless of whether these are public or private; when for practical reasons exceptions appear necessary [...] the legislator is better commanded to let stakeholders find practical solutions with negotiated agreements rather than by interfering in copyright law".\footnote{CEPIC e.e.i.g. (Co-ordination of European Picture Agencies Press Stock Heritage), Comments to the Green Paper on Copyright in the Knowledge Economy at the European Commission, p. 2} In addition; the Designs and Artists Copyright Society points out that "copyright, though partially harmonised, remains an intellectual property right which is strongly influenced by the culture and tradition of the respective Member State [...] the current system of non mandatory exceptions accurately reflects this understanding and constitutes the correct instrument to provide for sufficient flexibility for the Member States while guaranteeing a certain degree of harmonisation and security for users of copyright
protected work." In the same vein, others claim that this "local approach" "has many benefits, with lower costs of enforcement and review via member states' own domestic legislatures and courts."

It has also been stressed that "an exhaustive list of mandatory exceptions would have achieved an impression of harmonization, but the satisfaction would have been short lived and merely intellectual [...] such method would have inevitably sacrificed the principle of subsidiarity." The proponents of this argument underscore that "the regime of copyright exceptions established in article 5 of the Copyright Directive works well in practice." At the same time they emphasise that "in any case, any discussion concerning exceptions and limitations, even if only with reference to their application and interpretation, must take place with full respect for the 'Three-Step-Test' principle."

c) Evaluation

The previous arguments are only an indicative list of the various opinions that have been expressed by the diverse market players regarding the matter of the exceptions and limitations of the Copyright Directive. They reveal the profound differences that exist between the stakeholders on this issue. All the points raised however should be taken into account as the starting point of a discussion on the issue at stake (see below), since it is essential for the efficient functioning of the Single Market that all those that participate in it feel secure and satisfied.

From the point of view of the Single Market, a set of fully harmonised exceptions and limitations would enhance legal certainty for both the rightholders and the users. In addition it would limit the costs of licensing drafting for those who wish to uphold cross border on line digital content trade and/or for those who wish to use their DRM systems to protect their work within all the Member States of the Single Market. At the same time it would improve the co-operation between the different Member States in the effort to tackle digital copyright infringements and to deal with all the issues related to copyright infringements. All of the above are in line with article 118 of the Lisbon Treaty which as it has been already stressed in the introduction of the present chapter, stipulates that "in the context of the establishment and functioning of the internal market, the European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall establish measures for the creation of European intellectual property rights to (emphasis added) provide uniform protection of intellectual property rights throughout the Union and for the setting up of centralised Union-wide authorisation, coordination and supervision arrangements."

838 DACS (Designs and Artists Copyright Society), Comments to the Green Paper on Copyright in the Knowledge Economy at the European Commission, p. 2
839 ALLIANCE AGAINST IP THEFT, Comments to the Green Paper on Copyright in the Knowledge Economy at the European Commission, p. 1
840 ICMP (International Confederation for Music Publishers), Comments to the Green Paper on Copyright in the Knowledge Economy at the European Commission, p. 2
841 BSA (Business Software Alliance), Comments to the Green Paper on Copyright in the Knowledge Economy at the European Commission, p. 2
842 ASSOCIAZIONE ITALIANA EDITORI, Comments to the Green Paper on Copyright in the Knowledge Economy at the European Commission, p. 1
7.4. **Dealing with TPMs**

7.4.1. **Statutory provisions to encourage the development of PETs**

The Copyright Directive does not make the use of PETs mandatory, and does not instruct their direct use\(^\text{395}\). Consequently, PETs are not enforced by legislation and are not widely used. Although TPMs are a method to protect rightholder's legitimate interest nevertheless, these technological measures must not be used in a way that circumvents provisions regarding data protection. For that reason, statutory rules can be envisaged to protect a user's personal data, in order to enhance security of the user's privacy and avoid possible manipulation of his/her personal data\(^\text{396}\). It could be considered, for example, to impose statutory provisions for the protection of personal data when using TPMs. Direct instructions about their enforceability should be adopted, so that Member States would be obliged to adopt privacy protective measures in their TPMs regimes. This would also enhance user's security and willingness to accept TPMs/DRMs.

7.4.2. **TPMs and minimum uses**

Enforcement mechanisms and technological measures related to copyright protection should be flexible and effective without however affecting the user's lawful uses. The measures applied to secure access to the content should enable rights holders to protect their works, without disregarding the lawful uses bestowed to the user of the content. As pointed out in section 3.1, DRMs may deprive users from lawful uses permitted under the exceptions and limitations to the reproduction rights, effectively limiting various personal and transformative uses\(^\text{397}\). Current DRM technology is unfit to accommodate the myriad of possible transformative uses that copyright exceptions may prove to allow\(^\text{398}\).

It could therefore be envisaged to adopt rules that would narrow force technical measures to take into consideration that consumers in the online environment should be able to interact with the content. "Right holders and DRMs creators should not use DRMs to lock out disfavoured digital media device and software creators by refusing those licenses"\(^\text{402}\). In this regard, rightholders should be obliged to adopt a "fair use by design" approach for TPMs\(^\text{403}\).

---

\(^{395}\) See section 3.1

\(^{396}\) Copyright Law and Consumer Protection, o.c., p.23

\(^{397}\) Content and control: Assessing the impact of policy choices on potential online business models in the music and film industries, Berkman Center for Internet Society,p.11

\(^{398}\) MAZZIOTTI, o.c., p. 228

\(^{399}\) COM (2009) 532 final, p.8

\(^{400}\) Ibid.

\(^{401}\) Ibid.

\(^{402}\) MAZZIOTTI, o.c., p. 228

\(^{403}\) MAZZIOTTI, o.c., p. 292
7.4.3. **Interoperability of TPMs**

The notion of interoperability bears different meanings: for **consumers**, interoperability is the enabler that allows them to choose/use different devices that still would not impede them from downloading different services. For **rights holders**, on the other hand, interoperability means the ability to use more that one channel for distributing their content. For **device developers**, interoperability means that they are able to extend their market to several and different content services. Even so, interoperability can at the same time, serve both the rightholder’s and the user's interests.

Therefore, it is necessary for all stakeholders to reach to a consensus on the basic framework in order for interoperability to be developed. In this context, some have suggested that "**DRMs should not become a commercial or technology licensing control point, thus stakeholders should continue to work on open cross platform DRM systems and standards and member states should be encouraged to foster open standards so that the security of DRM is not undermined**".

The viability of TPMs is closely related to their acceptance by users. If a copyrighted work is protected by TPMs that are not user-friendly, users will be discouraged to use the work. This fact should urge rightholders to adopt user friendly TPMs, which allow the normal processing of the work, secure its future readiness, promote its technological neutrality and at the same time allow technological interoperability. Apart from legislative intervention, technical standardisation should be used to improve technological interoperability. Open standards in TPMs marketplaces should be established that would allow different entities to create technically compatible equipment and services. In addition, the European Parliament Resolution on consumer confidence in the digital environment considers that consumers - in order to profit fully from such (on line) services and have their expectations fulfilled - need clear information on what they can and cannot do with regard to digital content, digital rights management and technological protection matters; is convinced that consumers should be entitled to interoperable solutions.

Furthermore, it could be envisaged to create a third party (e.g., a public agency) who could mediate between rightholders and consumers, and who could even be assigned the task to hand over a technically unrestricted copy of the requested work when rightholders refuse to cooperate.

Finally, another recommendation is to specify in the Copyright Directive that the legal protection of TPMs does not apply to the extent that a TPM does not grant users the right to exercise all their statutory exceptions. In this way, similar to the way the Software Directive allows reverse engineering to ensure compatibility, the Copyright Directive should not sanction users who deliberately circumvent TPMs in order to exercise their statutory exceptions.

---

404 Com (2007) 836 Creative content online in Single market, as above, p. 7
405 Ibid.
407 Ibid.
409 European Parliament resolution of 21 June 2007 on consumer confidence in the digital environment (2006/2048(INI)),2006/2048 (INI), recital 27
410 MAZZIOTTI, o.c., p. 229
411 MAZZIOTTI, o.c., p. 286
7.4.4. **Incorporating basic consumer protection in TPMs**

In line with the aforementioned Resolution of the European Parliament, consumer protection rules increase the information provided to consumers and grant protection against unreasonable one-sided contractual terms. It could be envisaged to develop legal obligations to clearly mark goods protected by TPMs with visible information regarding the TPMs used, and to explicitly inform users on the interoperability of the TPMs.

Some of these suggestions have already been adopted by the European Consumer Law Group with respect to the design and use of DRMs. It was held that copyright contractual provisions should promote a consumer friendly design of DRMs, so that DRMs will not conflict with the legitimate rights and interests of consumers, notably privacy rights. In addition, DRMs should be designed to avoid impeding normal processing of the content and consumer’s ability to benefit from innovations and technological progress. The Group also held that legislation must be drafted in such way to force rightholders to design DRMs to satisfy also the needs of persons with special requirements. Finally, it was proposed that when DRMs cause damage to the property of consumers, the controllers of the DRMs should be considered liable for that damage.

7.5. **Start a fundamental copyright debate**

Statutory provisions with regards to copyright protection must focus on the true balance of interest of the participating parties. As emphasised in the 2008 Green Paper, “technologies and social and cultural practices are constantly challenging the balance achieved in the law, while new market players such as search engines, seek to apply these changes to new business models.” Thus the balance provided by the law must stay in line with the ongoing changing digital environment. This is a difficult goal to achieve, since in many occasions the interests of the participants are contradictory and collide with each other.

Even though we are convinced that our recommendations above will significantly contribute to restoring the currently skewed balance, we think a fundamental copyright debate is necessary, because ad hoc measures and stopgaps do not fundamentally resolve the issues at stake. We therefore welcome the recent reflection paper of the European Commission.

**Copying: from exception to rule** – Current copyright legislation was conceived in the analogue era, where copies were an exception and would almost always lead to a decrease of quality. In a digital environment, however, copying is the rule and no longer the exception. Any use of a work – even mere consultation – leads to many partial or entire copies of the initial work, each of which is of the same quality as the initial work. Conversely, many uses of the same work in an analogue environment (reading, lending, selling, ...) are not regulated by copyright law. In other words, there has been a shift...
from an environment where copying is the exception and inherently leads to inferior copies, to an environment where copying is the rule and copies are identical to the initial work. The law, however, still reflects the analogue ideas, where permission must be obtained for each copy (unless an exception would apply).

**Automatic protection** – Another example where the law does not reflect today's reality, is in the automatic copyright protection afforded to most digital content. Although it is not contested that an important portion of this digital content should receive automatic protection (e.g., films, music and novels), the question arises to which extent content should be protected for which the "creative inspiration" was very low (e.g., user comments on a forum, or occasional photos taken by consumers with their point-and-shoot cameras), which was automatically created by computer software, or for which the rightholder cannot be found (orphan works). Copyright laws were conceived in an era where content production was expensive, and only a limited selection of content was made publicly available. Conversely, content production has become very easy, and content is literally only a mouse click away.

**Copyright paradox** – Consequently, current copyright laws do not appropriately reflect the day-to-day reality on the Internet, where users copy photos, music and texts without permission — often unaware of the fact that they breach the law (particularly when the user is a minor). These users are caught in a fundamental "copyright paradox": never before have copyrighted works been so important to consumers (and minors in particular), yet never before have users disrespected copyright in this amount.

Aware of this paradox, rightholders start lawsuits against direct and indirect copyright infringers, hesitate to sell digital works online due to the risk of infringements, or sell digital works that are DRM-protected and consequently do not allow users to enjoy their legal exceptions. One observer would point out that users are stealing digital property and that this attitude must be stopped, another observer would point out that the established business models of rightholders are no longer appropriate and that rightholders must find alternative models instead of spending energy on copyright wars. As noted by Commissioner REDING: "(A)re there really enough attractive and consumer-friendly legal offers on the market? Does our present legal system for Intellectual Property Rights really live up to the expectations of the internet generation? Have we considered all alternative options to repression? Have we really looked at the issue through the eyes of a 16 year old? Or only from the perspective of law professors who grew up in the Gutenberg Age? In my view, growing internet piracy is a vote of no-confidence in existing business models and legal solutions. It should be a wake-up call for policy-makers."  

**Economic and societal effects of copyright infringements** – The effects of copyright infringements may not be so obvious as may be intuitively felt at first glance. Both scientific and anecdotal evidence suggests that there are, in fact, many beneficial effects linked to some forms of copyright infringements. Similarly, it has been pointed out that from a historical perspective, each threat to copyright protection due to the introduction of new technologies (from the printing process to the

419 L. LESSIG, Free culture, o.c., p. 143
421 See, for example, the 2009 study from Frank N. Magid Associates, which concludes that users of illegal peer-to-peer networks generate more legal turnover for the media industry than other users: "the P2P user attends 34% more movies in theaters, purchases 34% more DVDs and rents 24% more movies than the average Internet user." - see www.businessinsider.com/chart-of-the-day-content-stealers-spend-a-ton-on-media-2009-8
phonograph, radio and VCR) eventually turned out very beneficial to rightholders\textsuperscript{422}, and that the figures used to describe the impact of the copyright infringements phenomenon are not always correct\textsuperscript{423}.

**Conclusion: a fundamental debate is required** – We are of the opinion that the fundamental and highly complex opposition between the interests of online service providers, consumers and rightholders requires a fundamental debate, that goes well beyond mere legal issues. This debate must touch upon subjects such as the balance between copyright and privacy; balancing the rights of consumers in DRM'ed works; the threshold for copyright protection; copyright duration; fostering the public domain; multi-territorial licensing; etc. It is important for this debate to be held between three parties: online service providers, rightholders and consumers\textsuperscript{424}.

Although we are convinced that many improvements can be made to current copyright legislation, we think a more fundamental revision of copyright legislation is required, because merely tweaking a legal framework that may no longer be supported by a significant portion of the citizens, may not be sufficient.


\textsuperscript{423} For example, the official figures on the level of illegal file sharing in the UK seems to from questionable research commissioned by the music industry. See [www.pcpco.co.uk/news/351331/how-uk-government-spun-136-people-into-7m-illegal-file-sharers]{http://www.pcpco.co.uk/news/351331/how-uk-government-spun-136-people-into-7m-illegal-file-sharers}

\textsuperscript{424} In a speech in November 2008, EU Commissioner Reding criticised efforts at the EU and national level to narrow the digital content issue to two camps only. The “third camp” (consumers) must also be part of the equation. See [www.out-law.com/default.aspx?page=10377]{http://www.out-law.com/default.aspx?page=10377}
6. Liability of online intermediaries
Table of contents

Chapter 6 Liability of online intermediaries .................................................................2
1. Introduction...................................................................................................................2
2. Liability before the eCommerce Directive .................................................................3
   2.1. Introduction ...........................................................................................................3
   2.2. Member State overview: case law, legal doctrine and legislation ......................3
   2.3. Reasons to adopt EU-level measures ................................................................5
3. Liability under the eCommerce Directive .................................................................7
   3.1. Introduction to the special liability regime .........................................................7
   3.2. Characteristics of the special liability regime .................................................8
4. Issues linked to the special liability regime ...............................................................10
   4.1. Ambiguities in the definition of “information society services” ......................10
   4.2. Ambiguities in articles 12 (mere conduit) .......................................................14
   4.3. Ambiguities in article 13 (caching) ..................................................................14
   4.4. Ambiguities in article 14 (hosting) ..................................................................15
   4.5. No harmonised notice-and-takedown procedure .............................................19
   4.6. Possibility of to issue injunctions ......................................................................21
   4.7. Gaps in the scope of the special liability regime ..............................................24
   4.8. Result: considerable legal uncertainty .............................................................25
5. Liability of online intermediaries in the United States .............................................26
   5.1. Case law secondary liability for copyright infringements ..................................26
   5.2. Digital Millennium Copyright Act ....................................................................27
   5.3. Communications Decency Act .........................................................................31
6. Comparison with the United States .......................................................................33
   6.1. Less protection and more uncertainty for online service providers .................34
   6.2. More uncertainty for rightholders and users ....................................................34
   6.3. Examples ..........................................................................................................34
   6.4. Dual protection regime ....................................................................................36
7. Conclusions ..............................................................................................................37
8. Recommendations .....................................................................................................39
   8.1. Overview of recommendations ........................................................................39

This study was commissioned by the European Commission’s Information Society and Media Directorate-General, in response to the invitation to tender OJ 2007/S 202 244659 of 19/10/2007. The study does not, however, express the Commission’s official views. The views expressed and all recommendations made are those of the authors.
Chapter 6
Liability of online intermediaries

1. Introduction

On 4 June 2008, the French Civil Court of Troyes ruled that auction website eBay was liable of counterfeit for the sale of a counterfeited luxury bag by one of its customers. eBay was ordered to pay 20,000 EUR in damages, as well as a maximum of 15,000 EUR for publishing the decision in four different magazines. The Court also considered that eBay’s efforts to suppress counterfeit were not sufficient.

Less than one month later, the Commercial Court of Paris found eBay liable for infringing the selective distribution agreements of several perfume producers, and ordered eBay to pay 3,052,000 EUR in damages, as well as a maximum of to 15,000 EUR for publishing the decision. eBay was also ordered to remove from its systems all advertisements relating to the perfumes of these producers, under a penalty of damages of 50,000 EUR per day, despite eBay’s claim that there exist no filtering mechanisms that can effectively filter out all such advertisements.

Only one month later, on 31 July 2008, the Court of Brussels decided in a very similar case against eBay that eBay’s efforts to suppress counterfeit were sufficient, that eBay could not be held liable and that eBay cannot be required to actively monitor the auctions offered on its website. Almost one year later, the French Tribunal de Grande Instance issued a similar decision1, squarely contradicting the aforementioned French decisions.

Meanwhile, in the United States, the District Court of New York had ruled on 14 July 2008 in a similar case of alleged jewellery counterfeit, that eBay could not be held liable for trademark infringements. The plaintiff did not even bother to invoke any allegations outside trademark law, as US law and established US case law shields online service providers such as eBay from almost any form of liability triggered by third party content.

Although it is not uncommon for different Courts to decide differently in complex cases, the European eBay decisions are particularly remarkable when considering that in each of the cases, there were arguments why eBay could be considered a "hosting provider", which is shielded from liability by a set of rules set forth in the eCommerce Directive. However, the precise scope of these special liability rules is not clear, so that it is actually not surprising that each court applied these rules differently: according to the Court of Paris, these special liability rules did not apply at all, because eBay’s auction services do not only consist of hosting-related activities; according to the Court of Troyes, the rules only apply to a limited subset of the auction-related services; and according to the Court of Belgium, the rules simply did apply to eBay.

* *

The above cases are only the tip of the iceberg: across Europe, the special liability regime has been implemented in different ways in national systems, as well as diverging case law. Courts seem to have difficulties to apply the special liability regime, so that online intermediaries are increasingly exposed to lawsuits triggered by content provided by their users, which is particularly worrying in the "Web 2.0" era, where user-generated content has become a driving factor.

1 Tribunal de grande instance de Paris, 3ème chambre, 13 May 2009, L’Oréal et autres / eBay France et autres
This chapter therefore investigates the various issues surrounding the liability of online intermediaries — such as internet access providers, web hosting companies, content aggregators, Web 2.0 service providers and other "online service providers" — in order to investigate whether the current rules are still suitable, and which balance should be found to balance the rights of all stakeholders and foster the position of Europe in today's information society.

It should be noted that this chapter does not deal with all aspects of online liability of intermediaries. More in particular, it does not deal with the contractual liability (such as exclusions of liability in online terms and conditions). Furthermore, this chapter is limited to the liability incurred by intermediaries, excluding direct liability issues that do not involve intermediary roles (e.g., a party's own liability for harmful content created by it, or a party's own liability for direct copyright infringement). Also note that some of the issues touched by this chapter, are linked to topics investigated in other chapters, such as copyright and privacy issues. These issues will be discussed in the other chapters of this study.

2. Liability before the eCommerce Directive

This section provides a concise historical overview of how the liability of online intermediaries was treated by national laws and national case law. As will be explained below, the direction headed by case law and the divergences in national law have spurred to the adoption of the harmonising eCommerce Directive.

2.1. Introduction

As online service providers generally only have a limited degree of knowledge about the data they transmit or store, the liability allocation between online service providers and the persons who originally put such information online can be problematic. Although the liability issues faced by online service providers are caused by their customers or users, the service providers are an attractive target for legal action, as they are visible, well known, and their financial strength is likely to be greater than that of their customers or users.

Hence, long before the rise of e-commerce, internet intermediaries were already accused of defamation, copyright infringement and obscenity and indecency issues. As a reaction, some Member States started regulating certain aspects of their liability, often inspired by the established rules regarding publisher's liability. Pending such legislation, national judges mostly relied on general rules of contributory liability – including publisher's liability rules – to address the issue. Due to the difficulties to apply the established principles of publisher's liability to the new media, case law varied significantly, both within one Member State and across Member States.

2.2. Member State overview: case law, legal doctrine and legislation

Austria – Austria regulated the liability of online intermediaries by approving a federal bill to enact the Federal Telecommunications Statute in 1997, which held that owners of "broadcasting installations and terminals" (such as computer servers) were held liable, unless they would have taken appropriate and reasonable steps to prevent wrongful use of their equipment.

---


5 Study on liability of internet intermediaries, p. 30 and 47

Legal analysis of a Single Market for an Information Society – Liability of online intermediaries 3
France – To counter the protests arising after the confiscation of the computer equipment of two internet access providers Francenet and Worldnet, the Minister of Telecommunication introduced a bill in 1996 to limit the liability of online intermediaries. This bill exempted online service providers from criminal liability for third party infringements, provided they did not participate in these infringements, they offered filters to prevent access to certain services, and their services were not disapproved by the Committee of Telematics. The proposed amendment was, however, annulled by the Constitutional Council due to formal errors.

In the meantime, French legal doctrine reverted to general tort law and the general cascading system of liability for crimes committed by the press. Nevertheless, case law varied considerably. For example, in 1996, a court rejected a request to block access to negationist messages, because "an access provider [is] under no legal obligation to regulate the information available on the network (...) since the authors alone are liable in respect of such information". Conversely, another court ruled in 1998 that a hosting provider was obliged to monitor content providers to whom it rents out space. According to this court, a hosting provider had to demonstrate it had fulfilled its monitoring obligations, and had taken the necessary technical measures to stop the illegal activity, in order to be exempted from liability. In 1999, another French court assimilated a hosting provider with the director in charge of publications on an audio-visual communication service, but nevertheless concluded that control by the service provider was impossible because the transfer between the actual author and the public had taken place electronically and at high speed. Yet another court ruled in the same year that a hosting provider has a surveillance duty to not infringe third party rights.

The Netherlands – The liability of online intermediaries was first addressed in the Netherlands in Bridgesoft v. Lenior, in which a bulletin board operator was charged with direct copyright infringement, because it allowed its subscribers to upload and download pirated software. The court found the operator to be liable for copyright infringement, and also found that the operator had acted negligently since it should have been aware of the possibility of copyright infringements.

In the 1996 Scientology-case, several internet service providers were sued for copyright infringements, as they enabled the online publication of copyrighted work. In summary proceedings, the court’s president found the providers not to be liable, on the grounds that “they do no more than provide the opportunity to public disclosure, and that in principle, they are unable to influence, or even have

---

7 E. WERY, i.c., note 120
8 Decision 961378 DC, 23 July 1996, J.O. 27 July 1996, as referred to by E. WERY, i.c., note 121
10 Act on the Regulation of the Press of 1881. With the Act on Audiovisual Communications of 1982, this system of cascade liability was extended to apply to audio-visual communications (see K. KOELMAN and B. HUGENHOLTZ, "Online Service Provider Liability for Copyright Infringement", WIPO Workshop on Service Provider Liability, November-December 1999, available at www.ivir.nl/publicaties/hugenholtz/wipo99.pdf (last viewed 20 January 2009)
11 Paris Regional Court, 12 June 1996, Réf. 53061/96
13 Ava v. Infonie and others, District Court of Puteaux, 28 September 1999
14 Lacoste/Multimania, Esterel and Cybermedia, TGI de Nanterre, 8 December 1999
15 District Court of Rotterdam 24 August 1995, Informatierecht/AMI, 1996/5, p. 101
knowledge of the things disseminated by those who have access to the Internet through them\textsuperscript{16}. This decision was later on confirmed\textsuperscript{17}.

The Dutch Penal Code also provides for a cascade liability system for publishers or printers. In 1998, a bill was introduced to rewrite these provisions, to ensure that they would apply to all intermediaries, including online intermediaries. The proposal exempted online intermediaries from liability if they would reveal the identity of the infringer, provide all information necessary to identify the infringer, and take all reasonable measures to prevent any further dissemination of the infringing materials\textsuperscript{18}. The proposal was not accepted by the Dutch Parliament until after the introduction of the E-Commerce Directive.

**United Kingdom** – The United Kingdom was the first European country to specifically adopt legislation to limit online intermediary liability prior to the introduction of the E-Commerce Directive, although this legislation was limited to defamation issues. The Defamation Act of 1996 introduced an “innocent dissemination” defence for distributors of hard copy publications, as well as online service providers and internet access providers. It exempted online intermediaries from liability for third party materials, provided they could prove to have taken reasonable care with respect to the publication, and did not have any reason to believe that it contributed to the publication of a defamatory statement. However, in the first case in which these provisions were applied – *Godfrey v. Demon Internet*\textsuperscript{19} – the court ruled that the service provider could not take the advantage of this defence introduced by the Defamation Act, as it had failed to comply with the plaintiff's request to remove offensive postings from one of its newsgroups. The court therefore found that Demon did contribute to the publication of the defamatory statement.

**Germany** – Felix Somm, general manager of CompuServe Germany, was prosecuted for facilitating access to violent and child pornographic content stored in newsgroups accessible by CompuServe's customers. As a reaction, the Teleservices Act and Multimedia Law was adopted in 1999\textsuperscript{20}, which established criteria for the liability of online intermediaries and exempted transmission providers and short-term storage providers from liability, unless they would initiate, select or modify the information. Long-term storage providers were not liable when they did not have actual knowledge of illegal information, and upon obtaining such knowledge, would act expeditiously to remove or disable access to such information\textsuperscript{21}.

**Spain** – Spain had not adopted any specific legislation regarding the liability of online service providers and did not have any relevant case law in this area either, which created considerable legal uncertainty for online service providers\textsuperscript{22}. With respect to copyright, both the Spanish copyright law\textsuperscript{23} and the general

\textsuperscript{16} President of Court of 's Gravenhage 12 March 1996, *Informatierecht/AMI*, 1996/5, p. 96-97  
\textsuperscript{17} Court of 's Gravenhage 9 June 1999, *Computerrecht*, 1999, Vol. 4, p. 200  
\textsuperscript{19} *Godfrey v. Demon Internet* [1999] 4 All ER 342  
\textsuperscript{20} However, this new Act could not stop Felix Somm from being convicted. In 1998, the *Amtsgericht* of Munich convicted Mr. Somm for facilitating access to violent and child pornographic content stored in newsgroups hosted by CompuServe Inc (AG Munich 12 May 1998, *Computer und Recht* 1998, p. 500). The court ruled that CompuServe Germany, a subsidiary of CompuServe US, could not invoke the Act, because access to the Internet was provided by the parent company, and not by CompuServe Germany. The court therefore considered CompuServe as a hosting service provider, and found that CompuServe had not done all the technically feasible to block access to the newsgroups concerned. The decision was later reversed by the *Landgericht* of Munich (LG Munich 17 November 1999, *Computer und Recht* 2000, p. 118)  
\textsuperscript{23} Royal Legislative Decree No. 1/1996 of 12 April approving the Revised Text of the Intellectual Property Law
tort liability rule\textsuperscript{24} apply a with-fault liability standard. In addition, criminal law could impose civil liability for crimes committed by other persons. A majority of legal commentators considered article 120 of the Spanish Penal Code\textsuperscript{25} to introduce a strict liability, applicable to online intermediaries to the extent they could be regarded as "owners of any other method of communication"\textsuperscript{26}. Regarding defamation, the general tort liability rule would (hypothetically) also have applied, as well as the Spanish Press Act\textsuperscript{27}, which both maintain a fault-based liability standard. It remained unclear, however, whether an online service provider would have fallen into one of the categories set out in the Press Act (such as authors, publishers and editors).

**Sweden** – Sweden only regulated the liability of electronic bulletin board operators. The 1998 Act on Responsibility for Electronic Bulletin Boards required operators to monitor the bulletin board, supervise the activities of subscribers and remove any infringing material.

### 2.3. Reasons to adopt EU-level measures

The case law and legal doctrine referred to above illustrate the varying, often burdensome obligations and responsibilities imposed on online service providers in the EU, which entailed the risk that the further development of the Internet would be impeded\textsuperscript{28}. Several Member States acknowledged this issue and reacted by adopting specific legislation. However, even such legislation failed to provide the online intermediaries with the necessary certainty\textsuperscript{29}. Moreover, the divergences in national legislation, the divergences in case law between Member States – and even the divergence of case law within one single Member State – created additional legal uncertainty for online service providers in the EU, which faced almost as many legal regimes as there were Member States\textsuperscript{30}.

The European Commission recognised these problems in its proposal for the Directive on electronic commerce: "There is considerable legal uncertainty within Member States regarding the application of their existing liability regimes to providers of Information Society Services when they act as "intermediaries", i.e. when they transmit or host third party information (information provided by the users of the service). These activities have been the subject of the different Member States’ initiatives adopted or currently being examined on the issue of liability"\textsuperscript{31}.

The Commission further referred to the "divergent principles" adopted by those Member States which have introduced new legislation. Despite the limited availability of case law in Europe regarding this issue, the Commission also found the "divergences in rulings and reasoning by the courts" to be an

\textsuperscript{24} Article 1903 of the Civil Code

\textsuperscript{25} "(…) actors will incur civil liability regardless of their criminal liability, where they are (…) owners of any other method of communication of written, spoken or visual material for criminal offences carried out through such methods (…)"

\textsuperscript{26} R. JULIA-BARCELO, l.c.

\textsuperscript{27} Article 65(2) of Act 14/1996 of 18 March regarding Press and Print.

\textsuperscript{28} J. HUGHES, l.c., p. 382

\textsuperscript{29} See the Somm case in Germany and the Godfrey v. Demon case in the United Kingdom


\textsuperscript{31} Commission Proposal, p. 12
obstacle for the internal market\textsuperscript{32}. The national approach was obviously found to be ineffective in trying to provide favourable conditions for Internet transactions and publications\textsuperscript{33}.

The E-Commerce Directive finally introduced a European regime, and intended to equalise service providers’ obligations in all Member States. As further discussed below, these intentions have not been fully realised, so that the mosaic of case law and national regulations has again returned to the EU information society scene — particularly for services that do not neatly fit within one of the three categories predefined by the eCommerce Directive.

3. Liability under the eCommerce Directive

This section 3 provides an overview of the scope and features of the "special liability regime" introduced by the eCommerce Directive. The different issues linked to this special liability regime are not discussed in this section 3, but are instead discussed in section 4 below.

3.1. Introduction to the special liability regime

The eCommerce Directive introduced a set of special liability rules, which are set forth in Section 4 of the eCommerce Directive (articles 12 to 15). It provides for a "safe haven" regime, under which three types of service providers are exempt from liability under certain conditions. This safe haven was considered indispensable to ensuring both the provision of basic services and the provision of a framework which allows the Internet and e-commerce to develop\textsuperscript{34}.

The special liability regime can be briefly described as follows:

- "Mere conduit" service providers (article 12) deliver either network access services or network transmission services. The typical service providers targeted by article 12, are traditional internet access providers (which connect their subscribers to the Internet using dial-up modems, xDSL modems, cable connections or fixed lines) and backbone operators (which interconnect various subparts of the Internet). Both types of service providers transmit large amounts of data at the request of their subscribers.

This liability exemption only applies when the service provider is passively involved in the transmission of data. When the transmission would be initiated, selected or modified by the service provider, or when the receiver of the data would be selected by the service provider, the exemption does not apply.

- "Caching" providers (article 13) temporarily and automatically store data in order to make the onward transmission of this information more efficient. The typical service envisaged by article 13 is a so-called "proxy server", which stores local copies of websites accessed by a customer. When the same website is subsequently accessed again, the proxy server can deliver the locally stored copy of the website, which avoids that the original web server needs to be contacted again, hence reducing network traffic and speeding up the delivery process.

\textsuperscript{32} Ibid.

\textsuperscript{33} L. EDWARDS, "Defamation and the Internet", in L. EDWARDS and C. WAELEDE (eds.), Law & the Internet, a framework for electronic commerce, Oxford, 2000, p. 268

As information is locally stored by the caching provider during a certain period of time — which, depending on the configuration of the servers and websites involved, can be up to several months — various conditions need to be met by the caching provider in order to benefit from the liability exemption. The most important conditions impose that the local copy must be identical to the original information, and that the service provider must comply with the access conditions associated with the locally stored information. Furthermore, the service provider must update the copy in the manner specified by the original website, and must remove (or block access to) the local copies when it obtains actual knowledge of the fact that the original data is removed, or access to the original data is blocked.

Hosting providers (article 14) store data provided by their users. The data being stored is specifically selected and uploaded by a user of the service, and is intended to be stored (“hosted”) for an unlimited amount of time. The typical service envisaged by article 14, is a webhosting company, which provides webspace to its customers, on which they can upload content to be published on a website.

Hosting providers can only benefit from the liability exemption when they are "not aware of facts or circumstances from which the illegal activity or information is apparent" (when it concerns civil claims for damages) or they "do not have actual knowledge of illegal activity or information" (when it concerns other claims). Article 14 thus differentiates the level of knowledge, depending on the type of claim asserted against the service provider. Furthermore, service providers must expeditiously remove, or block access to, such information once they are aware of their unlawful nature.

3.2. Characteristics of the special liability regime

Passive, intermediary role – The eCommerce Directive requires the service providers to act as intermediaries and to maintain a passive role in order to benefit from the liability exemption. However, the level of passiveness differs among the three types of service providers.

Mere conduit service providers transport enormous amounts of data for recipients they even may not know, and are therefore envisaged as having a strictly passive role. If they want to benefit from the special liability regime, they are not allowed to take any initiative with respect to the transmission or interfere in any way in the data or the recipient selection process.

Compared to mere conduit service providers, caching providers can be more actively involved towards their users, as they are allowed to select the data or the recipient of the service (although they are not allowed to modify the local copy of the data stored by them). In fact, the ability to select the data or the receiver, is a key feature of a caching provider, which may want to restrict the access to its services, or which may want to filter the information made available to its users.

The required level of passiveness is the lowest for hosting providers, which are allowed to select and modify the data they store, as well as to select the recipient of the data. If, however, the user of their

---

35 For example, when the service provider stores a local copy of website content protected by a password, other non-authorised customer should not be allowed to access this local copy.

36 For example, a web server may specify the maximum period during which copies can be stored on a proxy server. After this period of time, the original web server should be contacted again by the proxy server in order to obtain a new copy of the data concerned.

37 For example, proxy servers are frequently installed by employers to facilitate blocking of certain websites (e.g., sports websites or websites with adult content).
services would be acting under the authority or control of the hosting provider, the liability exemption will no longer apply.

**Horizontal effect** – The special liability regime installs a horizontal liability regime for the three types of service providers covered by it. Provided they meet the criteria laid down in Section 4, the service providers will be exempted from contractual liability, administrative liability, tortuous / extra-contractual liability, penal liability, civil liability or any other type of liability, for all types of activities initiated by third parties, including copyright and trademark infringements, defamation, misleading advertising, unfair commercial practices, unfair competition, publications of illegal content, etc.\(^{38}\)

It is important to note, however, that the special liability regime only protects the service providers from liability claims. Article 12.3, 13.2 and 14.3 explicitly state that courts and administrative authorities can still request the service providers to terminate or prevent infringements. Consequently, a service provider can be requested to take measures to terminate or prevent an infringement, even when the service provider cannot be held liable for this infringement.

**No general obligation to monitor** – Section 4 (article 15) of the eCommerce Directive sets forth the principle that the three types of service providers have no obligation to monitor the data they transmit or store, nor a general obligation actively to seek facts or circumstances that would indicate illegal activity.

However, despite this prohibition for Member States to impose general monitoring obligations, courts and administrative authorities can still request the service providers to terminate or prevent infringements, for example through injunctions.\(^{39}\) According to recital 47 of the eCommerce Directive, such monitoring obligations must be limited to specific, clearly defined individual cases.

**Application at the service level** – The special liability regime applies to the services provided by a person, and not to the person itself. When a party would supply several types of services, this party may simultaneously qualify for articles 12, 13 and 14.\(^{40}\)

For example, when an internet access provider connects its customers to the Internet through a proxy server, and also offers web space for a personal homepage, this provider will qualify as a mere conduit service provider (for the internet access provided), a caching provider (for operating a proxy server) and a hosting provider (for the web space offered). However, the liability exemptions will not apply to any additional services offered by this provider, such as a news portal, a localised search engine or a domain registration service.

**Additional protection** – While the special liability regime constitutes an additional shield for service providers, it does not modify each Member States’ underlying material law governing liability. The only effect of not (or no longer) meeting the criteria of article 12, 13 or 14 (e.g., because data is modified during transmission, or when access to hosted data is not blocked upon awareness of the unlawfulness), will be the loss of the additional protection. Service providers will then become subject to the general rules of tortuous or penal liability, which may or may not hold the service provider liable, depending on each Member State’s laws.\(^{41}\)

---


**Specific rules for the online world** – Together with the other provisions in the eCommerce Directive, the special liability regime creates specific rules for online services. Accordingly, service providers become subject to different rules, depending on whether they provide their services online or offline. This preferential regime was deliberately envisaged by the European Commission to allow the online service market to develop.\(^{42}\)

4. **Issues linked to the special liability regime**

The special liability regime introduced by the eCommerce Directive has contributed to the further development of online services, particularly in the initial years following the introduction of the Directive.\(^{43}\) Even so, various problems have emerged over time, which have become more pronounced with the advent of new technologies and "Web 2.0" online services. These problems are discussed in detail in this section 4, and can be summarised as a lack of clarity, implementation differences between Member States, gaps in the scope, and the threat of injunctions.

4.1. **Ambiguities in the definition of "information society services"**

The special liability regime applies to information society services, which are defined as services that are "normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services", whereby the service "is sent initially and received at its destination by means of electronic equipment for the processing [...] and storage of data".\(^{45}\) Well-known examples of information society services include web shops, on-line information access tools and search engines.\(^{46}\)

The key elements of this definition are "normally provided for remuneration" and "by electronic means". The question arises how both elements must be interpreted. While this may seem obvious, there are many ambiguities when these concepts are studied in detail.

Please note that, while the ambiguities described in this section 4.1 are applied to the special liability regime for online intermediaries, the impact of these ambiguities is much larger, as it affects the entire scope of the eCommerce Directive. Accordingly, online service providers that do not meet the "normally provided for remuneration" and "by electronic means" criteria, will also be exempted from the transparency obligations of the Directive and rights of free establishment.

4.1.1. **"Normally provided for remuneration"**

"Information society services" are a subcategory of the general concept of "services", as defined in article 50 of the EC Treaty. Accordingly, any activity which would not fall within the scope of article 50 of the EC Treaty, will a priori not qualify as an information society service.

---

\(^{42}\) First Report on the application of the E-commerce Directive (21 November 2003), p. 14: "The limitations on the liability of intermediaries in the Directive were considered indispensable to ensuring both the provision of basic services which safeguard the continued free flow of information in the network and the provision of a framework which allows the Internet and e-commerce to develop."

\(^{43}\) In its First Report on the application of the E-commerce Directive, the Commission stated that "the feedback received so far from the Member States and interested parties has, in general, been positive", although "there is still very little practical experience on the application of articles 12-14".


\(^{45}\) Definition set forth in article 1(2) of Directive 98/34/EC (as amended by Directive 98/48/EC), as referred to by article 2.a eCommerce Directive.

\(^{46}\) Examples taken from recital 18 of the eCommerce Directive
Recital 19 of Directive 98/48/EC, which introduced the concept of "information society services", explicitly refers to article 50 of the EC Treaty, as well as the corresponding case law of the Court of Justice, when giving background information regarding "normally provided for remuneration" 47 48.

Although the existing case law 49 regarding the general concept of "services" upholds a relatively wide interpretation 50 – as it argues that any consideration for an economic activity can constitute "remuneration" – it is not unlikely that new case law would consider that some online activities are not included in the scope. Difficulties may therefore arise when applying the case law of article 50 EC Treaty – which targets issues dealing with freedom of movement for goods, capitals and persons – to emerging commercial models online, because this case law is focused on the question to which extent activities of a State fall within the scope of article 50. It may therefore be complicated to apply this case law to the typical online activities offered by online service providers.

**Explicitly excluded** – According to the case law of the Court of Justice regarding article 50 EC Treaty, some activities are explicitly considered as not "normally being provided for remuneration" (such as public education and governmental services 51). Accordingly, taking into account that the core education activities offered by public schools and public universities are out of scope, it could be argued that elements that are part of this activity (such as providing internet access to classrooms) are excluded from the scope of the eCommerce Directive. It can be questioned whether this exemption is (still) justified 52, particularly when considering how the Internet is becoming an essential tool for education 53.

**Indirectly paid activities** – The Court of Justice has clarified that an activity that is remunerated by a third party, can also qualify as a service "normally provided for remuneration" in the sense of article 50 of the EC Treaty, as this article does not focus on the specific nature of the remuneration, and does not require that the user him/herself pays 54. Consequently, an activity paid for by advertisements was considered to fall within the meaning of article 50.

According to legal doctrine 55, this reasoning can be applied by analogy to online service providers that do not charge fees to their end users, but derive an income from commercial banners presented on their websites. The indirect remuneration established by such advertising revenue is indeed well known, and

---

47 "Whereas, under Article 60 [now 50] of the Treaty as interpreted by the case-law of the Court of Justice, 'services' means those normally provided for remuneration; whereas that characteristic is absent in the case of activities which a State carries out without economic consideration in the context of its duties in particular in the social, cultural, educational and judicial fields; whereas national provisions concerning such activities are not covered by the definition given in Article 60 of the Treaty and therefore do not fall within the scope of this Directive."


49 See, for example, the Humbell case (Case 263/86 Belgian State v Humbel [1988] ECR 5365) and the case of Stephan Max Wirth v Landeshauptstadt Hannover (Case C-109/92, 7 December 1993).

50 For example, private television broadcasting is regarded as a service provided for remuneration because it is paid for through advertising, and hospital services are also provided for remuneration, as hospitals are financed by health insurance companies.

51 As also repeated in recital 19 of Directive 98/48/EC

52 Of course, it should be taken into account that the qualification of an "information society service provider" also entails some drawbacks from the service provider's point of view, as an information society service provider is required to comply with the various obligations set forth in the eCommerce Directive (information to be provided, order placement procedure, ...)

53 Note that the Digital Millennium Copyright Act, which provides a special liability regime for copyright infringements similar to the eCommerce Directive, contains specific wording targeted at nonprofit educational institutions (see section 27 below). Furthermore, public authorities are also protected by the US Communications Decency Act (see section 5.3 below).

54 See Case 352/85, Bond van Adverteerders v the Netherlands [1988] ECR 2085

is frequently used in the offline context (e.g., to sponsor journals), so that application to websites that are sponsored by banners, is immediately evident. Accordingly, the example of a website sponsored by commercial banners is typically cited by legal doctrine that discusses the scope of the eCommerce Directive. 

Although activities sponsored by advertisements are explicitly considered as falling within the scope of article 50 by the case law of the Court of Justice, the question arises to which extent this case law can be applied to other services, for which the link between the service recipient and the remuneration/the remunerating party is far more indirect or remote.

- If, for example, an online activity is provided completely for free by an internet startup company (which, typically, hopes to establish an online presence and then later on find a lucrative business model) and no advertising revenue is generated, can it still be claimed that such service is provided “for remuneration”?

- How should services be qualified that are offered for free by a company, with the sole intention of creating goodwill?

- Consider an amateur developer who offers an open source software package on its website. The website contains no sponsored advertisements and does not attract other types of revenue (such as value added services), so that the developer is not subject to the eCommerce Directive. At a certain point in time, a third party recognises the value of this open source software and offers the developer a job opportunity. Does the website now suddenly become subject to the eCommerce Directive?

It is difficult to predict how a court would react to these cases.

Meaning of "normally" – Another question relates to the term "normally". This word excludes entire categories of online services that are not funded by advertising revenue (such as banners), and are typically provided for free by most service providers — for example, online wiki’s (such as the popular Wikipedia), photo-sharing sites (such as Flickr and Imageshack) and microblogging tools (such as Flickr and Jaiku).

The potential impact of this issue should not be underestimated, as many services on the Internet are offered for free (are not even paid by advertisements). Furthermore, the emerging business model on the Internet is the "freemium" model, whereby more than 95% of the users make free use of a service, and less than 5% of the users pays some kind of remuneration to the service provider (e.g., to get access to restricted features, to get professional support, to get more storage capacity, etc.).

When the "freemium" model and the "entirely free" model become the dominant business models within a certain

56 See, for example, P. VAN EECKE, "Artikelsgewijze bespreking van de wetten elektronische handel", in P. VAN EECKE and J. DUMORTIER, Elektronische handel - commentaar bij de wetten van 11 maart 2003, die keure, 2003, p. 13; M. ANTOINE, o.c., p. 3; M. SCHAUB, European legal aspects of e-commerce, 2004, p. 28; Belgian preparatory documents for the Act of 11 March 2003 (implementing the eCommerce Directive), p. 13-14; etc.

57 E.g., a free wireless hotspot service that would be offered in a certain area by a company, that can be used by anyone, and does not generate remuneration through advertising.

58 It is not entirely clear from the case law of the Court of Justice at which level this the "normally" should be interpreted. Based on the impersonal wording ("service that is normally provided for remuneration") instead of wording such as "a service that is normally provided by the service provider for remuneration") we assume it should be interpreted at a global level, i.e. on the level of the market and not at the level of a specific service provider. Hence, a service will be in scope when most of the service providers in the market provide the service for remuneration in most of the cases. We do not consider it unreasonable, however, to argue that the interpretation should instead occur at the individual service provider level, so that the criterion for a service to be in scope is whether the individual service provider concerned normally provides the service for remuneration. In this report, we will target at the interpretation at the market level, however.

59 See C. ANDERSON, Free - the future of a radical price, 2009
online model, the risk exists that courts would consider that all service providers within this market will fall outside the scope of the eCommerce Directive.

The question also arises which market or category of service providers should be taken into account when assessing "normally". For example, should photo-sharing websites and photo selling websites be considered as being part of the same category? If this is the case, then all of the free photo-sharing websites would be "normally provided for remuneration"; if this is not the case, then even the paid photo-sharing websites would not be considered "normally provided for remuneration", because most of the photo-sharing websites are provided for free.

**Evaluation** – Although no case law exists regarding the application of the criterion "normally provided for remuneration" to online services, there is a risk that some online activities could be deemed to not meet this criterion. Accordingly, such online activities will not be able to take advantage of the freedom of establishment, the freedom of online service delivery and the special liability protection.

Considering the potentially large impact of this potential issue, we therefore advise that, if it would not be resolved by case law, it could be envisaged to decouple the scope of the special liability regime from article 50 of the EC Treaty.

4.1.2. **By electronic means**

The definition of "information society services" requires a service to be provided by electronic means, i.e. on top of existing network infrastructure and telecom-related services. Conversely, telecom-services and network infrastructure deal with low-level, physical signal transmission, and are defined as "electronic communications services" in Directive 2002/21/EC.

According to the definition of electronic communications services, information society services and electronic communications services need to be clearly distinguished, because "[an electronic communications service] does not include information society services, as defined in article 1 of Directive 98/34/EC, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks." The definition of "information society services" itself also implies that information society services cannot consist of signal conveyance, as an information society service "is entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means". In other words: an information society service itself is being transmitted, conveyed and received by some physical means.

As these definitions make it very clear that information society services cannot consist of low-level signal transmission, the question arises whether it is actually correct to assume that traditional internet access provision falls within the scope of article 12 of the eCommerce Directive, considering that the very essence of internet access provision consists of physical signal transmission. This issue is not widely

---

60 It could also be a solution to decouple the scope of "information society services" from article 50 of the EC Treaty, as this would resolve this potential issue for the entire eCommerce Directive (instead of online the special liability regime). However, such would require a change of the EC Treaty.


62 Article 2.c of Directive 2002/21/EC: “electronic communications service’ means a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting (...)

63 Ibid. (underlining added)
discussed and most legal doctrine qualifies typical internet access providers as "mere conduit" providers – although it seems to be recognized in Germany, France and Poland.

4.2. Ambiguities in articles 12 (mere conduit)

Communications network – Taking into account the aforementioned discussion regarding the definition of information society service and the lack of a definition of a "communications network", one could argue that operators of chat networks, instant messaging networks or even peer-to-peer networks, are to be considered as mere conduit providers, as they "provide access to a communications network". This may not be in line with the original intentions of the European legislator.

Select or modify information – In light of the growing amount of online threats (malware, server attacks, botnets, etc.), Internet access providers are increasingly inclined – or even legally required – to take measures to filter the internet traffic received by their customers. Furthermore, new revenue models are emerging, where internet access providers insert banners in webpages visited by users, in exchange for free internet access. Also, Voice-over-IP operators may want to periodically introduce spoken publicity during conversations, in exchange for a free service. As another example, operators of chat networks (to the extent they qualify as mere conduit service providers) may want to automatically block profanity wording and/or sexually oriented conversations.

Although recital 43 of the eCommerce Directive clarifies that "manipulations of a technical nature which take place in the course of the transmission" should be allowed "as they do not alter the integrity of the information contained in the transmission", it is not clear whether traffic filtering, insertion of advertisements and textual filtering of chat conversations can be considered as such "manipulations of a technical nature". Hence, it is not clear whether these parties can still benefit from the liability exemption introduced by article 12.

4.3. Ambiguities in article 13 (caching)

Article 13 lists the conditions under which a caching service is exempted from liability. This article illustrates the technology-dependent drafting of the eCommerce Directive, as it was clearly conceived to protect traditional "proxy-servers". Although article 13 clearly targeted one specific technology (proxy-servers), the conditions set forth in article 13 can also be applied to other technologies, although such may not be in line with the original intentions of the European legislator.

---

64 See, however, J. HARRINGTON, "Information society services: what are they and how relevant is the definition?", Computer Law & Security Report, Vol. 17, no. 3, 2001, p. 179. In this article, it is suggested that the provision at individual request may also not be fulfilled for access providers.

65 See, however, I. WALDEN, "Discussion of Directive 2000/31/EC", in Concise European IT law, 2006, Kluwer law international, p. 248-249 (arguing that mere conduit access providers are subject to both article 12 and the telecommunication directives)

66 Study on the liability of Internet intermediaries, p. 32. [Drafting note: the study on the liability of Internet intermediaries refers to country reports of Germany, France and Poland, which are not available to us. This issue therefore needs to be further investigated, once the country reports are available.]

67 Article 13 describes caching as "the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information’s onward transmission to other recipients of the service upon their request".

68 This is particularly illustrated by conditions (c) and (d) of article 13, which require the provider to comply with updating rules and hit counting rules "widely recognised and used by industry". These conditions only seem for proxy servers.
For example, the question has arisen whether "Usenet" newsgroups can be considered to be a form of caching. Usenet is a system in which users post messages to a newsgroup, which are then automatically broadcasted to, and mirrored on, other servers using a wide variety of networks. Each server then retains the messages in each newsgroup for a limited amount of time. Although it is questionable whether this automatic redistribution of newsgroup messages is really performed "for the sole purpose of making more efficient the information's onward transmission", the German Regional Court of Munich qualified the Usenet service as a caching provider. Meanwhile, other courts qualified the Usenet service as a hosting service.

Similarly, various decentralised content distribution systems could also be qualified as caching providers, although only limited case law has emerged on this topic. For example, the Domain Name System (DNS) uses a hierarchy of servers to distribute information across the globe regarding the mapping of each internet domain name to specific IP-addresses. Such system meets all the criteria set forth in article 13, although it is questionable whether such qualification would be in line with the spirit of article 13, which clearly targets proxy-servers. However, taking into account the increasing amount of domain name disputes, it is not unlikely that a court will face this question, when a plaintiff would request a top-level DNS-provider to block access to a specific domain name.

It would be even more controversial to qualify each peer-to-peer user as a caching provider, although such could be in line with the letter of the eCommerce Directive.

4.4. Ambiguities in article 14 (hosting)

Out of all articles in Section 4 of the eCommerce Directive, article 14 has clearly spawned the greatest amount of discussion and case law.

This ambiguity was plainly recognised by the French artistic commission, who issued a report dedicated to this subject. Analysing the French and European legislation, it stated that "the Commission cannot conclude how participatory Web 2.0 websites should be qualified (...) so that one arrives at the boundaries of the concept of hosting provider". Accordingly, the Commission notes that the case law is dispersed on this subject.

70 LG Düsseldorf, 23 May 2007, 12 O 151/07, MMR 2007, 534 (535); Queen's Bench Division, 10 March 2006, Bunt v. Tilley, as mentioned in T. VERBIEST, G. SPINDLER, G.M. RICCIO, A. VAN DER PERRE, Study on liability of Internet intermediaries, ordered by the European Commission, November 2007 (hereafter "Study on the liability of Internet intermediaries"), p. 34
71 For example, according to German Courts the liability exemptions do not apply to domain name registries, as these exemptions only refer to the provision of content: see the (rather old) cases mentioned by the Study on liability of Internet intermediaries, p. 105
72 leaving aside the question of whether participation in peer-to-peer networks meets the ambiguous "normally provided for remuneration" criterion described above in section 4.1.1
73 For example, the popular Bittorrent protocol distributes information in a decentralised manner, whereby each user simultaneously downloads and uploads information from and to other users. This protocol is clearly intended to "make more efficient the information's onward transmission to other recipients of the services". Furthermore, users do not modify the information that is being exchanged (condition a), there are generally no access conditions or updating conditions that apply (conditions b and c), there are no widely recognised technologies used by industry to obtain data on the use of the information (condition d) and it occurs only rarely that "the information at the initial source of the transmission has been removed from the network, or access to it has been disabled" (condition e). Each Bittorrent user may therefore qualify as a caching provider, although it should be recognised that this would require a rather literal interpretation of conditions (b) and (e) of article 13
"Consists of" – According to article 14, a hosting service "consists of the storage of information provided by a recipient of the service". This "consists of" criterion is used to distinguish mere hosting providers (who are not involved in the creation of the content) from content providers (who are themselves involved in creating the content, and do not benefit from the special liability regime). Although this criterion may be very suitable for the traditional services for which it was conceived\(^75\), its weaknesses become apparent when applied to other services\(^76\), and particularly cloud computing services and other Web 2.0 services where storage is just one aspect of the entire service package.

The criterion's weakness essentially boils down to its failure to specify to which extent a service should relate to hosting: is it sufficient that some aspects of the service deal with hosting, should the majority of aspects deal with hosting, or should all aspects of the service deal with hosting? Due to the margin of appreciation left by the "consists of" criterion, courts have adopted various interpretations:

- The Court of Paris\(^77\) ruled in June 2008 that "the essence of eBay's service is to mediate between buyers and sellers", so that eBay cannot benefit from article 14, as "it deploys a commercial, auction-related activity that is not limited to hosting". Such interpretation excludes article 14 when the hosting-related aspects of a service are not the most important aspects of the service.

- Several courts seem inclined to qualify a web service as a publishing activity when the service provider offers editing tools, or forces its users to adopt a certain structure in the content. For example, in the famous Lafesse v. MySpace case\(^78\), the Court of Paris ruled in 2007 that, although social website MySpace indeed hosts information provided by its users "[MySpace] does not limit itself to this function; indeed, by clearly offering a presentation structure via frames to its users, and by displaying banners during each visit from which it clearly draws profits, [MySpace] is an editor, and must take on the responsibilities of an editor"\(^79\). Meanwhile, the Court of Paris did recognise video platform YouTube as a hosting provider in 2009\(^80\), stating that the presentation structure and search facilities offered by YouTube did not influence its qualification as hosting provider.

- Instead of focusing on the editing tools / content structure, some German and Italian case law and doctrine focus on the question of whether the service provider has "adopted" the third party content, or has instead (seriously) distanced itself from this content. This doctrine refuses to qualify online service providers as hosting providers when the third party content appears to be the provider's own content\(^81\). This criterion is also adopted by Advocate-General Poiares Maduro in the pending Google Adwords case\(^82\). The Advocate General argues that the Google Adwords service (which displays

---

\(^75\) i.e., hosting web space to publish a website

\(^76\) For example, e-mail services (temporary storage of e-mails) and newsgroup access (temporary storage of newsgroup "posts")

\(^77\) Three separate cases of the same date, all issued by the Commercial Court of Paris, First Chamber, on 30 June 2008 (Louis Vuitton Malletier / Christian Dior Couture and Parfums Christian Dior, Kenzo, Givenchy et Guerlain v. eBay)


\(^79\) Still, in another famous case regarding a video sharing website less than one month later, the Court of Paris ruled that "[DailyMotion] cannot be qualified as an editor, as the content is furnished by the users of the service", even though the editing facilities and banners offered by DailyMotion and MySpace are very similar from a functional point of view. (T.G.I. Paris, 13 July 2007, Nord-Ouest Production c. s.a. Dailymotion)

\(^80\) Bayard Presse / YouTube LLC, TGI de Paris 3ème chambre, 2ème section, 10 July 2009, available at www.legalis.net/jurisprudence-decision.php3?id_article=2693

\(^81\) P. BALBONI, p. 65-66

\(^82\) Joined Cases C-236/08, C-237/08 and C-238/08 of Google France Inc. v. Louis Vuitton Malletier e.a.
advertisements next to search results) is not protected by the special liability regime, because – although it stores certain information – the service is not neutral as regards the information it carries, because the display of ads stems from Google’s relationship with its advertisers. Consequently, Google can be held liable for trademark infringements occurring through its Adwords service.

- Still other courts **subdivide** a single commercial service into several distinct activities, and only apply the special liability regime to some activities. For example, in France, the court of Troyes\textsuperscript{83} considered in June 2008 that, although online auction provider eBay indeed provides hosting activities by storing photos and texts associated with items put up for sale, it also provides various other auction-related activities (rating systems, payment facilities, advertisement tools, etc.), to which article 14 does not apply\textsuperscript{84}. The Tribunal de Grande Instance came to a similar decision in May 2009\textsuperscript{85}.

- UK courts tend to differentiate between service providers that only **facilitate** infringements by a third party, and service providers that **authorise** infringements by a third party\textsuperscript{86}.

- Some courts do not seem to use a specific criterion, and qualify a service as a hosting service as soon as there is **some storage activity** involved\textsuperscript{87}.

"**Under the control**" – Article 14.2 holds that the liability exemption does not apply when the recipient of the service is acting "**under the authority or the control of the provider**". It is indeed obvious that an employer who hosts illegal information created by an employee at the employer’s request, should not benefit from the liability exemption.

Less obvious, however, is to which extent hosting providers can monitor and manipulate the information stored on their website. Community encyclopaedia Wikipedia, for example, is permanently monitored by a team of content managers, to ensure that the information being published is accurate, verifiable, built on solid sources, and excludes personal opinions. As these content managers have the possibility to modify and delete articles uploaded by other users, there is clearly a level of control being exercised. The same is true for many social community websites and blogs.

Another example is discussion forums, where there is already case law that exempts service providers from the special liability protection when the messages are moderated or compiled by a forum administrator\textsuperscript{88}.

**Illegal information** – Since the actual knowledge requirement only concerns knowledge of **illegal** activity, providers will need to make an assessment of what does and what does not constitute illegal information, in order to make a decision to block access to certain content. This has led to complaints of

\textsuperscript{83} T.G.I. Troyes 4 June 2008, Hermès International v. eBay. The case concerned a counterfeited bag being put up for sale by one of eBay’s customers.

\textsuperscript{84} Identical analysis performed by the Brussels Court of Commerce, decision of July 31, 2008 (A/07/06032), although this court did not conclude that eBay was to be held liable. See E. MONTERO, 33/2008). Contrary to the French Courts, the Brussels Court did apply the liability protection to the hosting-related activities of eBay.

\textsuperscript{85} Tribunal de grande instance de Paris, 3ème chambre, 13 May 2009, L’Oréal et autres / eBay France et autres

\textsuperscript{86} Bunt v. Tilley, [2006] EWHC 407 (QB) at 22, as mentioned by P. BALBONI et al, o.c., p. 67

\textsuperscript{87} For operators of blogging websites, see the Greek case No 44/2008 of Rodopi Court of First Instance (website blogsport.com), published in Armenopoulos 2009/3, p. 406. According to this decision, the company that hosts the blog cannot be considered as the owner, the publisher, the director of editing and/or the editor of the blog posts themselves. The blog operator only provides space for the blogs, and does not initiate the transmission of information, does not choose the receiver of the transmission, does not choose or alter the transmitted information.

\textsuperscript{88} Court of Amsterdam, 12 March 2009, regarding messages available at www.internetoplichting.nl
stakeholders\(^89\), who feel incapable of taking up such responsibilities. The issue is aggravated by the fact that the answer to the question as to when content can be deemed manifestly unlawful is answered differently in various Member States. While the illegal nature of some types of information will be obvious to any person (e.g., pirated copies of commercial software or recent Hollywood movies), the legal assessment becomes more difficult for cases of defamation or texts that may be in the public domain. Notice-and-takedown letters may therefore induce service providers to take down material without reason, if they do not want to have the material examined by a legally trained person\(^90\).

For example, in Germany, trademark infringements were judged to be a obvious infringement, while an Austrian court found that such infringements could not be qualified as obvious\(^91\). In France, a judge found that the sale of copyrighted videogames under the counter price constituted a manifest infringement. On the subject of defamation, a Dutch court found that such content was not unmistakably unlawful, while an Austrian court ruled that insulting statements could be qualified as obvious, since anyone is capable of determining the defaming character of such statements\(^92\).

**Required level of knowledge or awareness** – Caching providers and hosting providers can only benefit from the limited liability regime when they expeditiously remove or disable access to illegal information as soon as they either "have actual knowledge" or "are aware of facts or circumstances" regarding this illegal information. While these concepts are crucial to adequately determine the liability of caching and hosting providers, the eCommerce Directive does not define what should be considered as "actual knowledge" or "awareness". Consequently, it is left to the courts to determine which level of knowledge or awareness is required.

This issue was discussed in a number of German court decisions\(^93\). It was decided that the term actual knowledge implies actual human knowledge, as opposed to computer knowledge. Negligence and conditional intent were not considered to constitute actual knowledge. In addition, German courts found that knowledge of specific illegal content is required, as opposed to a general awareness of the past presence of illegal material on a server\(^94\). Under German law, providers can only enjoy liability in the absence of facts or circumstances from which illegal activity or information would be apparent, a condition which is interpreted in German jurisprudence as the absence of gross negligence. A similar condition exists under Dutch law, where providers can not be held liable if they could not reasonable be expected to know of the illegal nature of an activity\(^95\).

---

\(^89\) See, for example, E. MONTERO, "La responsabilité des prestataires intermédiaires sur les réseaux", in Le commerce électronique européen sur les rails?, Bruylant, Brussels, 2001, p. 290-291

\(^90\) In a test conducted in the Netherlands, where takedown letters regarding material that was clearly in the public domain, 7 out of 10 ISPs took down the allegedly infringing material (see http://www.bof.nl/docs/researchpaperSANE.pdf). See also section 5.2.3 (particularly footnote 174) below for a comparison with the United States, where this issue is even more relevant, as US hosting providers cannot be held liable by their users for taking down content by mistake.

\(^91\) Study on liability of Internet intermediaries, p. 38

\(^92\) www.internet4jurists.at/entscheidungen/olgi_114_05i.htm

\(^93\) Study on liability of Internet intermediaries, p. 36

\(^94\) BGH, 23/09/2003, VI ZR 335/02, NJW 2003, 3764

\(^95\) Study on liability of Internet intermediaries, p. 37
4.5. **No harmonised notice-and-takedown procedure**

Although the majority of Member States have followed an almost verbatim transposition of articles 12, 13 and 14 of the eCommerce Directive\(^\text{96}\), some examples can be found of diverging statutory implementations of article 14 and (to a limited extent) article 13. These implementation divergences concern, particularly\(^\text{97}\), the notification procedure for hosting providers \(^\text{98}\).

Caching providers and hosting providers can only benefit from the limited liability regime when they expeditiously remove or disable access to illegal information as soon as they either "have actual knowledge"\(^\text{99}\) or "are aware of facts or circumstances"\(^\text{100}\) regarding this illegal information. Despite the importance of these concepts, the eCommerce Directive does not define them, nor does it establish a procedure to establish the "actual knowledge" or "awareness", or define what should be considered "expeditiously". The eCommerce Directive does, however, allow Member States to "[establish] specific requirements which must be fulfilled expeditiously prior to the removal or disabling of information"\(^\text{101}\).

As a result, Member States have developed different practices for verifying the presence of the required level of knowledge, and right holders submit notices in a variety of forms\(^\text{102}\):

- Most Member States have not established formal notification procedures, although various criteria may have been developed in case law or legal doctrine.
  
  In the Netherlands, for example, the parliamentary preparatory works state explicitly that a "simple" message is not sufficient, whereas a court order will always be sufficient. In a Germany, case law considers that a notice that lacks detail as regards the claimed copyright, is not sufficient.

- Other Member States have not established a formal procedure in their laws, but have nevertheless certain statutory criteria that must be met by the notification.
  
  For example, a hosting provider is not required to remove or block access under Portuguese law "only because of the fact that a third party is arguing an infringement", which restricts private notifications. The United Kingdom, on the other hand, requires courts to take into account all circumstances, in particular whether the notice was received through a specified means of contact, whether the notice included the contact details of the sender, and whether the location and unlawful nature of the information was described.

- Some Member States have established a formal notification procedure (commonly referred to as a "notice-and-takedown procedure").

\(^\text{96}\) Study on the liability of Internet intermediaries, p. 32, 33 and 34

\(^\text{97}\) See Study on the liability of Internet intermediaries for other examples of divergences. In summary, for almost every aspect of article 14, there is at least one Member State that uses a different wording or a different approach. For example: the Netherlands, Portugal, Germany and the Czech Republic have slightly varied the words used in article 14 (p. 34); the Czech Republic, Hungary, Latvia, Malta, Poland, Slovak Republic and Spain do not distinguish between actual knowledge (for criminal liability claims) and awareness of facts / circumstances (for civil liability claims); Lithuania, Poland, Finland, the Slovak Republic and Sweden vary with respect to the requirement to remove or disable access to unlawful information; etc. Implementation differences for article 12 and article 13 are less pronounced between Member States.

\(^\text{98}\) Although Member States also differ significantly regarding their interpretation of "illegal information", "actual knowledge" and "awareness", these differences result from court decisions, and are therefore discussed below in section 4.4 above

\(^\text{99}\) Requirement for caching providers (regardless of the type of claim) and hosting providers (for claims other than claims for damages)

\(^\text{100}\) Requirement for hosting providers that are confronted with claims for damages. Hence, the threshold for incurring liability as a hosting provider due to claims for damages, is lower than the threshold for incurring liability due to other claims (such as criminal allegations).

\(^\text{101}\) Recital 46

\(^\text{102}\) Study on liability of Internet intermediaries, p. 14 and 41 onwards
Such is the case with Spain, where a “competent body” – such as a court or administrative authority – must order the removal or blocking of information, although this strict procedure does not seem to be followed by all Spanish courts. Similarly, Italian law requires a notice from relevant authorities, although it is not clear whether hosting providers should inform their customers/users about the notification. Finish and Hungarian law have established detailed formal procedures, although they are limited to intellectual property infringements. French and Lithuanian law have opted for optional notification procedures.

**Subsidiarity** – It has been subject to debate whether some kind of subsidiarity principle applies regarding injunctions against providers. Such a principle would entail that right holders have to address the author of illegal content, before directing a claim against the host provider and (possibly after addressing the host provider) the access provider. French courts have used the subsidiarity principle by only ordering injunctions against access providers for cases where hosting providers refrained from acting, a practice later confirmed by the French Court of Appeal. The German Federal Court of Justice, on the other hand, dismissed the principle of subsidiarity in the context of injunctions against host providers.

**Disclosing information** – Online intermediaries have been the target of claims for disclosure of information in a variety of cases, mainly concerning copyright infringement. Such claims have been directed against providers in various Member States with varying success. In Austria, successful claims for information have been made based on national intellectual property law, which explicitly provides for a right for copyright holders to demand information against intermediaries in case of copyright infringement. Similar claims have been known to be granted in the Netherlands and France. In the common law Member States, the "Norwich Pharmacal rule" permits a court to order a third party to disclose documents related to a litigation in its possession. The rule has been applied to online intermediaries in Ireland and the UK, in copyright as well as defamation cases.

However, requests for information are sometimes also dismissed on data protection grounds. Italian, Belgian and German courts refused requests for information on the grounds that data protection regulation did not give providers the right to disclose user information. For example, in an Italian copyright infringement case regarding the use of file-sharing networks, a court dismissing a claim for disclosure of information, based its opinion on arguments of the Data Protection Commissioner, who argued that the disclosure of user data and logs represented an invasion of privacy. Under Irish data protection law, intermediaries are not allowed to share user information with anyone, although the Norwich Pharmacal rule provides an exception, if the claimant can obtain a court order.

---

103 Some case law pre-assumes “effective knowledge” due to the hosting provider’s duty to monitor the content hosted by it (SGAE v. Asociacion de Internautas, case pending before the Supreme Court)
104 Study on liability of Internet intermediaries, p. 50
105 BGH, 27/03/2007, VI ZE 101/09, MMR 2007, 518
106 Study on liability of Internet intermediaries, p. 77
107 Court of The Hague, 05/01/2007, 276747/KG ZA 06-1417, available at www.rechtspraak.nl
108 www.legalis.net/breves-article.php3?id_article=1648
109 Study on liability of Internet intermediaries, p. 79
110 Study on liability of Internet intermediaries, p. 81
111 Tribunale di Roma, Sezione IX civile (IP specialized section), 09/02/2007, Peppermint Jam Records v. Telecom Italia
112 Study on liability of Internet intermediaries, p. 82
4.6. **Possibility of to issue injunctions**

Although the eCommerce Directive protects providers of mere conduit, caching and hosting services against liability, the Directive explicitly mentions that "[t]he limitations of the liability of intermediary service providers established in this Directive do not affect the possibility of injunctions of different kinds; such injunctions can in particular consist of orders by courts or administrative authorities requiring the termination or prevention of any infringement, including the removal of illegal information or the disabling of access to it". Thus, even when an online service provider would not be held liable for storing or transmitting third party content, it can still be ordered to remove third party content and/or prevent the alleged infringements from re-occurring in the future.

The possibility to issue injunctions against service providers should not be underestimated: while liability claims against mere conduit service providers (and caching service providers) are not important in court practice, injunctions are frequently issued against them. Injunctions therefore constitute important tools for plaintiffs.

**Legal basis** – Which types of injunctions can be requested by a plaintiff, depends on the Member State considered. While a few Member States (Austria, France, Italy, Sweden and the United Kingdom) have adopted specific provisions for injunctions against intermediaries, most Member States require plaintiffs to rely upon general procedural rules to request injunctions against online service providers. Such general procedures can have far-reaching effects: according to the German legal doctrine of accessory liability, all parties involved in a wrongdoing activity can become subject to the injunction, without necessarily being wrongdoers or participants.

**Links with other Directives** – In practice, many injunctions against online intermediaries are (directly or indirectly) based on the Enforcement Directive and Copyright Directive, which require Member States to provide for the possibility of injunctions:

*Article 8.3 Copyright Directive: Member States shall ensure that rightholders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right.*

*Art. 11 Enforcement Directive: Member States shall ensure that, where a judicial decision is taken finding an infringement of an intellectual property right, the judicial authorities may issue against the infringer an injunction aimed at prohibiting the continuation of the infringement. Where provided for by national law, non-compliance with an injunction shall, where appropriate, be subject to a recurring penalty payment, with a view to ensuring compliance. Member States shall also ensure that rightholders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe an intellectual property right, without prejudice to Article 8(3) of Directive 2001/29/EC.*

Both Directives clearly state that they leave the eCommerce Directive untouched:

*Consideration 16 of the Copyright Directive: This Directive is without prejudice to provisions relating to liability in [the Ecommerce Directive].*

113 See articles 12.3, 13.2 and 14.3, as well as recital 45
114 Study on liability of internet intermediaries, p. 66-69
115 Study on liability of internet intermediaries, p. 52-66

Although the E-commerce, Copyright and Enforcement Directive do not seem to contradict each other, the question arises how the reconciliation between these three Directives should be accomplished in practice, because injunction (on whatever legal basis) must not lead to general obligations in practice.

**Types of measures** – Courts differ in the range of measures they impose: plaintiffs can ask to block access to certain websites\(^{116}\), block access to file sharing networks, block infringing users\(^{117}\), filter unauthorised copyrighted works from a customer's internet traffic\(^{118}\), filter trademark-infringing auction items, or expose the contact details of the alleged infringers\(^{119}\).

**Diverging case law** – Across Member States, courts react differently to requests for injunctions. While some courts seem openly sympathetic towards the plaintiff\(^{120}\), other courts consider the injunctions to be disproportionate\(^{121}\). Still other courts openly admit that the possibility to issue injunctions and the relationship between the eCommerce Directive and the Enforcement Directive is highly unclear:

> "I conclude that the scope of the obligation placed on Member States by the third sentence of Article 11 [of the Enforcement Directive], and in particular the scope of the injunction which it requires to be available against intermediaries, is unclear. This is another matter upon which the guidance of the ECJ is required."  \(^{122}\)

Also, Member States differ in whether or not they apply the principle of subsidiarity, which requires a plaintiff to first seek relief against the content provider, and only claim an injunction against the service provider as a last resort\(^{123}\).

**Preventing future infringements** – Injunctions can not only impose the termination of an infringement, but also the prevention of future infringements. However, the prevention of future infringements often leads de facto to a general monitoring obligation for the hosting provider, and may therefore conflict with article 15 of the eCommerce Directive, which prohibits Member States to impose general monitoring obligations on service providers that fall within the scope of the special liability regime.

---

\(^{116}\) See, for example the famous Danish "Tele2" case, in which access provider Tele2 was ordered to block access to the Russian webshop allofmp3.com (Court of Copenhagen, 25 October 2006)


\(^{118}\) Either by blocking a specific IP-address, or blocking the DNS-translation from a domain name to an IP-address

\(^{119}\) Study on liability of internet intermediaries, p. 13

\(^{120}\) For example, the Brussels Court of First Instance in the Sabam v. Tiscali/Scarlet cases (26 November 2004 and 29 June 2007), in which the court ordered internet access provider Tiscali/Scarlet to install filtering software to prevent copyright-infringing songs from being downloaded, even though there were various technical, operational and legal concerns associated with such filtering software; the Court of Copenhagen in the Tele2 case (25 October 2006); the Court of The Hague, which ordered internet access provider KPN to cut off customers’ access to the Internet due to copyright infringements (5 January 2007)

\(^{121}\) UK Queen’s Bench Division, 10 March 2006, [2006] EWHC 407 (QB); [2006] 3 All ER 336; [2006] EMLR 523, Bunt v Tilley & Others

\(^{122}\) nr. 465

\(^{123}\) For example, French courts follow this principle, contrary to German courts: see Study on liability of internet intermediaries, p. 49-50
Courts across the EU have different opinions on the required conditions and the extent of injunctions to prevent future infringements. In Germany, the Federal Court of Justice decided that a provider should not only remove unlawful content of which it was informed, but should also take all technically feasible and reasonable precautions to prevent future infringements. This decision was confirmed in 2008. The German Court ruled that it was not sufficient to use a manual screening process consisting of six full time-employees, combined with a hashing system to prevent uploads of banned files.

In Austria, the Supreme Court decided that an obligation to monitor was legitimate, where the provider had obtained notice of at least one infringement so that the danger of further infringements by individual users was substantiated. In France, the Court ruled in the Dailymotion case that a service provider who was aware of the possibility that users upload illegal content, had an obligation to monitor this content before it was published on the website. Similarly, in the Google Video case, the Italian Court obliged the service provider to take measures to prevent that videos that had previously been removed due to their illegal nature, would be uploaded again.

Even more interesting is the Belgian Sabam v. Tiscali/Scarlet case (29 June 2007), in which the judge considered that the possibility to issue injunctions against an intermediary was in no way restricted by the eCommerce Directive, because the prohibition on general monitoring obligations is listed in section 4 of the eCommerce Directive (entitled “Liability of intermediary service providers”), while injunctions only concern the termination of infringements, and do not deal with liability at all.

**Practical example: videos on a social community.** In a currently pending case, a leading European video platform is being sued by a rightholders association. According to the plaintiff, the platform operator is an intermediary, who (based on article 8.3 of the Copyright Directive) must take all steps required to remove copyright-infringing videos from its platform.

The platform operator, on the other hand, argues that the special liability regime does not allow the court to grant this request, as it would boil down to a general monitoring obligation.

While the plaintiff does not hold the platform operator liable for the infringing material, it does ask the court to impose an injunction which – if granted – would immediately render the platform operator bankrupt, due to the sheer volume of videos available on the platform, which must be manually screened to comply with the plaintiff’s request.

**Comparison with the US** – It is interesting to note that, contrary to the eCommerce Directive, the US Digital Millennium Copyright Act – which also introduces a special liability regime for some service providers – explicitly includes the prevention of future infringements as a condition to fall within the scope

---

124 BGH, 11/03/2004, ZE 304/01, MMR 2004, 668

125 RapidShare cases: Oberlandesgericht Hamburg, 2 July 2008; District Court of Düsseldorf, 23 January 2008; Regional Court of Hamburg, 12 June 2009 (available at www.gema.de/fileadmin/inhaltsdateien/presse/pressemitteilungen/GEMA_RapidShare_Urteil_LG_Hamburg_vom_12062009.pdf)


127 Study on liability of Internet intermediaries, p. 752

128 T.G.I. Paris, 13 July 2007, Nord-Ouest Production c. s.a. Dailymotion

129 See footnote 117
of the liability exemptions. Under the Digital Millennium Copyright Act, all types of online service providers must implement a policy to terminate repeating infringements.130

Result: no liability, but similar costs incurred – The uncertainty surrounding the possibility to issue injunctions, also undermines the strength of the liability regime. Even when a service provider would not be held liable for certain infringement committed by its users, the practical consequences of an injunction will often lead to similar results (lawsuits, exposure, legal costs, technical costs, technical measures being imposed, etc.).

Meaning of recital 48 – Recital 48 holds that the eCommerce Directive "does not affect the possibility for Member States of requiring service providers, who host information provided by recipients of their service, to apply duties of care, which can reasonably be expected from them and which are specified by national law, in order to detect and prevent certain types of illegal activities". It is not clear to which extent the reference to "duties of care" can allow Member States to introduce some kind of general obligation for hosting providers to monitor their systems, or may even broaden the ways by which a hosting provider may be deemed to obtain "knowledge" under article 14. Accordingly, it is not clear how recital 48 can be reconciled with articles 14 and 15, and most authors consider it a mere glitch.131

4.7. Gaps in the scope of the special liability regime

Protection of search engines – Despite the importance of search engines for the functioning of the Internet, the eCommerce Directive does not set out a liability regime for these intermediaries, to which it refers as location tool services.132 However, some Member States, such as Portugal and Spain, have provided for limitations to the liability of search engines by extending the special liability regime of the Directive.133 Interestingly, the United States have also adopted a similar special liability regime for search engines.134 While search engines seem to have fared pretty well at the hands of courts in most Member States, their position remains unclear for the time being.135 Moreover, Advocate-General Poiares Maduro recently acknowledged that – contrary to the Google Adwords service – the Google search engine qualifies as a hosting service.136

Although the European Commission has encouraged Member States to further develop legal security for internet intermediaries, some Member States, such as the United Kingdom, have adopted a minimalist

130 See section 5.2.2 below
132 Article 21 Electronic Commerce Directive
133 COM/2003/0702, p 13
134 See section 5.2 below
135 See, for example, the UK case Designtechnica Corporation v. Google, available at www.bailii.org/ew/cases/EWHC/QB/2009/1765.html, in which the court concluded that it was unclear whether the provider of a search engine fell within the scope of articles 12 to 14 of the eCommerce Directive. The court also refers to similar cases where search engines were not held liable: Jensen v Google Netherlands (26 April 2007, court of Amsterdam); SARL Publison System v SARL Google France (Court of Appeal in Paris, 19 March 2009); Palomo v Google Inc (Court of First Instance in Madrid on 13 May 2009)
136 Joined Cases C-236/08, C-237/08 and C-238/08 of Google France/Inc. v. Louis Vuitton Malletier e.a.
137 Ibid.
approach to the adoption of the Directive and offer no additional protection\textsuperscript{138}. The lack of harmonisation in this area seems problematic in view of the important function performed by search engines and their significant impact on the online world.

**Protection for hyperlinking** – Similar to the issue of search engines, the eCommerce Directive does not set out a specific liability regime for hyperlinks, although hyperlinks are at the very core of the functioning of the Internet, and have already triggered substantial case law. Only some countries, such as Austria, Spain and Portugal\textsuperscript{139} (as well as Liechtenstein), have implemented a liability model for hyperlinking, based on article 14 of the Directive. As such, providers of hyperlinks cannot be held liable for changes to linked content of which they are not aware, unless notification has been given\textsuperscript{140}.

4.8. **Result: considerable legal uncertainty**

Due to the various ambiguities in the eCommerce Directive and the diverging national implementations of the eCommerce Directive, the manner in which courts and legal practitioners interpret the special liability regime across the EU, varies widely across EU Member States\textsuperscript{141}. It seems that courts and legal practitioners find it difficult to apply the special liability regime, and seem inclined to find arguments to put aside the special liability regime and instead revert to more general rules of legal doctrine\textsuperscript{142}. This may be linked to the fact that a Member state's approach to the issue of provider's liability is often based upon a general doctrine of contributory liability, which renders the horizontal liability exemptions provided for by the eCommerce Directive difficult to implement\textsuperscript{143}.

As a result, online service providers, users and third parties face considerable legal uncertainty in the European Community, in particular when it concerns services that do not qualify as the "traditional" internet access, caching or web hosting services envisaged by the eCommerce Directive.

While not all of the uncertainties and ambiguities enumerated above have been tested in court\textsuperscript{144}, we assume that it is only a matter of time before national case law is triggered in this regard. Other ambiguities – in particular the definition of hosting services – have already been discussed at length, although no convergence can be found across the Member States. Consequently, stakeholders are once again faced with legal uncertainty, as was the case before the introduction of the eCommerce

---

\textsuperscript{138} See www.out-law.com/page-7670.

\textsuperscript{139} COM/2003/0702, p 13.

\textsuperscript{140} Study on liability of Internet intermediaries, p. 18

\textsuperscript{141} Study on liability of internet intermediaries, p. 30; A. SAINT MARTIN, "Les obligations du fournisseur d'hébergement Web 2.0", Revue Lamy Droit de l'Immatériel, 2008/36, p. 26

\textsuperscript{142} Spanish legal doctrine even reports that in Spain "some judgments simply have completely ignored the existence of a legal provision specifically aimed at excluding intermediary liability. (...) Indeed, the very existence of the exemption is not even mentioned, much less considered." (M. PEGUERA, "I just know that I (actually) know nothing": actual knowledge and other problems in ISP liability case law in Spain", EIPR, 2008, issue nr. 7, p. 281). It can be assumed that similar situations arise in other Member States.

A more recent Dutch example is the case LJN BJ1409, Rechtbank Utrecht, 267630 / KG ZA 09-5161, in which the court ruled that the eCommerce Directive does not protect an online service provider against data protection infringements committed by its users.

\textsuperscript{143} Study on liability of Internet intermediaries, p. 30

\textsuperscript{144} For example, we are not aware of case law regarding the ambiguities surrounding "normally provided for remuneration" (section 4.1.1), "by electronic means" (section 4.1.2) and "select or modify" (section 4.2).
History therefore seems to repeat itself, despite the protective efforts of the eCommerce Directive, for example:

- **Costly involvement** – In 1996, the computer equipment of two French internet access providers was confiscated during a criminal investigation of acts performed by their users. Also in 2008, internet access providers can incur significant costs due to counter actions performed by their users, for example by having to install filters on their networks.

- **Criminal charges** – In 1996, the CEO of an internet access provider was personally convicted for having provided access to illegal third party information. In 2009, natural persons can still face criminal charges. For example, Google executives are personally prosecuted in Italy for an illegal video uploaded by a user.

- **Publisher's liability** – In 1996, French and Dutch national law reverted to a system of publisher's liability to assess defamation cases. Due to the specific nature of the Internet, the publisher's liability doctrine is often difficult to apply to an online context. However, despite the introduction of the eCommerce Directive, the publisher's liability doctrine is still frequently used by Courts.

5. **Liability of online intermediaries in the United States**

This section discusses how the case law and legislation of the United States deal with the topic of online intermediary liability. Online intermediaries are essentially protected through three different channels in the United States: the case law on secondary liability, the Digital Millennium Copyright Act and the Communications Decency Act. Section 6 below will then compare the EU to the United States.

### 5.1. Case law secondary liability for copyright infringements

**Types of secondary liability** – US case law generally recognises two types of secondary liability in the context of copyright infringements: ***contributory infringement*** and ***vicarious liability***. Contributory liability arises when a party with knowledge of another party’s infringing conduct has materially contributed to that conduct, while vicarious liability is incurred when a defendant has enjoyed a financial benefit from the infringing conduct of another person, whose infringing conduct the defendant had the “right and ability to supervise”.

**Sony Betamax case** – The milestone case in which secondary liability for copyright infringements was first assessed, is the 1984 Sony Betamax case. The US Supreme Court ruled that VCR manufacturer Sony was not liable for contributory infringement, even when some users would use Sony’s VCR for the illegal copying of television shows, because its product was “capable of substantial non-infringing uses”.

---


147 See footnotes 116 to 119.


149 See MySpace case (footnote 78) and eBay case (footnote 77)


This decision constituted an important restriction on secondary liability for copyright infringement, and is therefore often hailed as having spurred innovation. Accordingly, the Sony Betamax decision forms an important protection for producers that can ensure that their service or product is capable of substantial non-infringing use.

**Scope of the Sony Betamax protection** – Although the Sony Betamax decision constitutes an important protection, several limitations should be pointed out. First, the protection is limited to copyright infringement. Second, some courts limit the Sony Betamax protection to contributory infringement, leaving open the possibility of vicarious liability. Third, subsequent decisions have not always been consistent, and have carved out this protection when an online service provider has actual knowledge and fails to block access to (or remove) the offending copyrighted material.

**Refinement in the Grokster case** – The Sony Betamax protection was further refined and carved out in the 2005 case against peer-to-peer software manufacturers Kazaa, Morpheus and Grokster, in which the Supreme Court held that an actor “who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement by third parties.” Consequently, even if a product would be capable of legal uses, a manufacturer would still be liable for intermediary infringement when the manufacturer induces its users to infringe third party rights, which requires both an affirmative act and intent on the part of the defendant to foster infringing uses.

**Result** – Despite the limitations in the scope of the Sony Betamax protection and the ambiguity created by inconsistent case law, the Sony Betamax decision is deemed central to any discussion of the secondary liability of online service providers. Although the Sony Betamax defence was not accepted for high-profile cases involving services that were designed to infringe copyright, it seems to clear the way for service providers to experiment with new services that depend on third party content.

### 5.2. Digital Millennium Copyright Act

#### 5.2.1.Overview

**Introduction** – The Digital Millennium Copyright Act ("DMCA"), adopted in 1998, was a legal compromise for the strong lobbying work of both content providers and online service providers. On the one hand, it responded to the concern that online service providers would become so fearful of incurring secondary liability that they would be reluctant to invest in technological experimentation, while

---

152 It is sometimes called the "Magna Carta" of product innovation and technology. See P. MENELL and D. NIMMER, o.c., p. 2, although this author argues that the impact of the Sony Betamax decision should not be exaggerated, as the "capable of substantial non-infringement use" criterion has not prevented companies such as Napster, Aimster and Grokster from being held liable for secondary liability.

153 See F. VON LOHMANN, What Peer-to-Peer Developers Need to Know about Copyright Law, January 2006, available on www.eff.org

154 particularly the Napster, Aimster and Grokster cases, which deal with peer-to-peer technology to exchange (copyrighted) files between users


156 See Z. LOCKE, o.c., p. 19

157 F. VON LOHMANN, o.c., p. 9

158 M. SCOTT, o.c., p. 106

on the other hand it also responded to the concern that copyright holders would refuse to make works available online unless they were assured that their works would be adequately protected. The DMCA made US law compliant with the 1996 WIPO copyright treaties\textsuperscript{160}, heightened the penalties for online copyright infringement and addressed issues such as anti-circumvention of protection measures and access restrictions.

Most importantly from a liability point of view, section 512 of the DMCA (entitled the Online Copyright Infringement Liability Limitation Act / "OCILLA") introduces a safe harbour to online service providers for copyright claims resulting from the conduct of their customers, in light of the emerging case law regarding contributory and vicarious liability of online service providers\textsuperscript{161}. The safe harbour was conceived as to ensure that online service providers would have incentives to remove infringing material, while online service providers would also be protected from lawsuits and judgments based on secondary liability for their copyright infringements\textsuperscript{162}.

**OCILLA** – Similar to the eCommerce Directive, the DMCA reflects the state of the technology at the time the Act was adopted, and distinguishes between several types of functions that are protected from liability: mere conduit services, caching services and hosting services. Unlike the eCommerce Directive, however, the DMCA also recognises information location tools (search engines) as a fourth category of protected services. These four categories of services are subjected to various conditions that are broadly similar to the conditions imposed by Section 4 of the eCommerce Directive. For example, mere conduit service providers must not initiate the transmission, select the recipient or modify the content, while caching services must comply with information updating rules, and hosting providers (as well as search engine) must comply with notice-and-takedown requests. As is the case in the eCommerce Directive, online service providers are not required to actively monitor their systems for infringing activities\textsuperscript{163}.

**Additional layer of protection** – Similar to the eCommerce Directive\textsuperscript{164}, OCILLA only provides another layer of protection ("shield") for online service providers. When an online service provider does not meet the requirements of OCILLA, the additional layer of protection provided by OCILLA will not apply, so that the liability of the service provider will be assessed under traditional liability rules. Hence, OCILLA has merely added a second step to assessing infringement liability of service providers\textsuperscript{165}.

### 5.2.2. Differences between OCILLA and the eCommerce Directive

Despite their striking similarities, two interesting differences between OCILLA and the eCommerce Directive merit a further discussion.

**Scope** – While the eCommerce Directive protects the online service provider against liability for any type of infringement, OCILLA is strictly limited to copyright infringements.

\textsuperscript{160} WIPO Copyright Treaty art. 11, Dec. 20, 1996 and the WIPO Performances and Phonograms Treaty


\textsuperscript{163} §512(m)

\textsuperscript{164} See section 3.2 above

\textsuperscript{165} CoStar Group, Inc. v. LoopNet, Inc., 373 F.3d 544, 555 (4th Cir. 2004)
Termination policy – Unlike the eCommerce Directive, all types of online service providers (including mere conduit service providers) must implement a policy for termination of account holders who are repeat offenders, in order to benefit from the liability exemptions\textsuperscript{166,\ 167}.

Notice-and-takedown provisions – The E-Commerce Directive only states\textsuperscript{168} that the service provider must expeditiously remove or disable access to illegal information, and leaves it up to the Member States to establish procedures to implement this requirement. Conversely, OCILLA sets forth a detailed notice-and-takedown procedure. When an online service provider receives a compliant takedown notice\textsuperscript{169}, the material must be taken down expeditiously, and reasonable steps must be undertaken by the service provider to notify the alleged infringer that the material has been removed\textsuperscript{170}. The alleged infringer then has the possibility to file a counter-notice, which must be forwarded to the complainant by the service provider. In case such counter-notice has been submitted by the alleged infringer, the service provider must reinstate the allegedly infringing material if the complainant has not filed a lawsuit against the alleged infringer within 10-14 days.

5.2.3. Evaluation

The DMCA has been heavily debated, and its interpretation is far from settled\textsuperscript{171}. The criticism can be summarized around three issues: incentives to take down, incentives to send, monitoring obligations, privacy concerns and notice requirements.

Incentives to take down – The DMCA is criticized for making it too easy for copyright owners to encourage website owners to take down allegedly infringing content and links which may in fact not be infringing. When online service providers receive a takedown notice, it is almost always in their interest to take down the material, even if it is not clear if infringement is taking place, because they will never be liable to take down the allegedly infringing material\textsuperscript{172}, also when it would turn out that the material is not infringing. In practice, online service providers are therefore strongly encouraged to take down the infringing material "since no subscriber is worth even the price of a phone call to a lawyer to figure out...".

---

\textsuperscript{166} Section 512 (i): "[adopt] and reasonably [implement] ... a policy that provides for the termination in appropriate circumstances of [users] ... who are repeat infringers"

\textsuperscript{167} Furthermore, §512(i) requires the systems of online service providers to accommodate standard technical measures broadly used in industry by copyright owners to identify or protected their copyrighted works

\textsuperscript{168} Article 14.1.(b) and 14.3 of the eCommerce Directive

\textsuperscript{169} The requirements for the takedown notice are set forth in §512(c)(3). The notice must be a written and signed communication sent to the "designated agent" of the service provider, which identifies the copyrighted work, the material that is claimed to be infringing, information on how to contact the complaining party, a statement that the complaining party has a good faith belief that the use of the material is unauthorised, as well as a statement that the information is accurate and the that the complaining party is authorised to act on behalf of the owner of the material. Interestingly, the complaining party is not required to give a description of the nature of the alleged infringement (see 17 U.S.C. § 512(c) (2000))

\textsuperscript{170} Such notification must not be undertaken by search engines, as they rarely have the contact details of the alleged infringer.


\textsuperscript{172} §512(g)(1) holds that "a service provider shall not be liable to any person for any claim based on the service provider's good faith disabling of access to, or removal of, material or activity claimed to be infringing or based on facts or circumstances from which infringing activity is apparent, regardless of whether the material or activity is ultimately determined to be infringing."
what to do, it is easier just to cancel them.” 173. Anecdotal evidence indeed indicates that online service providers indeed take down content, even when the material is clearly not infringing. 174.

Such anecdotal evidence also exists for the EU. For example, in a recent Dutch study (2009), a first researcher uploaded material to seven different high-profile social network sites. Next, a second researcher submitted a complained to each high-profile social network site, asking to take down the alleged copyrighted material uploaded by the first researcher. In reality, however, the uploaded material was not copyrighted, as the copyright protection had recently expired. However, among the seven social network sites, five sites (erroneously) removed the uploaded material. 175

Incentives to send takedown notices – Copyright holders are incentivised to send takedown notices. They are not required to describe which rights are infringed. Furthermore, only “knowingly materially misrepresented” takedown notices 176 can lead to liability of the copyright holder, so that non-compliant, vague or unfounded takedown notices will generally 177 not raise any liability for the copyright holder. As demonstrated by an ongoing study 178, the incentivation of copyright holders to send non-compliant takedown notices is not merely theoretical: out of a set of 876 takedown notices, almost one third contained at least one major non-compliance flaw 179, such as an issue with the underlying copyright claim 180, formal non-compliance 181 or non-applicability of the takedown procedure 182. In practice, the DMCA shields copyright owners from liability for shutting down non-infringing content by mistake, “even if the copyright owner acted unreasonably in making the mistake” 183. Only recently has some case law criticized evident notice-and-takedown abuses by copyright holders 184.

No incentive to counter-notify – Contrary to the incentives given to copyright holders to file a takedown notice, the DMCA is much more demanding with respect to the counter notice 185. First, the content owner must wait until the allegedly infringing material is effectively removed, before he can take any action at

---

173 M. SCOTT, o.c., p. 129
174 See (1) C. AHLERT, C. MARSDEN and C. YUNG, How Liberty Disappeared From Cyberspace, May 2003, available at http://www.socleg.ox.ac.uk/text/liberty.pdf. The authors posted texts that were clearly in the public domain on a free website hosted by a UK and a US ISP. The UK-based ISP promptly took down the site with minimal investigation, while the US-based ISP first requested compliance with the DMCA requirements; (2) In a similar follow-up test conducted in the Netherlands, 7 out of 10 ISPs took down the allegedly infringing material (see www.bof.nl/docs/researchpapersSANE.pdf).
175 §512(f)
176 Contra: Online Policy Group v. Diebold, Inc., 337 F. Supp. 2d 1195 (N.D. Cal. 2004), in which the Court ruled that the complainant (Diebold) should have known that internal corporate e-mails are not protected by copyright, and could therefore not be used to request a takedown. Despite this high-profile case, supported by pro bono legal support, the threshold for invoking §512(f) is very high, as the mere subjective belief that materials were infringing (even if that belief was incorrect) does not qualify as a “knowing misrepresentation”: J.M. URBAN and L. QUILTER, o.c., p. 630
177 Rossi v. Motion Picture Ass’n of America, 391 F.3d 1000, 1004-05 (9th Cir. 2004).
178 “Chilling Effects Project” (www.chillingeffects.org), a joint project of the Electronic Frontier Foundation and a consortium of law faculties, as reported by J.M. URBAN and L. QUILTER, o.c. One of the reasons to create this project, is to monitor the use of the notice-and-takedown procedures. In light of the fact that these procedures are handled by private parties, few cases actually reach a court, which renders it difficult to track such procedures.
179 J.M. URBAN and L. QUILTER, o.c., p. 666
180 For example, takedown claims regarding information that is not copyrightable, takedown notices where a fair use defence clearly applied, or takedown notices relating to other areas than copyright (such as trademarks or unfair competition).
181 such as a failure to identify the allegedly infringing material, or a failure to provide the complainant’s contact information
182 such as a takedown notice being sent to a mere conduit service provider
183 M. SCOTT, o.c., p. 101-102
184 Lenz v. Universal Music Corp. (572 F. Supp. 2d 1150 (N.D.Ca. 2008))
185 M. SCOTT, o.c., p. 132
all. Secondly, the content owner must be willing to swear, under the penalty of perjury, that the material was removed as the result of "mistake or misidentification". Third, it is not clear whether this "mistake or misidentification" also covers an erroneous legal analysis. As a result, there is growing evidence that the counter-notification possibility is rarely used\(^\text{186}\).

**Privacy concerns** – Regardless of whether the online service provider effectively takes down the material, copyright holders can issue a subpoena to the service provider, who is then legally obliged to disclose the identity of the alleged infringer to the copyright holder (assuming such information is in its possession)\(^\text{187}\).

**Effectiveness** – Despite the various concerns, most legal commentators accept that the DMCA has spurred the development of new online services, in particular Web 2.0 services that deal with large amounts of third party content\(^\text{188}\).

### 5.3. Communications Decency Act

#### 5.3.1. Overview

**First purpose** – The Communications Decency Act\(^\text{189}\) ("CDA") was adopted in 1996 as a response to the rising concern over the impact of Internet pornography on children. It criminalises anyone who exposes minors to offensive, obscene or indecent material online.

**Second purposes** – At the same time, the CDA was a response to prior case law that penalised online service providers that had made efforts to police such material\(^\text{190}\). According to this prior case law – particularly the notorious *Stratton v. Prodigy* case\(^\text{191}\) – online service providers that would monitor or edit the content hosted by them, were opened up to a greater liability than service providers that do not make such choice. Consequently, this case law induced service providers to refrain from monitoring any content hosted by them, as the less engaged they were with the content, the less likely they could be held liable\(^\text{192}\).

---

\(^{186}\)&nbsp;According to the data set gathered by Chilling Effects, only 7 counter-notifications were filed on a total of 2000 takedown notices

\(^{187}\)&nbsp;§512(h)

\(^{188}\)&nbsp;D. KRAVETS, "10 Years Later, Misunderstood DMCA is the Law That Saved the Web", available at blog.wired.com/27bstroke6/2008/10/ten-years-later.html, 27 October 2008: "If you’re wondering whom to thank for the Web 2.0 explosion in interactive websites, consider sending a bouquet to Congress. Today’s internet is largely an outgrowth of the much-reviled Digital Millennium Copyright Act"


\(^{190}\)&nbsp;O. MEDENICA and K. WAHAB, o.c., p. 247

\(^{191}\)&nbsp;In this case, the plaintiff (Stratton) sought to hold a network provider (Prodigy) liable for libellous comments posted on one of its bulletin boards. Although prior case law (*Cubby, Inc. v. CompuServe, Inc*, 1991) had considered a network operator to be a distributor (who is only liable for defamatory comments if he knew their libellous nature), the Court ruled that Prodigy was to be considered as a publisher, as it positioned itself as a family-oriented computer network and had advertised to exercise control over the content on its bulletin boards. As publishers are subject to a strict liability regime for defamatory content, the Court held Prodigy liable. See H. HOLLAND, "In defense of online intermediary immunity: facilitating communities of modified exceptionalism", *Kansas Law Review*, Vol. 56, 2007, p. 103-104

Content – As a direct response to this case law, the CDA also introduced a liability exemption against publisher's liability in its section 230: "no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider". Furthermore, the CDA tries to encourage service providers to self-regulate content, as "no provider or user of an interactive computer service shall be held liable on account of (...) any action voluntarily taken in good faith to restrict access to or availability of [obscene material]". Note that, contrary to the eCommerce Directive and the DMCA, the CDA does not require the service providers to comply with a notice-and-takedown procedure in order to benefit from the liability protection.

Although most of the CDA's anti-indecency provisions (§223) were held to be unconstitutional by the Supreme Court in 1997 due to a violation of the freedom of speech provisions of the First Amendment, the CDA's liability exemption (§230) still applies.

5.3.2. Interpretation

Service providers covered – Starting with the Zeran v. America Online, Inc. case, courts consistently extended the application of the CDA by using a broad definition of "interactive computer services", which is found to encompass hosting services, e-mail service providers, auction websites, general web shops, personal home pages, company websites, dating websites, chat rooms and internet access points. These parties are also allowed to make (minor) alterations to the information, while still benefiting from the liability protection.

Users covered – The courts have also made clear that not only providers, but also users of such services are within the scope of the protection: "Congress did not intend for an internet user to be treated differently than an internet provider". As a result, a user of a newsgroup cannot be held liable for reposting libellous comments made by another use, and a service provider cannot be held liable for the content published on its request.

Types of liability covered – Furthermore, although the text of the CDA only refers to publisher's and speaker's liability, the courts have considered that distributor's liability was covered by the CDA. Finally, the courts have expanded the types of claims against which protection is provided: these not only include claims regarding defamation, but also sale/distribution of (child) pornography, sexual assault, distribution of incorrect information and privacy infringements. The only types of claims that are not covered by the CDA, relate to intellectual property infringements (including trademarks).

---

193 Conference report on the CDA (H.R. Conf. Rep. No. 104-458 at 194 (1996)): "One of the specific purposes of [Section 230] is to overrule Stratton-Oakmont v. Prodigy and any other similar decisions which have treated such providers and users as publishers or speakers of content that is not their own because they have restricted access to objectionable material."


195 129 F.3d 327 (4th Cir. 1997)

196 See H. HOLLAND, o.c., p. 105-107

197 Barrett v. Rosenthal, 146 P.3d 510, 527 (Cal. 2006)

198 ibid.

199 Blumenthal v. Drudge, 992 F. Supp. 44 (D.D.C. 1998), in which internet service provider AOL was not held liable for the defamatory statements made by columnist Matt Drudge, even though these defamatory statements were part of a set of rumour & gossip columns written by Drudge at the request of AOL.

200 H. HOLLAND, o.c., p. 106

201 See Jane Doe v MySpace (available at http://en.wikisource.org/wiki/Doe_v._MySpace,_Inc.), in which a US District Court agreed that social community site MySpace is protected by the CDA from liability for the sexual assault and subsequent suicide of a 14-year-old girl who met her attacker on the website.
Minority view – It should be noted that the analysis below reflects the majority view on the CDA. There is some case law that adheres to a more narrow view on the protection offered by the CDA

5.3.3. Evaluation

Very wide scope – The CDA shields online service providers from nearly all forms of tort liability for defamatory speech and other types of content created by a third party, effectively becoming an absolute shield for service providers. For example, in a delicate case of child pornography, the chat room owner was informed that photographs and videotapes were being exchanged. Even though the terms & conditions of the chat room allowed to terminate the membership of any member infringing the T&C, the chat room owner neither warned the member to stop, nor suspended access to the chat room. The Florida Supreme Court found the chat room owner to be immune under the CDA. In another case, auction website eBay was found to be protected by the CDA for the sale of fraudulent autographed sports memorabilia, even though Bay was extensively informed about the fraud and did not undertake action. The very wide scope of and effects of the CDA is criticised by US legal authors, who question whether the distinction between online service providers (who are almost absolutely shielded from liability claims) and offline players, such as printed newspapers (which are subject to a strict liability regime), is still valid in today's internet society.

Discouraging monitoring and self-regulation – Although the CDA was initially conceived to encourage online service providers to self-regulate, US case law relating to the CDA does not encourage service providers to self-regulate. Neither does the CDA incentivise online service providers to monitor the third party content hosted by them. On the contrary: due to the absence of a notice-and-takedown procedure in the CDA and the absolute shield accorded, online service providers are encouraged to take no action at all under the CDA. As from the Zeran case, US courts have clearly wanted to shield online service providers from the chilling effects of tort liability: “[I]t would be impossible for service providers to screen each of their millions of postings for possible problems. Faced with potential liability for each message republished by their services, interactive computer service providers might choose to severely restrict the number and type of messages posted.”

6. Comparison with the United States

This section provides a high-level comparison of how the United States and the EU deal with the legal treatment of online intermediaries. These differences are then applied to various types of online service providers.

---

202 See Doe v. GTE (347 F.3d 655 (7th Circ. 2003)) and Barnett v. Rosenthal (later on reversed by the Supreme Court of California). Some influential US authors also argue against broad protection for online intermediaries, because broad protection discourages intermediaries to take preventive measures, although they are closest to the source of the harm, so that it would be cheapest for society if these intermediaries are held liable for illegal material.
203 O. MEDENICA and K. WAHAB, o.c., p. 239-240
204 L.P. MACADO, o.c., p. 4
205 O. MEDENICA and K. WAHAB, o.c., p. 252
206 Doe v. Am. Online, Inc., 783 So. 2d 1010 (Fia. 2001)
207 Gentry v. eBay, Inc., 121 Cal. Rptr. 2d 703, 717 (Ct. App. 2002).
208 Zeran v. America Online, Inc., 129 F.3d 327 (4th Cir. 1997), at 331
6.1. Less protection and more uncertainty for online service providers

In the United States, online service providers seem well protected – perhaps even overly protected – against third party liability, due to the combination of a clear takedown procedure for copyright infringements, an extensive court interpretation of the exemption for defamatory content and an interesting “Sony Betamax” defence for services that are capable of substantial non-infringing use.

Although the information available to us indicates that the eCommerce Directive sufficiently protects “traditional” services that entirely correspond to the technologies available at the time the E-commerce Act was drafted (i.e., internet access, caching and web hosting), the protection accorded to other types of online services is not clear. Accordingly, providers of new business models – particularly Web 2.0 models\(^{209}\) – are less protected in Europe than in the United States against liability claims caused by third party content.

6.2. More uncertainty for rightholders and users

Although primarily online service providers are impacted by this legal uncertainty, it should be pointed out that other parties are also affected. For example, discussions between internet service providers and rightholders will often break down due to the varying case law and the divergent national laws, resulting in increased litigation. Furthermore, due to the lack of a harmonised, clear and detailed notice-and-takedown procedure, rightholders face greater legal costs and/or more uncertainty when trying to take down illegal information across the EU.

Users of online services may also be affected, as service providers may be become more cautious in their online offerings, or implement monitoring systems, in order to reduce the likelihood of liability claims. It is also interesting to note that, contrary to the wide protection granted by the CDA, users in the EU are not protected by liability exemptions when distributing content posted by other users.

6.3. Examples

In order to illustrate the concerns, it is useful to investigate several examples:

**Traditional web space hosting** – Traditional web space hosting – i.e., providing space to upload files, which are subsequently published on a website – is clearly targeted by article 14, as evidenced by the term "hosting" in the heading of article 14, as well as legal doctrine\(^{210}\). However, web space hosting services offered by public authorities (universities, municipalities, ...) may not fall within the scope of article 14, contrary to the situation in the United States.

**Internet access provision** – Traditional internet access (by dial-up, ADSL, cable, satellite, ...) offered by commercial companies is said to fall within the scope of article 12\(^{211}\). However, internet access provision offered by public authorities may not fall within the scope of article 12. Furthermore, internet access provided by free wireless networks, citizen networks or distributed network anonymisation services, may not fall within the scope of article 12 either. Conversely, the US DMCA does not require remuneration, so that all examples enumerated will benefit from its protection regime.

**File storage services** – File storage services – e.g., online backup services – qualify for protection as hosting providers under the eCommerce Directive (on the condition that service providers comply with

---

\(^{209}\) French Commission Report, o.c., p. 7


\(^{211}\) Although we refer to the ambiguity created by the definition of information society services: see section 4.1.2 above
the takedown provisions). Even so, service providers may be required to actively monitor files that are being uploaded by their users \(^{212}\). Conversely, in the United States, file storage services will likely be protected by the CDA and the DMCA.

**Online auctions** – As already pointed out in the introduction, French and Belgian courts do not qualify online auction providers (such as eBay) as hosting providers, as their services are not limited to the storage of information regarding auctioned items. In the United States, online auctions are protected by the CDA, although it should be pointed out that the scope of the CDA does not extend to copyright or trademark infringements.

**Blogs** – It is questionable whether writers of blogs \(^{213}\) fall within the scope of the special liability regime of the eCommerce Directive when they would face liability questions due to comments being posted by their readers. First, it should be recognised that blogs are typically provided for free \(^{214}\), so that the activity of writing a blog will often not qualify as an information society service. Second, the storage of reader comments is only a small part of the blog writing activity, so that courts are not likely to qualify blog writers as hosting providers. Conversely, US case law has accorded CDA protection to comments provided by third parties.

**Discussion forums** – The analysis of the liability of discussion forum operators is analogous to blog writers: the "normally provided for remuneration" requirement may not be met, and the act of storing discussions may not qualify as "hosting", as discussion forum operators may be involved in some of the discussions and discussion forums may also offer editing facilities. Conversely, US case law has accorded CDA protection to comments provided by third parties.

**Wiki’s** – Similar to blogs and discussion forums, wiki’s – which are often accessible for free – may not qualify for the special liability regime, as they may not meet the "normally provided for remuneration" criterion, they may provide facilities beyond mere storage (such as publishing tools, editing tools, revision history, ...) and they may exercise control over the content \(^{215}\). Some courts may, however, sub-divide the services offered by wiki’s into various sub-services, and qualify only selected sub-services as hosting services. Again, US case law offers a better protection for such wiki’s.

**Chat networks** – Operators of chat networks do not qualify as hosting or caching providers, but may qualify as mere conduit service providers, as they provide access to communication networks \(^{216}\). In order to benefit from the special liability regime, however, chat operators must refrain from filtering or modifying the chat conversations. Conversely, case law has applied the CDA protection to chat networks.

**Virtual worlds** – A considerable amount of courts will not consider operators of virtual worlds (such as Second Life) and multiplayer online games (such as World of Warcraft) to meet the conditions of the special liability regime, as storage-related facilities only constitute a small part of the service offering \(^{217}\). Some courts may, however, sub-divide the service into various sub-services.

---

\(^{212}\) See footnote 125

\(^{213}\) A different analysis applies to operators of blog tools, who are more likely to qualify as hosting providers vis-à-vis the blogs written by their users and the comments posted by blog readers.

\(^{214}\) Some blog writers may be sponsored by advertising revenue.

\(^{215}\) As an example, encyclopaedia Wikipedia is permanently monitored by a team of content managers, to ensure that the information being published is accurate, verifiable, built on solid sources, and excludes personal opinions.

\(^{216}\) See section 4.2 above

\(^{217}\) which also includes software to build characters and environments, chat facilities, programming tools, currency exchange, etc.
Social websites – Social community websites (such as MySpace, Netlog, Facebook and Twitter) offer tools to their users to build a personal profile online, publish photos, host music, post blog messages, communicate with friends, etc. Similar to virtual worlds, there is a risk that courts across the EU will not qualify social community websites as hosting providers, considering that storage is merely one of the various aspects of their services. Again, some courts may sub-divide the service into various sub-services.

Photo sharing websites – Even photo sharing websites (such as Flickr and PhotoBucket) may not qualify for the special liability regime, as they offer various tools to edit photos, order prints and communicate with other users.

Web services and "mash-ups" – The provision of software is shifting from a traditional licensing model towards a service-oriented architecture ("software as a service" model), where software and computing facilities are rented on an as-needed basis, and so-called "web services" from various vendors are concatenated. The integration of web services may result in a mash-up, i.e. a web application that integrates data from various sources and webservices.

While some of these web services involved may store information (and may thus qualify as "hosting services"), other web services merely process information, whereby storage would at most be a mere ephemeral phenomenon. On a conceptual level, the question arises why only the storage-related web services would qualify for protection under the eCommerce Directive (excluding other web services), while the amount of data being processed would call for protection of the online intermediary.

Cloud computing – Cloud computing refers to the internet-based ("cloud") development and use of computer technology, whereby dynamically scalable virtualised resources are provided "as a service over the Internet". Cloud computing services are the latest trend in information processing technology, and encompass a variety of services, which may also relate to data storage. However, considering that cloud computing services are usually not limited to storage, it is questionable whether cloud computing service providers qualify as "hosting providers" under article 14 of the eCommerce Directive.

6.4. Dual protection regime

While the protection regime afforded to online intermediaries is stronger in the United States, this regime is not without issues either.

Contrary to the European Union, the United States uses a dual protection regime (the DMCA and the CDA, each with their own scope and purpose). It is only through the combination of both Acts that the United States offers a better protection than the European Union for online intermediaries. This dual protection regime results in a more fragmented regime than the approach taken by the European Union, because the DMCA and the CDA have a very different scope, and use different procedures (only the DMCA imposes a notice-and-takedown procedure).

The question arises whether this fragmentation is desirable from a policy point of view. For example, a right of an injured party of defamation is not protected at all under the CDA. On the other hand, the right of the intellectual property right holder is much more protected by the DMCA, because the right holder is likely to be successful in having the allegedly infringed material taken down. The question arises whether it is desirable to treat rights other than intellectual property rights in a subordinate way.

218 See the Wikipedia-entry for cloud computing (en.wikipedia.org/wiki/Cloud_computing)
7. Conclusions

1. The special liability regime introduced by the eCommerce Directive has contributed to the further development of online services, particularly in the first years following the introduction of the Directive. Despite some court decisions to the contrary, the three traditional types of services targeted by the special liability regime (internet access, caching and web hosting) seem to have received adequate protection to further develop their services. The Directive has therefore reached its goal of protecting traditional internet access providers, caching providers and web hosting companies against liability caused by content provided by their users.

2. However, over the years, various weaknesses of this liability regime have emerged. One such weakness is formed by the legal gaps in the scope of the special liability regime: no uniform notice-and-takedown procedure, no uniform conditions regarding injunctions, no mandatory protection for search engines, and no mandatory protection for hyperlinking. These gaps, in particular the lack of a uniform notice-and-takedown procedure and the lack of uniform conditions regarding injunctions, have led to considerable divergences across Member States, which is likely resulting in increased costs and risks for cross-border transactions. These legal gaps no longer seem justified, in particular when compared to the United States.

3. The special liability regime is too focused on (only) three types of services. While the focus on these services was arguably relevant at the time when the Directive was drafted – because these were the services that needed protection at that time – a staggering amount of new types of services and service delivery models have developed, which are increasingly exposed to liability issues, due to the fact that the scope of the special liability regime is too specific, too dependent on particular technologies. As a result, an entire list of, particularly new, service models — including Web 2.0 services, cloud computing services and web services — are not protected, contrary to a highly specific service such as caching. It is difficult to find a justification for this discrepancy.

4. The scope of "hosting services" is ambiguous, and has triggered diametrically opposing decisions from courts across the EU. The most important cause of confusion is the requirement that a hosting service must "consist of" the storage of information. When intermediary immunity was first introduced, there was a clear economic separation between the intermediary and the content originators. However, modern intermediary business models are moving away from this clear separation. This leads to the question of to which extent heterogeneous/hybrid services (such as auction services, content sharing services, wiki's, cloud computing services, web services, etc.) can be considered hosting services. Accordingly, if the overarching aspects of a service do not relate to storage, there is a considerable risk that the service no longer qualifies for protection under the special liability regime.

Another ambiguity in this regard is the assumption of article 14 that hosting providers have no interest in the relationship between the communicating parties. This divide is increasingly blurred. Service providers sometimes do exercise some level of editorial control (for example, when moderating or compiling user contributions), although the bulk of the content remains user-contributed. Similarly, online auction providers do not merely provide a sales platform to sellers, but also advise their users on effective selling techniques and shares in their success\(^\text{219}\).

5. The special liability regime allows courts to issue injunctions: even when online service providers would not be liable for storing or transmitting third party content, they can still be ordered to remove third party content and/or prevent the alleged infringements from re-occurring in the future. Member States vary to a significant degree as to the conditions for an injunction to be issued, as well as the

---
different types of measures that can be imposed on service providers. The uncertainty surrounding the possibility to issue injunctions should not be underestimated, as injunctions can lead to costly lawsuits, public exposure and technical implementation costs for service providers.

6. **Various ambiguities** in the special liability regime undermine its strength, triggering uncertainty among stakeholders and courts. History therefore also repeats itself with respect to the divergences in national case law. The most detrimental ambiguities can be summarised as follows:

- The fundamental definition of "information society services" excludes services that are not "normally provided for remuneration". Depending on the interpretation, this may create uncertainty for online activities that are provided for free, depend on indirect revenue models or are provided by public authorities. This criterion particularly risks to expose "freemium" web services to liability.

- It may be the case that various decentralised content distribution systems, including popular peer-to-peer networks, can be qualified as "caching services", so that their users would enjoy considerable protection under the special liability regime.

- It is not clear for online service providers which information qualifies as "illegal information", which must be removed or blocked by online service providers.

7. The legal gaps of the eCommerce Directive, its dependence on specific services, its various ambiguities and its restricted scope lead to **diverging case law**, across (but sometimes also within) Member States, and thus considerable legal uncertainty for online service providers. There is abundance evidence that courts and legal practitioners encounter difficulties to apply the special liability regime, and seem inclined to find arguments to put aside the special liability regime and instead revert to more general rules of legal doctrine. This results in **considerable legal uncertainty for online service providers**, in particular for new service models.

8. Meanwhile, in the United States, online service providers benefit from an **almost absolute protection** under the Communications Decency Act for a variety of liability claims caused by third party content, including defamation, distribution of unlawful content and incorrect information, as well as privacy infringements. Although this almost absolute shield does not protect online service providers against intellectual property claims in the US, they are also better protected against these claims due to the Digital Millennium Copyright Act's straightforward and harmonised notice-and-takedown procedure. There are clear indications, however, that the US notice-and-takedown procedure gives too much incentives to service providers to always block / remove third party content when receiving a claim (which may chill free speech and foster censorship by copyright holders). Finally, also **US case law relating to secondary liability** incentivizes service providers to experiment with services that depend on third party content, as they are deemed exempted from liability when their services are capable of substantial non-infringing use.

9. **Japan** has also adopted a legal framework which protects online intermediaries against third party liability. Contrary to the European and American approaches, the Japanese special liability regime does not divide service providers into three / four subcategories. Instead, the liability protection applies to any online service provider whose purpose is to communicate third party information to other parties, whether or not such service is offered for remuneration. Similar to the eCommerce Directive, the Japanese legal framework protects against any type of liability, but does not protect against injunctions. Interestingly, the Japanese legal framework also protects the intermediary against claims from its users for having wrongfully taken down illegal material.

---

Hence, the United States and Japan offer a significantly better level of liability protection to “new” types of online services, such as Web 2.0 and cloud computing services.

8. Recommendations

In this section, we provide a list of recommendations to solve various issues identified in this chapter. A distinction is made between recommendations that can be implemented on the short term (2010-2015), the mid-term (2015-2020) and the long term (2020 and beyond). These time frames align with the relative political and legal difficulty to implement these recommendations, as well as the urgency involved. Hence, the threshold for implementing recommendations for the short term is relatively low, or the urgency involved is rather high. Conversely, recommendations for the mid-term require important legal modifications, or may receive more political resistance. Recommendations for the long term are of a more visionary nature.

8.1. Overview of recommendations

8.1.1. Scope of "information society services"

Taking into account the ambiguities relating to the criterion of "normally provided for remuneration", the risk exists that case law may arise that would consider that some types of mere conduit / caching / hosting activities do not qualify as "information society services" because they are provided for free, or are remunerated only very remotely. Accordingly, such activities would not be protected by the special liability regime, and would not benefit from the freedom of establishment and the freedom of online service delivery (even when they would meet all other criteria set forth in articles 12 to 14).

When this ambiguity would not be resolved by case law, we recommend to consider adopting a different criterion.

It could, for example, be envisaged to abolish the requirement that activities must constitute economic activities, as it is difficult to justify why economic activities merit a better protection level than non-economic activities.

In the short or medium term, this different criterion could be used to define the scope of the special liability regime. However, in order to also use this different criterion for the freedom of establishment and the freedom of service delivery, a change of the EC Treaty will be necessary. Such will, obviously, only be possible in the long term.

8.1.2. Optimised wording

In the short term, several flaws in the wording of the eCommerce Directive should be fixed, in order to render the definition of "information society services" and the concepts used in articles 12 to 14 more suitable for new technologies and new business models, and to improve legal certainty.

Selection or modification – The "selection or modification of information" criterion for mere conduit providers should be changed to avoid that minor selections or modifications to the information transmitted, undermine the applicability of the special liability regime.

---

221 because the scope of the special liability regime is not necessarily restricted by the scope of article 50 of the EC Treaty (which deals with the essential freedoms)
**Mere conduit** – In order to resolve the issue described in section 4.1.2 – *i.e.*, “mere conduit” services cannot deal with physical signal transmission – we recommend to clarify the scope of “mere conduit” services, by removing the "normally provided for remuneration" requirement (e.g., by the decoupling described above) and clarifying that mere conduit services also encompass "electronic communication services", as defined in Directive 2002/21/EC.

**Caching** – Although several ambiguities can be found in the definition of caching, we do not consider it a priority to clarify this definition in the short term. In the medium term, however, we recommend to merge the caching exemption in a broader field of protected services.

### 8.1.3. Hosting

The definition of hosting services has arguably triggered most of the case law concerning the special liability regime. We therefore recommend to at least clarify this definition, and also to resolve – if possible – the discrimination between storage-focused services and information-processing services.

**Short term** – In the short term, the definition of hosting service could – for example – be redefined as an information society service that consists, in at least one aspect, in the storage of information provided by a recipient of the service. It should then also be clarified that related information society services together constitute one information society service.

**Mid-term** – In the medium to long term, we would consider it appropriate to replace the current three-fold structure of the special liability regime by a two-fold structure, consisting of:

- mere conduit service providers; and
- third party information processors, *i.e.* anyone who provides a service for which at least one non-trivial aspect consists of the processing of information provided by a recipient of the service (whereby processes is to be construed as including activities such as collecting, indexing, hyperlinking, storing, recording, organising, publishing, altering, consulting, using, etc.)

The protection of caching services – which is too technology-specific and does not seem to be frequently invoked anyway – would then be distributed over both categories: the transmission aspects would be covered by the protection of mere conduit service providers, while the storage aspects would be covered by the protection of third party information processors. Conversely, search engines and hyperlinking activities would be subsumed entirely by the second category.

In our opinion, such larger protection of information society providers, would foster the further uptake of online services. However, this enlargement should always be balanced by an appropriate notice-and-takedown procedure (for example the procedure outlined above in section 8.1.4), as well as a "Grokster-like" provision to counter online piracy and alleviate concerns of copyright holders. Such provision

---

222 Provided, of course, that the "normally provided for remuneration" requirement is also removed from the definition of "electronic communication service"

223 Should clarification nevertheless be considered (and the caching exemption would not be merged into a broader exemption), we would recommend to clarify to which extent hierarchically distributed systems fall within the scope of the caching exemption.

224 Assuming that the recommendations for the short term have been implemented

225 Our proposal is similar to the proposals of C. REED, "Policies for Intermediary Immunity", *Computers & Law*, February & March 2009, p. 20-23. He claims that "immunity should be granted to those whose primary function in respect of content is communicating it on behalf of others. Secondary activities would not normally affect immunity".

226 In the famous 1984 case against Sony, the US Supreme Court held that Sony had no liability for manufacturing VCRs, even though some users would use Sony's VCR for the illegal copying of television shows. According to this decision, a
would exclude companies that offer services that *induce users to infringe third party rights*. According to this test, companies do not incur liability when their products or services do not induce infringements by users, even though some users would use the services in a clearly infringing manner.

**Good faith control** – Online service providers that exercise good-faith control over third party content hosted by them (e.g., cleaning up offending user comments on a blog; removing spam messages from a forum; monitoring offensive language in a chat room; etc.) must not loose the protection afforded by the special liability regime.

### 8.1.4. Notice-and-takedown

A harmonised, detailed and clear notice-and-takedown procedure should be introduced\(^2\), which balances the rights of the online service providers, the service users, as well as the plaintiffs.

**DMCA-like model** – As a starting point, we are of the opinion that it could be interesting to investigate the procedural model used by the DMCA. However, considering that the DMCA clearly favours plaintiffs (and, secondarily, the service providers) to the detriment of the service users, we propose to alter the DMCA takedown procedure, so that the infringing material would not be taken down immediately. This is also the approach taken by the Japanese legal framework on the liability of online intermediaries\(^2\).

Similar to the Japanese approach, we propose that the service provider must forward the claim to the user. Provided the user has not responded, or does not contest the plaintiff's claim within a reasonably short period of time (e.g., five business days), the service provider must then take down the material.

The service provider should, however, immediately take down certain types of material, for which the infringement is highly obvious to any person (e.g., child pornography, obvious racist material, or piracy of (recent) audiovisual material).

---

\(^2\) The question arises, however, whether the European Community is competent to harmonise procedural law (such as a notice-and-takedown procedure) in light of article 65 of the EC Treaty, and the principles of subsidiarity and proportionality. Article 65 empowers the European Community to adopt measures in the field of judicial cooperation, and has generally been used to adopt "classical" private international law regulations. During the legislative procedure to adopt the regulation on a European order for payment procedures (1986/2006) and the regulation regarding a European small claims procedure (861/2007), the competence of the European Community to regulate procedural law, was discussed. Although the Commission and the Economic and Social Committee maintained the view that the scope of such procedures should not be limited to cross-border disputes, this view was not supported by the Parliament and the Council, so that both procedures were eventually limited to cross-border disputes. Hence, there are concerns with respect to the possibility to adopt a harmonised notice-and-takedown procedure, which should be further investigated. It should be noted, however, that voices are raised to further debate the scope of article 65 EC Treaty (See X.E. KRAMER, "A Major Step in the Harmonization of Procedural Law in Europe: the European Small Claims Procedure", in A.W. JONGBLOED (ed.), The Xllth World Congress of Procedural Law: the Belgian and Dutch Reports, 2008, Antwerp, Intersentia, p. 15)

\(^2\) The intermediary must first convey the takedown claim to its user. If the user consents to the blocking or fails to reply within seven days thereafter, the intermediary may block the right-infringing material without being liable to its user. According to the official comments on the legal framework, this procedure balances the interests of both the claimant and user: in order not to overly restrict the user’s speech right, he/she is given an opportunity to reply before his/her material being blocked.
Dedicated agents – Considering that notice-and-takedown procedures are more likely for specific services—such as auction websites—and taking into account that it can be difficult and costly for service providers to assess whether material is effectively infringing, it could be interesting to introduce sector-specific, dedicated (yet independent) third party agents who would be involved in the takedown procedure.

For example, in case a manufacturer would determine that a counterfeited product is offered for sale on an auction website, the manufacturer can contact the service provider's dedicated takedown agent (when no such agent would be known for a particular service provider, the country-level or sector-level agent can be contacted). This agent will then investigate the claim, and inform the service provider whether or not the claim is justified. If the claim is justified, the infringing material would be taken down immediately after the agent's decision, and the user would be informed. If either the user or the manufacturer would object against the decision of the agent, a court procedure can be initiated.

Both the user and the manufacturer should, however, be incentivised to not initiate legal procedures in vain. This could be achieved, for example, by requiring that the party which loses the lawsuit, has to pay the costs of the lawsuit and [three] times the cost of the agent (whereby the agent, the service provider and the winning party would be entitled to one third).

Finally, a scheme may be envisaged whereby the general cost of the agent would be borne by a sector-level cost distribution mechanism.

Standards and self-regulation – In addition to (or as an alternative to) dedicated agents, the European Commission should foster the creation of standards on how rightholders can cooperate with online intermediaries to make the notice-and-takedown procedure as efficient as possible for all parties involved. On large online platforms (such as video sharing platforms or online auctions), it can be burdensome for a rightholder to manually check whether the available content infringes its rights.

Technical standards should specify how selected rightholders (or rightholders associations or the dedicated agents described above) get privileged access to the platform and dedicated tools to search for infringements, while respecting the privacy of users and confidentiality of transactions/material. These standards should also specify how the rightholder can suspend a transaction/material, and how the platform user can protest against the takedown.

A well-known example is the Verified Rights Owner (VeRO) program of eBay, which provides right owners with additional possibilities to help reporting listings that infringe their rights. VeRO offers dedicated communication channels, with priority e-mail queues for reporting alleged infringements and offers rapid responses by eBay in ending listings reported as infringing. In addition, right owners subscribed to the VeRO program have the ability to obtain identifying information about eBay users (including name, address, phone number and e-mail address) in case of infringements.

While adoption of the standards would be optional (but recommended) for most online service providers, the standards should be mandatory for online platforms that are both sufficiently large and (by their nature or implementation) attract a non-trivial amount of infringing material. It is important to find such a threshold towards mandatory adoption that protects the interests of rightholders, yet does not discourage the creation of new platforms.

---

229 eBay VeRO Programme, available at http://pages.ebay.co.uk/vero/about.html
230 eBay Privacy Policy, available at http://pages.ebay.co.uk/help/policies/privacy-policy.html#disclosure_new
8.1.5. Injunctions

Mere conduit – In today's connected society, providers of central connectivity services (such as internet access and internet backbone operations, but also central DNS systems) are becoming increasingly important. As these service providers are technically involved in various steps of the information delivery workflow, they are increasingly facing injunctions to solve issues that arise between private parties with whom the service provider may even not have any (contractual) relationship.

We are of the opinion that such injunctions must be limited to the fullest extent possible. In other words, the special liability regime must be enlarged to not only protect these parties against liability, but also against costly and burdensome procedures initiated against them. We recommend to only allow injunctions when both the legal and technical costs associated with the injunction would be borne by the plaintiff, and all other legal (or technical) actions have been exhausted so that the injunction against the mere conduit service provider is a last resort. Injunctions against central connectivity service providers should also remain possible in urgent and seriously threatening cases.

Other online service providers – Injunctions against online intermediaries other than mere conduit service providers, are reported to be fairly limited in court practice. When it is also taking into consideration that the link between such intermediaries and their users is often more direct, and that their role is less central than the role of central connectivity providers, we do not consider it necessary at this moment to limit or harmonise injunctions against them.

8.1.6. Long term

Taking into account today's continuing trend of contradicting court decisions, we are convinced that the extra protection accorded to some online service providers is necessary in the short and medium term (if only to "educate" courts and legal practitioners on the business models and technical aspects of online services), particularly due to the fact that many online service providers inherently operate cross-border.

However, in the long run, we think that this distinction between online and offline service providers (the so-called "dualism" or "internet exceptionalism") should no longer be made, as we assume that the specific characteristics of internet services will become familiar to all legal practitioners, so that the "training wheels" accorded by the eCommerce Directive can be left out.

---

231 This will, in most cases, avoid that the scope of the requested injunction would be too large. For example, a rights holder will not request a service provider to screen each and every file uploaded by its users, because this would easily become prohibitively expensive.

232 See Study on liability of internet intermediaries, p. 32

233 See H. HOLLAND, o.c.; J. HUGHES, "The Internet and the Persistence of law", Boston Col. L. Rev, 2003
EU study on the

Legal analysis of a
Single Market for the Information Society

New rules for a new age?

7. Electronic payments
8. Electronic contracting

November 2009
Chapter 7 Electronic payments

1. Introduction
2. High-level overview of e-payments
   2.1. Why is there a need?
   2.2. Requirements for successful electronic payment systems
3. Legal instruments
   3.1. Previous eMoney Directive
   3.2. New eMoney Directive
   3.3. Payment Services Directive
4. Types and modalities of electronic payments
   4.1. Smart cards
   4.2. Server based e-money
   4.3. Disposable and virtual pre-funded cards
   4.4. Platform payment systems
   4.5. Mobile payment systems
   4.6. Vouchers and gift cards
   4.7. Money in virtual worlds
   4.8. Escrow services
5. Comparison with the United States
6. Comparison with Japan
7. Conclusions
8. Recommendations

Chapter 8 Electronic contracting

1. Historic evolution
2. Electronic contracting in the eCommerce Directive
   2.1. Background
   2.2. Electronic contracting under the eCommerce Directive
   2.3. Issues linked to the electronic contracting regime
3. eSignatures
4. E-invoicing
   4.1. Introduction
   4.2. The Electronic Invoicing Directive
   4.3. A moving target
5. E-archiving
   5.1. Introduction
   5.2. E-archiving and EU legislation
   5.3. Requirements
6. Digital evidence
   6.1. Introduction
   6.2. (Non-)existing legal framework
7. Conclusions
8. Recommendations

8.1. Article 5 of the eCommerce Directive
8.2. Article 9.2 of the eCommerce Directive
8.3. Article 10 of the eCommerce Directive
8.4. Article 11 of the eCommerce Directive
8.5. E-invoicing and e-archiving
8.6. Digital evidence
This study was commissioned by the European Commission's Information Society and Media Directorate-General, in response to the invitation to tender OJ 2007/S 202 244659 of 19/10/2007. The study does not, however, express the Commission's official views. The views expressed and all recommendations made are those of the authors.
1. **Introduction**

In 1999, eBay acquired Billpoint, an electronic payment service which could reduce the time required for eBay members to complete a transaction with several days. Billpoint was to become the “master merchant” for processing member transactions\(^1\). However, the service failed substantially, due to its poor business plan, hostility from eBay sellers and competition from PayPal.

Billpoint's failure was an illustration of the apparent lack of a market for e-payment systems. Oddly enough, the overwhelming majority of commercial transactions facilitated by the Internet use a conventional payment system. Even in 2002, shoppers made at least 80% of Internet purchases with credit cards. The early days of the Internet heralded a variety of proposals for entirely new payment systems—generically described as electronic money—that would use wholly electronic tokens that consumers could issue, transfer, and redeem.

But years later, no electronic-money system (other than PayPal) has gained a significant role in commerce – even the most famous of the electronic-money providers, DigiCash, eventually filed for bankruptcy. Those that exist, only make up for a tiny fraction of money being circulated.

This chapter will therefore assess the impediments for a further development and improvement of the e-money payment system caused by EU e-money legislation, taking into account the new eMoney Directive, adopted on 16 September 2009.

2. **High-level overview of e-payments**

2.1. **Why is there a need?**

**Dominance of credit cards** – The introduction of e-money led some to believe that conventional cash would be to an important extent replaced by e-money, so that society would become "moneyless" in the distant future\(^2\). However, against expectations, the use of traditional payment systems for online purchases still prevails over the use of online payment systems. Online purchases in Europe are being dominated by payment methods which are also customary in the offline world, such as credit cards\(^3\).

Whereas credit cards were originally developed for payments made in the context of a direct physical interaction between buyer and seller at the point of sale, they were also increasingly used for remote payments, such as transactions via telephone. Credit cards maintained their popularity for remote payments when the widespread introduction of the Internet entailed remote online shopping\(^4\).

---

\(^1\) T. CLARK, "eBay acquires two firms", CNET News, May 1999  
Nevertheless, the use of traditional payment methods in an online context seems to have reached its limits, particularly due to the high transaction costs and the security risks. For example, the transaction costs relating to payments of less than 10 EUR for multimedia content cannot be recovered if such payments are made by credit card.  

**Arrival of e-money** – Together with the rise of the Internet, several promising new payment techniques, including e-money, were developed to deal with the specificities of an online context. However, e-money continues to play a very limited role in the online payment sector in the EU. Despite a gradual increase in the period 2005–2007, the total amount of electronic money in circulation remains less than 1%. Expressed in enterprise turnover, e-money only accounts for 4.2% of all EU enterprise turnover. Only a limited number of electronic money issuers (20) have been created in the European Union, although 127 waivers were also granted.  

Besides the main issue of the legal hurdles imposed by the eMoney Directive, the limited penetration of e-money also results (although to a lesser extent) from technical and psychological barriers. E-money systems are often not interoperable, nor standardised. In addition, they cannot always guarantee the security of transaction, nor the anonymity of its users. Consequently, e-money schemes suffer from a lack of market confidence, and although a market for e-money payments does exist within the EU, it is of limited importance.  

**Mobile payment** – Another example of new payment techniques are mobile payment services (e.g., payment by cell phone), which have the advantage that they can be easily used in both an online and an offline context, enhancing their accessibility. Indeed, mobile devices can be carried around permanently and are personalised and designed to be connected. Moreover, the use of mobile devices is widely diffused in Europe, even more so than the use of computers and Internet.  

In the late 1990s and early 2000s, hundreds of mobile payment systems were being introduced worldwide. Even after the burst of the Internet hype, mobile payment services remained a hot topic. However, many mobile payment systems failed to reach their potential in the EU, due to their inability to attract customers, merchants and banks. Their limited success was partly caused by the fact that mobile technologies were not sufficiently mature and not easy to use. In addition, mobile payment services

---

5 S. HENG, o.c., p. 2  
7 Impact assessment, o.c., p. 7  
8 The most important one, PayPal, has adopted the status of a credit institution.  
9 Impact assessment, o.c., p. 10  
10 Impact assessment, o.c., p. 6  
11 Whereas cash is anonymous, certain types of e-payments require at least to counterparts which both have knowledge as to what goods are services are being purchased, namely the seller and the financial institution effecting the payment.  
13 Ibid., p. 10  
14 European Central Bank, E-payments without frontiers, o.c., p. 18  
16 Ibid., p. 2
were subject to a vague and unclear legal framework. In Japan, on the other hand, mobile payments have gained large adoption, and are still increasing in user base.

New technologies for mobile payments, including contactless vending and ticketing and RFID, now seem to stimulate a renewed interest in mobile payment services\(^\text{17}\). However, given the lack of standards and the immaturity of the market, it is doubtful whether these services will now be more successful. Financial institutions and mobile operators are trying to overcome these issues by launching isolated initiatives to respond to current specific market needs\(^\text{18}\).

2.2. **Requirements for successful electronic payment systems**

**Critical mass** – The success of a payment scheme depends on the number of users, both as regards merchants and consumers, as financial institutions. Especially merchants play a crucial role in the development of payment schemes, as their acceptance of e-payment systems creates the market for such schemes. Providers face the so-called "chicken and egg" problem, as merchant acceptance equally depends on customer acceptance\(^\text{19}\).

**Adoption at the EU-level** – In order to foster cross-border payments in the Internal Market, it is essential that payment schemes are developed that apply across the EU. Merely national payment schemes will not increase cross-border e-shopping, because foreign customers cannot pay abroad with these national schemes. Payment schemes that are limited to the national level, should at least try to enter into cross-national associations to gain customer and merchant recognition.

**Limited costs** – The cost of using an electronic payment system should be limited to a minimum, so as to increase merchant and customer acceptance. This particularly holds true for low-value transactions, which must be facilitated by low transaction costs. (For example, the online purchase of a ringtone of 1 EUR should not result in the need to pay an additional 0,40 EUR for transaction costs.)

**User friendly / low effort** – Electronic payment systems should be user-friendly and should allow users to personalise the system to integrate their every day activities and personal financials. Simplicity is key to gaining wide acceptance, especially to persuade new Internet users who lack both experience and confidence to cope with complicated protocols\(^\text{20}\).

In Japan, for example, most electronic payment systems only require the user to enter a unique set of 16 digits for authentication and payment finalisation purposes.

**Speed** – Electronic payment systems should be able to process transactions very rapidly. Their speed allows them to be differentiated from other (offline) payment schemes such as credit cards, which are often subject to transaction terms of several days. Settlement of transactions in real time allows customers to be informed of their available funds at any moment.

**Security** – Fraudulent payment card transactions represent losses of roughly 1 billion EUR per year in the SEPA area\(^\text{21}\). Moreover, given their virtual nature, e-payment schemes do not allow to see the money physically represented, which often results in the feeling of having no control\(^\text{22}\). It is therefore essential

\(^\text{17}\) Ibid.

\(^\text{18}\) Ibid., p. 10

\(^\text{19}\) European Central Bank, *E-payments without frontiers*, o.c., p. 24

\(^\text{20}\) R. GUTTMANN, *Cybercash - the coming era of electronic money*, 2003, p. 89


\(^\text{22}\) Ibid., p. 94
that e-payment systems provide a sufficient level of security, both on a technological level as on a psychological level.

**Balance of interests** – The current financial crisis has demonstrated the importance of controlling financial institutions. Payment instruments which transfer substantial amounts of money, should be strictly regulated, regardless of the fact whether they constitute online or offline payment systems. However, there also is a need for balance. Strict compliance requirements could cripple the further development of e-payment systems, particularly if small money transfer would also be subject to such requirements. Hence, a balance between innovation incentives and the protection of consumers is required.

**Protection of privacy** – As is possible with cash payments, consumers will want to have at least the option of remaining anonymous in relation to e-payments. Moreover, the possibilities of profiling based on financial transaction data should be limited. For example, the use of transaction-related data outside the initial business context, of the sale of such data to third parties could lead to customer discrimination. Such practices should therefore be contained by legal privacy provisions.

**Transparency** – Electronic payment schemes must be transparent to consumers, in particular with respect to their personal financial data being handled by both merchants and financial institutions. Transparency requires merchants and financial institutions to describe the way in which an electronic payment system works, and how they intend to process any transactions requested by consumers.

**Predictability** – For adapted legal rules to be effective, it is required that e-payment systems are generally intelligible, clear and predictable to all actors involved. Any laws applicable to e-payment systems must therefore clearly establish which services do and which do not fall within their scope.

**Trust** – Both the electronic payment schemes themselves and the applicable legal framework must present a trustworthy system. Customers and merchants will refrain from using such payment schemes if the applicable laws cannot guarantee the protection of their interests. Equally important is the need to address the issue of perceived trust: the public must be convinced that cybercash is unforgeable.

**Reliability** – The legal framework applicable to electronic payments must be consistent in its effects on all participants. In case of a dispute, the application of such laws should be predictable, and the expected outcome of the dispute should be reliable.

### 3. Legal instruments

#### 3.1. Previous eMoney Directive

**3.1.1. Background to the Directive**

The emergence of e-money on the European market occurred in the non-financial sector. Non-bank companies were the first to issue pre-paid payment cards. The previous eMoney Directive represented

---

23 R. GUTTMAN, o.c., p. 87
24 European Central Bank, *E-payments without frontiers*, o.c., p. 34
a response to the emergence of these new pre-paid electronic payment products. The legislative process preceding the adoption of the previous eMoney Directive lasted over two years, especially due to the intensive interaction between the Commission and the European Central Bank (ECB) with respect to some key issues.

The Commission focused on competition issues and found it “necessary to coordinate and harmonise Member States’ laws.” The Commission also found it important to create a legal framework that would allow further innovation, and found it “desirable to provide a regulatory framework that assists electronic money in delivering its full potential benefits and that avoids hampering technological innovation in particular.”

The ECB maintained a different approach, however. The ECB was of the opinion that the legal framework should, amongst other things, ensure the protection of customers, merchants, guarantee the stability of financial markets, protect participants against criminal abuse and avoid market failures.

Caught between the cautious approach of the ECB and the more liberal stance of the European Commission, which placed greater emphasis on innovation and competition, the eMoney Directive became a compromise. The previous eMoney Directive intended to create a clear legal framework designed to strengthen the Internal Market and stimulate competition, whilst at the same time ensuring an adequate level of prudential supervision.

3.1.2. Most important issues under the previous eMoney Directive

The previous eMoney Directive was adopted in response to the emergence of new categories of pre-paid payment instruments, in the context of the rapid changes in the business environment linked to the information technology revolution. Despite the Commission’s intention to create a legal framework that would allow and enhance technological innovation, an evaluation of the application of the Directive shows that it rather impedes the further development of e-payment techniques. As a result, in most of the Member States, e-money is not a credible alternative to cash.

For example, with respect to mobile payments, Commissioner Reding declared in a recent speech: “Today, the lack of common EU-wide standards and rules for "m-cash" leaves the great potential of "m-commerce" and the mobile web unexploited. We have more than 500 million mobile users in Europe.

---

30 Ibid.
32 P. ATHANASSIOU and N. MAS-GUIX, o.c., p. 16
This section 3.1.2 provides a summary of the most important issues under the previous eMoney Directive. A detailed overview of all issues can be found in the Commission's Staff Working Document on the Review of the E-Money Directive\textsuperscript{36} and its Final Report on the Evaluation of the E-Money Directive\textsuperscript{37}.

1. The first problem relates to the unclear definition of electronic money and the scope of the Directive, which generates legal uncertainty and hinders the development of the market. The definition of electronic money is so unfettered that it was predestined to foster divergent interpretations of what is a key determinant of the eMoney Directive's applicability\textsuperscript{38}.

The definition of "electronic money" included in article 1.3(b) of the previous eMoney Directive sets forth three criteria to determine whether or not a product constitutes e-money:

- stored on an electronic device;
- issued on receipt of funds of an amount not less in value than the monetary value issued; and
- accepted as means of payment by undertakings other than the issuer.

As regards the first criterion (storage on an electronic device), the previous Directive intended to include a technology-neutral definition, which would avoid the need to constantly revise the directive to keep pace with technological changes. However, since the Directive's adoption, new business models were developed for which it is uncertain whether they fall within the scope of the Directive, such as mobile telephone prepaid payment cards, retail customer 'loyalty cards', re-loadable or one-off voucher-type electronic cards and employee-scheme electronic cards\textsuperscript{39}. In addition, the reference to "electronic device" raises the question whether this would include server-based e-money\textsuperscript{40}.

The second criterion (receipt of funds) has raised concerns that the inclusion of this criterion could constitute a potential loophole, as schemes issuing e-money at a discount would fall outside the scope of the definition. Several Member States have modified this criterion, so as to avoid that the issuance of e-money at a discount would not be subject to the Directive. For example, Ireland included an explicit prohibition on issuing e-money at a discount\textsuperscript{41}.

The legitimate purpose of the third criterion ("accepted as means of payment by undertakings other than the issuer") is to demarcate e-money products from payment instruments accepted by their issuer only. Nonetheless, it has been identified correctly by the Commission in its Staff Working Document as the criterion which is most open to misinterpretation\textsuperscript{42}. The question arises which number of entities is

\textsuperscript{35} V. REDING, EU Commissioner for Telecoms and Media Digital Europe - Europe's Fast Track to Economic Recovery, The Ludwig Erhard Lecture 2009 Lisbon Council, Brussels, 9 July 2009


\textsuperscript{38} P. ATHANASSIOU and N. MAS-GUIX, o.c., p. 19

\textsuperscript{39} \textit{Ibid.}, p. 18-19

\textsuperscript{40} Commission Staff Working Document on the Review of the E-money Directive, o.c., p. 11

\textsuperscript{41} Final Report on the Evaluation of the E-money Directive, o.c., p. 48

\textsuperscript{42} Commission Staff Working Document on the Review of the E-money Directive, o.c., p. 12
required to accept the e-money, and what sort of relationship needs to exist between issuer and accepting merchants.\textsuperscript{43}

2. The second problem relates to an inconsistent legal framework with a disproportionate prudential regime. To counterbalance the less cumbersome features of the prudential supervisory regime applying to e-money institutions, e-money issuers are subject to more stringent provisions than those applying to other credit institutions, notably as regards restrictions on the business activities they may carry on and, particularly, prudent limitations of their investments aimed at ensuring that their financial liabilities related to outstanding electronic money are backed at all times by sufficiently liquid low risk assets.\textsuperscript{44}

Whereas some cases of failure of e-money institutions occurred, none of them appeared to have impacted any consumers detrimentally. A strong body of opinion therefore finds that the abovementioned stringent rules are disproportionate to the risks.\textsuperscript{45}

3. The third problem relates to inconsistent waivers and passporting procedures. Article 8 of the previous eMoney Directive gave Member States the possibility to allow their competent authorities to exclude the application of the Directive to certain small businesses and to institutions of which the e-money is only accepted by affiliates or by a small number of companies. Article 8 further provides that e-money institutions which have been granted such waiver, cannot benefit from the mutual recognition procedures.

The waiver possibility included in article 8 leaves room for appreciation and therefore creates legal uncertainty. Again, the question arises which exact number of entities is required to accept the e-money, and precisely what sort of relationship needs to exist between issuer and accepting merchants, for an institution to qualify for a waiver.\textsuperscript{46}

In addition, substantial differences exist in the implementation of the waiver provision by the different Member States. Several Member States did not implement the provision at all, while others limited the implementation to some criteria included in article 8. Some Member States even imposed additional conditions. Among those Member States that have implemented article 8, important divergences exist between the application process for a waiver and the "waivable" provisions.\textsuperscript{47}

Whereas the Commission intended to create a legal framework that would enhance competition,\textsuperscript{48} evidence suggests that the inconsistent application with respect to waivers between Member States creates competitive distortions within national borders.\textsuperscript{49}

4. It is problematic for e-money institutions to be profitable, since article 1.5 of the previous eMoney Directive strictly limits the type of activities e-money institutions may perform. In addition to issuing e-money, these institutions may only provide closely related financial and non-financial services, and the storing of data on the electronic device. The issuance of e-money at a premium is thus, practically, the only source of return for e-money issuers.\textsuperscript{50}

\textsuperscript{43} P. ATHANASSIOU and N. MAS-GUIX, o.c., p. 22
\textsuperscript{44} Recital 12 of the previous eMoney Directive
\textsuperscript{45} Commission Staff Working Document on the Review of the E-money Directive, o.c., p. 5
\textsuperscript{46} See also third element of the definition of "electronic money"
\textsuperscript{48} See section 3.1.1 on p. 6
\textsuperscript{49} Commission Staff Working Document on the Review of the E-money Directive, o.c., p. 6
\textsuperscript{50} P. ATHANASSIOU and N. MAS-GUIX, o.c., p. 27
Consequently, e-money institutions mostly gain their profits from transaction fees. Only by charging transaction fees to merchants and/or consumers, e-money institutions can be profitable. A second consequence of the restriction of activities is the need for so-called "hybrid" companies to split up their activities into separate legal entities. This often constitutes a very costly and inefficient process.

3.2. New eMoney Directive

3.2.1. Overview

The new eMoney Directive\(^{51}\) has been adopted on 16 September 2009, and Member States are required to implement the Directive by 30 April 2011.

In its proposal for the new Directive, the Commission recognised the shortcomings of the previous Directive. The Commission found that e-money is still far from delivering its full potential benefits, and that some provisions of the previous eMoney Directive seem to have hindered the take-up of the e-money market. The Commission therefore proposed to focus on modernising the eMoney Directive\(^{52}\).

3.2.2. Issues addressed

The text of the new eMoney Directive indeed addresses several of the issues under the previous eMoney Directive.

1. The new Directive has **clarified the scope** of the Directive. Article 1.5 of the new Directive provides that it shall not apply to the situations described in article 3(l) of the Payment Services Directive, which states that it "shall not apply to services based on any telecommunication, digital or information technology (IT) device, where the goods or services purchased are delivered to and are to be used through a telecommunication, digital or IT device, provided that the telecommunication, digital or IT operator does not act only as an intermediary between the payment service user and the supplier of the goods and services".

It was further clarified by the first reading of the European Parliament that this exception envisages "the situation where a mobile phone or other digital network subscriber pays the network operator directly and there is neither a direct payment relationship nor a direct debtor-creditor relationship between the network subscriber and any third-party supplier of goods or services delivered as part of the transaction"\(^{53}\).

As indicated by article 1.5 of the new Directive, the same exception – which describes the negative scope of the Directive – has been included in identical wording in article 3(l) of the Payment Services Directive. Consequently, payments relating to the purchase of digital services such as ring tones, music or digital newspapers which are sent to a mobile phone (or some other digital device e.g. a computer) are not covered by the new eMoney Directive and the Payment Services Directive when the telecom provider does not act as a mere intermediary\(^{54}\).

---


The scope of the new Directive is further clarified by the exception included in article 1.4, which provides that it shall not apply to the situation set out in article 3(k) of the Payment Services Directive. Accordingly, the new Directive "shall not apply to services based on instruments that can be used to acquire goods or services only in the premises used by the issuer or under commercial agreement with the issuer, either within a limited network of service providers or for a limited range of goods or services".

This additional exception clarifies to a certain extent the third element of the e-money definition under the previous eMoney Directive: "accepted as means of payment by undertakings other than the issuer". The new eMoney Directive gives a hint as to the number of undertakings required ("a limited network"), and the required relationship between the issuer and such undertakings ("under commercial agreement") to fall outside its scope.

2. The new eMoney Directive also acknowledges the need to clarify the application of redeemability requirements. In its proposal for the new Directive, the Commission stated that consumers should have the right to redeem funds at all times\(^{55}\). Article 11.3 of the new Directive now provides that the contract between issuers and electronic money holders must clearly and prominently state the conditions of redemption, including any fees relating thereto. The electronic money holder must be informed of these conditions before being bound by any contract or offer.

Articles 11.4 and 11.7 of the new Directive further specify that redemption of a consumer may only be subject to a fee, if stated so in the contract between the issuer and the consumer, and only in one of the following cases:

- redemption is requested before termination of the contract;
- the contract provides a termination date and the consumer terminates the contract prior to that date; or
- redemption is requested more than one year after the date of termination of the contract.

3. Article 6 of the new eMoney Directive extends the possibility to deploy other activities for e-money institutions. In addition to the provision of payment services, operation of payment systems, granting of credit and the provision of closely related services, e-money institutions may also pursue business activities other than the issuance of e-money, having regard to applicable Community and national law. This possibility to perform additional activities is subject to the requirement of safeguarding any deposited money.

4. Finally, the new eMoney Directive further clarifies the prudential rules. The Commission found the previous prudential rules to be excessive with regard to the risk of the activity. The initial capital requirement has been lowered from 1 million EUR to 350 000 EUR\(^{56}\), and the ongoing capital requirements have been replaced with new methods of calculation, based on the nature and the risk profile of e-money institutions\(^{57}\).

3.2.3. Evaluation

The new eMoney Directive seems to resolve a number of important issues under the previous eMoney Directive. Nonetheless, the question arises whether all issues have been resolved, especially with respect to the scope exceptions included in the Directive. (Note: as these exceptions are also included in

\(^{55}\) Article 5 of the Commission Proposal for a new E-money Directive

\(^{56}\) Article 4 new E-money Directive

\(^{57}\) Article 5 new E-money Directive
Limited network of service providers – Article 1.4 of the new eMoney Directive and article 3(k) of the Payment Services Directive hold that the Directives shall not apply to services based on instruments that can be used to acquire goods or services only in the premises used by the issuer or under commercial agreement with the issuer, either within a limited network of service providers or for a limited range of goods or services. Recital 5 adds that "An instrument should be considered to be used within such a limited network if it can be used only either for the purchase of goods and services in a specific store or chain of stores, or for a limited range of goods or services, regardless of geographical location of the point of sale. Such instruments could include store cards, petrol cards, membership cards, public transport cards, meal vouchers or vouchers for services (such as vouchers for childcare, or vouchers for social or services schemes which subsidise the employment of staff to carry out household tasks such as cleaning, ironing or gardening), which are sometimes subject to a specific tax or labour legal framework designed to promote the use of such instruments to meet the objectives laid down in social legislation."

However, the criteria for what constitutes a "limited" network are still not entirely clear. The questions arises which number of service providers exceeds the threshold for being qualified as a "limited" network (four service providers, five or thirty-five?). A similar question arises with respect to a "limited" range of goods or services. For example, does a payment instrument which allows to pay for any type of software constitute a limited range of goods or services? As the preparatory works of the Directives provide little or no guidance for the interpretation of the concept "limited", a clarification will need to be provided by case-law.

It is also unclear what exactly is meant by a "commercial agreement with the issuer". The question arises whether a mere formal agreement is sufficient to fall within the scope of this exception, or whether a certain balanced content of such agreement is required.

Value added services – Article 1.5 of the new eMoney Directive and article 3(l) of the Payment Services Directive provide that the Directives shall not apply to services based on any telecommunication, digital or IT device, where the goods or services purchased are delivered to and are to be used through a telecommunication, digital or IT device, provided that the telecommunication, digital or IT operator does not act only as an intermediary between the payment service user and the supplier of the goods and services.

This exception is particularly vague, but seems primarily intended to allow telecom providers to sell ringtones, wallpapers, games and similar content for cell phones, without becoming subject to the requirements of the E-money or Payment Services Directive. However, the broad wording ("any telecommunication, digital or IT device") and limited conditions for the exception to apply (it suffices that the provider does not act only as an intermediary), seem to entail that this exception also applies to other services. It appears that the only requirement is that the supplier provides additional services, beyond the payment service. The question is, however, as from which moment a provider becomes more than a mere intermediary. Is it sufficient to offer a "web portal" or search engine through which customers can select products or services? Is it sufficient for a network operator to install a customer complaint line, through which customers can cancel a transaction? Both cases illustrate that, due to the sheer lack of guidance in this regard, case law will likely diverge between Member States.

It is therefore likely that this provision creates a loophole for numerous service providers, and vagueness for many other service providers. For example, several new e-shops for smartphones have been
launched during the previous months, such as the Apple iTunes shop for iPhone\textsuperscript{58}. The service providers of these e-shops do not act only as financial intermediaries, but also provide software back-ups, selection tools, user reviews and ratings, digital shop windows, etc. Consequently, these service providers could fall within the exception of article 1.5 the new eMoney Directive and article 3(l) of the Payment Services Directive. This new type of e-shop is increasingly popular, is starting to become a "platform" which acts as a central hub between consumers and content providers, and consumers often deposit and store large amounts of money in their online accounts for these e-shops. Whereas it could be acceptable to subject this type of service providers to a waiver regime when only small amounts are stored in each account, it should be avoided that they completely fall outside the scope of the Directives. Further, both with respect to the exception relating to limited networks and the exception regarding value added services, it is unclear whether money used in virtual worlds and online platforms (such as the hi5 coins system and the Nintendo Wii Points Card) falls within the scope of the exception. A more detailed analysis is set out in sections 4.4 and 4.7.

**Mobile payments** – As discussed above, it is not clear to which extent mobile payments relating to the purchase of ringtones, wallpapers, games and similar content for cell phones from telecom providers, fall within the scope of the new eMoney Directive.

On the other hand, similar types of typical mobile payments, such as the purchase of parking tickets or public transportation tickets via SMS, will be subject to the provisions of the eMoney Directive\textsuperscript{59}. Contrary to mobile payments relating to ringtones and similar content, such payments cannot fall within the scope of the value added services exception, since they do not relate to goods or services purchased which are to be used through a telecommunication, digital or IT device.

Accordingly, telecom operators issuing prepaid cards which can be used for such payments, will be considered as issuers of e-money, and hence, will need to comply with the eMoney Directive. This entails that telecom operators are, \textit{inter alia}, subject to the limitation to deploy other activities, and are thus often forced to establish a separate entity for the purposes of issuing prepaid cards.

**Waivers** – As is the case for the previous eMoney Directive, waivers will only apply on a Member State level under the new eMoney Directive. Furthermore, waivers do not exempt payment providers from all obligations of the eMoney Directive (national supervising authorities can decide which prudential rules, capital requirements, fund requirements and safeguarding requirements do not apply to a particular e-payment provider).

While waivers significantly reduce the administrative and regulatory burden for new e-payment providers, they do not reduce this burden entirely, as e-payment providers must still prepare and submit files to the national supervisory authority, must initiate discussions with the supervising authority, and possibly change some aspects of its intended payment scheme due to recommendations of the authority. While this is still manageable on a national level, it becomes prohibitive when the waiver must be requested in many Member States.

---

\textbf{Practical example: anonymous e-payment cards.} A Belgian start-up company was looking to enter the market of e-payments with an innovative, user-friendly e-payment scheme. The scheme would allow for anonymous online payments, by allowing customers to buy pre-paid scratch cards in local shops (e.g., a supermarket). The special code on the scratch card would then be entered into an online account, through which online payments can be made to affiliated online merchants.

\textsuperscript{58} Other examples include Google Android Market, BlackBerry App World, Nokia Ovi shop, Java shop as announced by Sun and Microsoft app store.

\textsuperscript{59} to the extent made with prepaid cards
The company spent over 80,000 EUR in legal fees, of which over 50,000 EUR was spent on preparing the waiver and investigating the costs and benefits of a full e-money license (eventually a waiver for Belgium was obtained). An important part of the remaining 30,000 EUR was spent on other regulatory issues (including consumer protection issues), to which any company dealing with sensitive products and services is generally subject.

These costs were, obviously, almost prohibitive to a new start-up, for which the cash flow in the start-up phase is problematic due to a "chicken-and-egg" problem of attracting at the same time sufficient customers and merchants.

Considering the crucial importance of having EU-level waivers, we are of the opinion that a second waiver scheme must be introduced, in addition to – or as a replacement of – the current optional, national waiver scheme set forth in article 10. This waiver scheme would apply on an EU-level, and would consist of a mere notification duty (similar to the notification duty for internet access providers60), whereby e-payment providers would be exempted from all financial regulations in the Payment Services Directive and eMoney Directive. However, in order to strike balance with consumer interests, this waiver scheme would only apply when the individual account held by each user, stores a maximum value of 150 EUR.

3.3. Payment Services Directive

3.3.1. Overview

The Payment Services Directive61 intends to establish a modern and harmonised legal framework to enable payments to be made more quickly and easily throughout the whole EU62. The Payment Services Directive constitutes an attempt to remove legal obstacles for the creation of a Single Payments Market, so as to enhance payment system competition and the creation of economies of scale. The Directive further intends to boost consumer confidence in payment systems such as electronic payments63. As is the case with the eMoney Directive, the Payment Services Directive intends to achieve a balance between consumer protection and market liberalization64.

3.3.2. Relation to e-money

In its Staff Working Document on the review of the eMoney Directive, the Commission acknowledged the need to ensure consistency between the eMoney Directive and the Payment Services Directive65. Considering the direct linkages between these two legal acts, and bearing in mind the undesirability of a

---

60 Article 3 of Directive 2002/20 on the authorisation of electronic networks and services provides that Member States may require internet access providers to submit a notification prior to beginning their activities.
64 Ibid., p. 177
proliferation of directives dealing with similar or overlapping issues (namely, payment services), it is a lost opportunity that the new eMoney Directive was not incorporated in the Payment Services Directive. Even so, it should be noted that the new eMoney Directive is clearly drafted to complement the Payment Services Directive, and to exclude any contradictions and overlapping issues between both directives.

3.3.3. "Payment institutions"

The Payment Services Directive introduces a new category of service providers which are subject to a different prudential regime than e-money institutions and credit institutions, namely the payment institutions. Payment institutions are legal persons that have been granted authorisation to operate in accordance with Article 10 of the Payment Services Directive, and which execute payment services.

A list of services which are considered as "payment services" has been included in an Annex to the Directive, and includes, inter alia, services enabling cash to be placed and to be withdrawn from a payment account, the execution of payment transactions and money remittance. Payment institutions cannot use the funds received from payment service users and specifically accepted in connection with a payment service to support other business activities other than payment services.

This new category was introduced to remove legal barriers to market entry and to establish a single license for all providers of payments services which are not connected to taking deposits or issuing e-money. The general underlying purpose of the introduction of this category is to remove the black economy by registering the identity and whereabouts of all persons providing payment services.

4. Types and modalities of electronic payments

This section assesses the legal issues under the new eMoney Directive and the Payment Services Directive with respect to electronic payment schemes frequently used in today's society, as well as an assessment of several modalities of e-payments.

4.1. Smart cards

4.1.1. Overview

A first type of e-money consists of so-called "electronic purses" in the form of smart cards. These cards resemble other types of plastic money, except that they have an electronic microchip embedded in a small gold plate in front of the card rather than a magnetic strip in the back. Smart cards for e-payments use the microchip to store a certain amount of value by use of encryption algorithms that can only be decoded by an adequate reader.

---

66 P. ATHANASSIOU and N. MAS-GUIX, o.c., p. 37
67 S. MERCADO-KIERKEGAARD, o.c., p. 181
68 Ibid., p. 180
69 Ibid., p. 181
70 R. GUTTMAN, o.c., p. 112
These card-based e-purses are generally intended for small payments. They allow the payment of exact amounts at unstaffed locations such as vending, parking and ticketing machines. Smart cards can also be used for online purchases if the consumer has a card reader attached to their computer. This card reader will unlock the value in the card and send the information to the online retailer, facilitating an anonymous e-commerce transaction.

The smart-card-based electronic wallet is known as Proton in Belgium, as Avant in Finland, Danmont in Denmark, Chipknip in the Netherlands, MEP in Portugal, Minipay in Italy, Minicash in Luxembourg, Moneo in France, Monedero 4B in Spain and GeldKarte in Germany. Whereas smart cards have been relatively successful in the Benelux countries, the take-up in most other European countries has been slow.

4.1.2. Legal assessment

There never seems to have been any doubt or dispute as to whether smart cards constitute e-money under the previous eMoney Directive. The modifications brought by the new eMoney Directive do not entail any additional terms or conditions that would change this situation.

Smart card providers often benefit from a waiver granted by their national authority under article 8 of the previous eMoney Directive. For example, the e-money institutions operating under a waiver in Germany include a smartcard scheme in a sports stadium.

4.2. Server based e-money

4.2.1. Overview

Server based e-money was developed almost simultaneously with the rise of card-based e-money, driven by the opportunities offered by the Internet. The most successful server based e-money systems consist of pre-funded personalised payment schemes, involving the transfer of funds stored on a personalised online account, similar to bank deposits. Server based money can be accessed via websites, e-mail or SMS. The innovative nature of these schemes lies in the fact that accounts can be opened and money can be sent by simple use of e-mail addresses or mobile phone numbers.

The most well-known and successful example of server based e-money is PayPal, an online payment system launched in the US in 1999. The main reason for its success lies in the fact that it suffices for online vendors to have an e-mail address and a PayPal account in order to receive payments; it excludes a complex credit card processing system as a prerequisite for online trading. Also, the PayPal system does not require consumers to transfer their credit card number to unknown vendors, as PayPal acts as a secure third party facilitating the payment.

---

73 A. GUADAMUZ, o.c., p. 3
74 S. HENG, o.c., p. 6
75 European Central Bank, E-payments without frontiers, o.c., p. 49
77 Ibid., p. 29
78 Ibid.
79 European Central Bank, E-payments without frontiers, o.c., p. 48
4.2.2. **Legal assessment**

The previous eMoney Directive was very unclear as to whether server based e-money falls within its scope. In the new eMoney Directive, the Commission clarified that "the definition [of electronic money] should cover electronic money which is (...) stored remotely at a server and managed by the holder through a payment account with the payment service provider." The new definition of e-money now provides that e-money is "stored electronically", hence clarifying that server based e-money falls within the scope of the new eMoney Directive.

Server based e-money may fail to meet the requirement of security, which was identified as an essential requirement for the success of electronic payment schemes. Although account based systems such as PayPal cannot be hacked in the same way as smart card technology, they do suffer from other security threats, for example, a type of online fraud known as "phishing".

4.3. **Disposable and virtual pre-funded cards**

4.3.1. **Overview**

Disposable and virtual pre-funded cards are a type of server based e-money which physically appear in the form of a card. Contrary to smart cards, the deposited funds are not stored on the card itself, but on a server. They typically imply a transfer of centrally stored anonymous claims that have been purchased in advance. These cards are often issued as scratch cards with a hidden identifying number, or sent as virtual cards via SMS. The received number must be entered into the issuer's website to activate the anonymous "card account", or can be used directly for paying at a content provider's website.

These disposable and virtual pre-funded cards typically target individuals that do not possess debit or credit cards (such as minors) and persons who wish to remain anonymous when making online purchases. Accordingly, they are being used increasingly in niche markets such as online entertainment, including gaming and adult entertainment.

Examples include PaySafeCard in Austria and Germany and SNAP Card and SplashPlastic in UK.

4.3.2. **Legal assessment**

This type of cards addresses the essential requirement of privacy and allows consumers to make anonymous purchases. As a form of server based e-money, these disposable and virtual pre-funded cards fall within the scope of the new eMoney Directive.

---

81 See Chapter 11 - Cybercrime
82 European Central Bank, *E-payments without frontiers*, o.c., p. 48
86 See section 4.2.2
4.4. **Platform payment systems**

4.4.1. **Overview**

“Platform payment systems” concern payment systems and virtual wallets created by online platform operators, which allow users of the platform to purchase various goods, usually (but not necessarily) related to the platform itself.

For example, social communities often allow their users to store money on their user accounts, in order to purchase digital services related to the community (e.g., tokens to buy applications to be displayed on the user’s home page and tokens to pay for premium places). An example of platform payment systems include the hi5 coins system and the Wii Points Card which can be purchased from local Nintendo retailers or via the Wii Shop.

Shops such as Apple iTunes and the Google Android Market can also be qualified as a type of platform payment systems, as these shops are increasingly becoming a central services hub that connects content providers to content consumers.

4.4.2. **Legal assessment**

The question arises whether such platform payment systems fall within the scope of the new eMoney Directive and the Payment Services Directive, taking into account the scope of the exceptions relating to "limited networks" of service providers and value added services.

**Limited networks exception** – Article 1.4 of the new eMoney Directive and article 3(k) of the Payment Services Directive provide that the Directives shall not apply to services based on instruments that can be used to acquire goods or services only within limited networks or for a limited range of products of services. The question arises whether the network of providers offering their services via a platform constitutes a limited network, similar to a chain of stores.

Similarly, it is unclear whether the limited range of payable services and products offered via such platforms qualify as a limited range of goods or services.

**Value added services exception** – As regards value added services, article 1.5 of the new eMoney Directive and article 3(l) of the Payment Services Directive provide that the Directives shall not apply to service providers that do not merely act as an intermediary. Platform operators generally provide several services other than payment services. It is unclear, however, which criteria should be used to determine whether such services should be considered as additional services within the meaning of the article 1.5 of the new eMoney Directive.

**Receipt of funds** – Also, the definition of e-money as included in article 2.2 of the new eMoney Directive provides that products must be "issued on receipt of funds" to qualify as e-money. Accordingly, platforms that allow collection of credits or points by performing certain activities distinct from the direct purchase of such credits or points, fall outside the scope of EU e-money legislation. The question arises then what is the status of platforms where the same credits or points can be both purchased and earned, since these platforms generally store purchased and earned credits in one user account.

---

87 See section 3.2.3

88 Recital 5 of the Commission Proposal for a new E-money Directive: “An instrument should be considered to be used within a ‘limited network’ if it can be used only for the purchase of goods and services in a specific store, a chain of stores (...) Instruments which can be used for purchases in stores of listed merchants should not be exempted as such instruments are typically designed for a network of service providers which is continuously growing.”
4.5. Mobile payment systems

4.5.1. Overview

A large variety of mobile e-payment schemes have been developed. One can distinguish between schemes that are funded via a prepaid account and schemes that are added to telephone bills ("post paid"). These mobile payment systems can either debit payments from the holder's credit card or from his bank account.

Mobile transactions can also be carried out via e-money schemes. Such e-money can either be integrated into mobile devices, or can be stored on a card or server. Mobile payment schemes are typically popular with minors, to perform purchases of limited value, such as the purchase of ringtones.

Another distinction to be made is between proximity payments and distance payments. The first type of mobile payments allows contactless transmission of the payment order, for example via radio frequency, as is used in public transportation. These represent one of the most important innovations in the banking system, increasing speed, simplicity and convenience when purchasing goods. The distance type of mobile payments usually requires the help of an SMS or automatic voice message.

So far, there is little progress visible on the standardisation and interoperability of payment solutions between mobile network operators in the national markets, and even less at the European level.

4.5.2. Legal assessment

The application of the previous eMoney Directive to prepaid payment services by mobile operators for third party offerings was controversial. In implementing the Directive at national level, some Member States decided that in certain circumstances, by supplying pre-paid phone cards, mobile operators in practice issue electronic money and that therefore they should comply with existing EU rules concerning its issuance. However, other Member States found that mobile operators should not be considered as e-money institutions.

To avoid further impediments to the Internal Market, caused by these divergent interpretations, the Commission carried out an analysis in 2003 so as to establish a common interpretation. According to that analysis, prepaid phone cards are covered by the Directive when the electronic value stored on them is used to purchase products and services offered by third parties (such as ring tones, news, games, CDs, books and ticketing services) rather than directly by the phone companies.

Value added services exception – The new eMoney Directive further clarifies the issue of mobile operators, by introducing an exception relating to value added services. Payments relating to the purchase of digital services such as ringtones or music which are sent to a mobile phone, are not covered by the eMoney Directive, nor by the Payment Services Directive when the telecom operator

---

89 European Central Bank, E-payments without frontiers, o.c., p. 52
90 For example, Oyster in London
92 European Central Bank, E-payments without frontiers, o.c., p. 52
93 Ibid., p. 39
94 EU Press Release, Electronic money: Commission consults on how the E-Money Directive applies to mobile phone services, 10 May 2004, IP/04/620
95 Ibid.
does not act as a mere intermediary. However, as pointed out above, this new exception is highly ambiguous, and promises to introduce a significant level of legal uncertainty.

Security and privacy – Another legal issue is that proximity contactless payments using RFID technology raise several security and privacy related issues. Traditional credit cards require visual access or direct physical contact for retrieving information such as the cardholder’s name and the credit-card number. RFID technology on the other hand makes these and other sensitive data available via radio frequency\textsuperscript{96}.

For example, a study of sample RFID credit cards found that the cardholder's name, card number and expiration are often leaked to unauthenticated readers, and that RFID-enabled credit cards are susceptible to a range of traditional RFID attacks such as skimming and relaying\textsuperscript{97}. In addition to this risk of unauthorised disclosure of personal data, the potential exists for this technology to be used to monitor individuals via the RFID applications they hold\textsuperscript{98}.

Although RFID operators are already subject to the strict security requirements set out in the Data Protection Directive and the consumer protection requirements set out in the Payment Services Directive, the risks created by RFID payment applications illustrate the need for additional standards. In this respect, the Commission recognised that RFID will only be able to deliver its economic and societal benefits if effective measures are in place to safeguard personal data protection and privacy. It therefore recommended that Member States should ensure that operators take appropriate technical and organisational measures to ensure the protection of personal data and privacy\textsuperscript{99}.

4.6. Vouchers and gift cards

4.6.1. Overview

Building on the popularity of frequent-flier miles and coupons, a number of internet start-ups started designing their own online currencies for use as a marketing tool to attract more customers to sites and entice them to shop there\textsuperscript{100}. Similarly, different issuers of paper vouchers and gift cards showed an interest in switching their products to an electronic format\textsuperscript{101}. As such, electronic coupons, vouchers and gift cards emerged, which can be used to purchase products and services from participating merchants.

Electronic vouchers and gift cards are one of the strongest growth markets for prepaid cards, particularly because they allow parents to enable their children to pay for services online without the use of an adult's credit card\textsuperscript{102}. Typical examples of electronic gift cards include the iTunes Gift Card and Amazon Gift Card, which can both be bought online. Vouchers and gift cards are very similar to smart cards and disposable and virtual pre-funded cards. However, they are typically obtained as a present or via a third party other than the issuer. In addition,

\textsuperscript{96} T.S. HEYDT-BENJAMIN et al, Vulnerabilities in First-Generation RFID-enabled Credit Cards, October 2006, p. 2, available at prisms.cs.umass.edu/~kevinfu/papers/RFID-CC-manuscript.pdf
\textsuperscript{97} Ibid.
\textsuperscript{98} Commission Recommendation of 12 May 2009 on the implementation of privacy and data protection principles in applications supported by radio-frequency identification, (C(2009) 3200 final)
\textsuperscript{99} Ibid., p. 3 and 6
\textsuperscript{100} R. GUTTMAN, o.c., p. 124
\textsuperscript{101} Final Report on the Evaluation of the E-money Directive, p. 33
\textsuperscript{102} D. SHANNON, o.c., p. 12
vouchers and gift cards are not always issued on receipt of funds. They may also be acquired by performing certain activities, such as collecting points or bringing in new customers.

4.6.2. Legal assessment

There is considerable legal uncertainty as regards the question whether electronic vouchers and gift cards constitute e-money under the previous eMoney Directive. In principle, they seem to fulfil all criteria of the definition. However, some of their inherent features are incompatible with the Directive, such as the redeemability requirement included in article 3, which provides that "a bearer of electronic money may, during the period of validity, ask the issuer to redeem it at par value in coins and bank notes or by a transfer to an account"\(^{103}\).

Under the new eMoney Directive, vouchers and gift cards will generally not fall within its scope, pursuant to the limited network exception, which exempts "instruments that can be used to acquire goods or services only in the premises used by the issuer or under commercial agreement with the issuer, either within a limited network of service providers or for a limited range of goods or services"\(^{104}\). Vouchers and gift cards can typically only be used for products and services of a limited number of participating merchants.

In its first reading, the European Parliament further clarified that social vouchers — such as vouchers for services such as childcare vouchers, or services voucher schemes which subsidise the employment of staff to carry out household tasks — should not be covered by the Directive. The agreed text of the Directive emphasises that, where such a specific purpose instrument develops into a general purpose instrument, the exemption should no longer apply\(^{105}\).

4.7. Money in virtual worlds

4.7.1. Overview

Similar to platforms such as Netlog and hi5, virtual worlds have created their own currency which allows their users to operate within their world. The most well-known virtual world is Second Life, an online 3D world imagined and created by its residents. Within Second Life, there is a marketplace where residents trade virtual goods and services. The Second Life economy has become one of the world’s largest user-generated virtual economies\(^{106}\).

Transactions within Second Life are based on the Linden dollar, Second Life’s own virtual micro-currency. Residents can buy and sell Linden dollars on LindeX, the official virtual currency exchange of Second Life. Linden dollars may also be freely distributed, at Second Life’s operators’ discretion. It is also interesting to note that the Second Life Terms of Service further clearly state that "Second Life ‘currency’ is (...) not redeemable for monetary value from Linden Lab\(^{107}\)."

---


\(^{104}\) Article 1.4 new eMoney Directive, which refers to article 3(k) of the Payment Services Directive

\(^{105}\) Recital 5 of the Proposal for a new E-money Directive, EP First reading, 24 April 2009

\(^{106}\) See http://secondlife.com/whatis/marketplace.php

\(^{107}\) See http://secondlife.com/corporate/tos.php
4.7.2. Legal assessment

The question arises whether currencies created by virtual worlds, such as the Linden dollars, fall within the scope of the new eMoney Directive. As regards the definition, virtual world currencies seem to comply with all criteria: they are stored electronically, are issued on receipt of funds, for the purpose of making payment transactions, and are accepted by other residents, i.e. natural or legal persons other than the issuer.

**Limited network exception** – It is, however, not clear whether virtual worlds which issue their own money, fall within the scope of the exception set out in article 1.4 of the new eMoney Directive and article 3(k) of the Payment Services Directive. These articles provide that the Directives shall not apply to services based on instruments that can be used to acquire goods or services only in the premises used by the issuer or under commercial agreement with the issuer, either within limited networks or for a limited range of products of services.

Furthermore, it is unclear whether a virtual world can be considered as "premises" in the sense of these articles. Similar to meal vouchers issued by a building owner that can only be used within such building, money issued by virtual worlds can typically only be used within that community.

The question also arises whether the other residents of a virtual world offering their products and services constitute a limited network. Similarly, it is unclear whether the limited range of payable services and products offered via such virtual worlds qualify as a limited range of goods or services.

**Value added services exception** – As regards value added services, article 1.5 of the new eMoney Directive and article 3(l) of the Payment Services Directive provide that the Directive shall not apply to service providers that offer additional services beyond the payment service. The services that are offered by virtual worlds in addition to any payment services, generally constitute services that are delivered to and are to be used through a computer. It is, however, unclear whether virtual worlds therefore fall outside the scope of the new eMoney Directive and Payment Services Directive.

**Receipt of funds** – Finally, the definition of e-money as included in article 2.2 of the new eMoney Directive provides that products must be "issued on receipt of funds" to qualify as e-money. The question arises as to what is the status of money issued by virtual worlds if it is not necessarily and not always issued on receipt of funds.

4.8. Escrow services

4.8.1. Overview

**Issue** – Contrary to point-of-sale transactions, remote transactions imply by definition a time interval between payment and delivery of goods, and hence, create a conflict of interest between buyer and seller. Neither party is interested in transferring its assets (be it money or goods), before receiving the other party's agreed asset. This conflict is especially pertinent in an online context, where the remote nature of transactions is often accompanied by unknown or anonymous trade partners, which aggravates the lack of trust between trade partners.

Online consumer-to-consumer environments in particular pose serious challenges to trust between trade partners. For example, an online auction such as eBay allows its users to remain nearly completely anonymous, which facilitates fraud. Although these platforms often take trust enhancing measures, such as the eBay feedback system, consumers' trust remains very low.
Solution – A solution to the diverging interests of buyers and sellers, be it consumers or merchants, is the use of Trusted Third Parties (TTP) as intermediaries to the transaction. A TTP can overcome the lack of synchronisation of delivery of the goods and payment. Buyers can submit their payment to a TTP, which will only release the payment to the seller upon receiving the buyer’s confirmation of receipt of the goods. Hence, the benefit of TTP intermediaries lies in the reduction of fraud possibilities. However, they also entail increased transaction costs.

An example of a TTP escrow service provider is escrow.com, which is eBay’s approved escrow service. Local escrow service examples include Pay&Deliver in Belgium, PayDutch in the Netherlands and Illoxx in Germany.

4.8.2. Legal assessment

Online escrow services may be subject to the Payment Services Directive, depending on their underlying transaction scheme. If, and to the extent, the TTP operates as a mere escrow agent, its services shall not be considered as payment services. For example, in the Pay&Deliver scheme, the buyer’s payment is transferred to an account which is administered by a third party, legally independent from Pay&Deliver. Hence, the payment is not executed by Pay&Deliver.

However, if the TTP actually effects the payment, such service will be qualified as a payment services as defined in the Payment Services Directive. Consequently, the TTP will be considered as a payment institution, and be subject to the authorisation as set out in the Payment Services Directive.

5. Comparison with the United States

MSB state laws – In the United States, regulation of non-bank financial service providers has been left to state banking regulators. A majority of the U.S. states has laws for so-called money services businesses (MSBs), which are non-banks that provide money services. As regards e-payment intermediaries, states have generally modified their existing regulatory frameworks for MSBs, rather than implementing a new legislative framework to deal with the specificities of e-payments. MSBs (including e-payment providers) operating in the United States, must comply with the laws of each state in which they operate.

UMSA – As these state laws vary considerably in their requirements imposed on MSB’s, the National Conference of Commissioners on Uniform State Laws (NCCUSL) approved the Uniform Money Services Act (UMSA) in 2000.

The UMSA contains a recommended common framework for licensing and regulating MSBs, including e-payment providers, throughout the different states in the United States.

---

108 European Central Bank, E-payments without frontiers, o.c., p. 32
110 NCCUSL, Uniform Money Services Act with prefatory note and comments, p. v, available at www.law.upenn.edu/bll/ulc/moneyserv/ms00ps.htm
111 The NCCUSL is a body of lawyers, judges, and law professors, typically appointed by the governor of each state. Although influential, the NCCUSL does not have any direct legislative power itself; uniform acts become laws only to the extent they are enacted into law by state legislatures.
112 Text available at www.law.upenn.edu/bll/ulc/moneyserv/ms00ps.htm
113 Ibid., p. 324
Stored value – Similar to the EU e-money concept, the UMSA defines "stored value" as monetary value that is evidenced by an electronic record, whereby "monetary value" is a medium of exchange, whether or not redeemable in money\textsuperscript{114}. The comments to the UMSA further state that "medium of exchange" connotes that the value that is being exchanged be accepted by a community, larger than the two parties to the exchange.

The comments to the UMSA further specify that, with Internet payments, the regulators will also have to make the same type of determination as to when a certain type of monetary value has become widely accepted as to constitute a medium of exchange. As regards Internet payment systems that involve Internet scrip or points (\textit{e.g.}, frequent flier or bonus points), it will be up to the state regulators to grapple with how widely circulating such points are, whether they are redeemable, and whether they can be used to purchase or acquire a wide range or products and services.

This definition of stored value is very similar to the definition of e-money under EU laws. In fact, the comments to the UMSA even explicitly refer to the eMoney Directive with respect to stored value. However, other than the eMoney Directive, and as indicated by the definition of monetary value, UMSA does not require stored value to be redeemable.

Money transmission – "Money transmission" is defined as the selling or issuing of payment instruments, stored value, or receiving money or monetary value for transmission (excluding the provision solely of delivery, online or telecommunications services, or network access)\textsuperscript{115}.

The comments to the UMSA clarify that Internet payment services that hold customer funds or monetary value for their own account rather than serve simply as clearing agents, fall within the definition of money transmission. However, entities that simply transfer money between parties as clearing agents fall outside the scope of a safety and soundness statute. The definition also excludes entities that solely provide delivery services (\textit{e.g.}, courier or package delivery services) and entities that act as mere conduits for the transmission of data (such as internet access providers). These exclusions are similar to the exclusion set out in the new eMoney Directive\textsuperscript{116}.

Licensing and prudential supervisory regime – Similar to e-money issuers under EU law, money transmission business must obtain a license prior to commencing their activities\textsuperscript{117}. As in the EU, this license needs to be obtained in each state in which a business operates, as UMSA is implemented on a state level, rather than on the federal level.

Although UMSA does not include any capital requirements, it does provide for a similar prudential supervisory regime as the eMoney Directive. Any business obtaining a license for money transmission, must be able to present a surety bond, letter of credit or other similar security acceptable, in the amount of $50,000, plus $10,000 per location, not exceeding a total of $250,000\textsuperscript{118}. Section 701 UMSA further specifies that money transmitters are required to maintain a certain level of investments that is equal to the value of their outstanding obligations as a means of protecting individual consumers.

\begin{itemize}
\item \textsuperscript{114} Section 102 UMSA
\item \textsuperscript{115} Section 102 UMSA
\item \textsuperscript{116} Which states that it "shall not apply to services based on any telecommunication, digital or information technology (IT) device, where the goods or services purchased are delivered to and are to be used through a telecommunication, digital or IT device, provided that the telecommunication, digital or IT operator does not act only as an intermediary between the payment service user and the supplier of the goods and services"
\item \textsuperscript{117} Section 201 UMSA
\item \textsuperscript{118} Section 203 UMSA
\end{itemize}
6. **Comparison with Japan**

**Overview** – In comparison with the EU, private players are rushing into e-payment systems in Japan. There are currently more than twenty different e-payment providers in Japan, which enjoy significant popularity. This success is attributed to a combination of factors, such as the ease of use, attractive bonus schemes, the possibility to make anonymous payments, and the suitability for small payment transactions.

Due to the relatively large amount of online payment providers, the providers are currently trying to build associations, in order to reduce fragmentation.

**Legal framework** – Japanese financial law makes a distinction between offline and online e-payments. While offline payment providers are currently subject to a prudential regime, online payment providers are not. However, online payment providers will soon also be subject to a prudential regime.

**Evaluation** – While an extensive comparison is beyond the scope of this study, it is important to recognise that – contrary to the EU – the Japanese e-payments market flourished. An important reason is that these e-payment providers were not subject to strict legal rules, and could develop their services without any regulatory burden. Japanese consumers have now adopted e-payment systems for various only payments, and the new regulatory framework will not likely change this situation. The reverse situation applies in the EU, where strict rules were enacted at the moment e-payment providers started to appear on the market.

7. **Conclusions**

1. The European framework for electronic money is rapidly developing. The 2007 Payment Services Directive is being implemented by Member States, and will enter into force in most Member States in November 2009. The previous eMoney Directive has been revised, and the new eMoney Directive has been signed on 16 September 2009. Also, the recent Commission Recommendation regarding RFID technology illustrates that specific legislation relevant for contactless mobile payments is in the making. Given the state of development of all e-payment legislation, it is not yet possible to draw any general decisive conclusions as regards its implementation and application in practice.

2. As recognised by the Commission in its proposal for the new eMoney Directive, the previous e-payment legislation, drafted around the year 2000, contained many legal problems, such as the unclear definition of electronic money, the unclear scope of the Directive, a disproportionate prudential regime, inconsistent waivers and passporting procedures, and difficulties for e-money institutions to be profitable.

3. The revision of the eMoney Directive constitutes a prime example of the authorities' acknowledgment of the need for modernization of its legislation. However, some ambiguities are still not resolved by the new Directive (e.g., the question to which extent a prepaid mobile phone card is e-money when used), and several new ambiguities are introduced (such as the exemption

---

119 customers only need to type in a 16-digit code in order to make a payment — no physical card or other multi-layered security system is used
120 e.g., receiving airmiles when using the e-payment systems
121 e.g., for buying a cell phone ringtone
122 An overview of the transposition of the Payment Services Directive is available at http://ec.europa.eu/internal_market/payments/framework/transposition_en.htm
for e-money used in a "limited network" of service providers, and the exemption for value-added services).

Furthermore, the new eMoney Directive does not fundamentally change the waiver regime, which still does not apply on a European level, and does not exempt the e-payment provider from all regulatory compliance issues. These waivers are still too burdensome in many cases: the exemption must be applied for on a national basis, and generally involve extensive administrative overhead for the e-payment provider.

4. As a result, the legal treatment of several types of e-payment services (particularly platform payment systems and mobile payment systems) is not clear. Interestingly, precisely these types of e-payment services seem to be the future of online payments.

5. We are therefore of the opinion that the improvements brought by the new eMoney Directive will not be sufficient to trigger an uptake of the e-payments market, and that a more fundamental revision of the eMoney Directive is necessary.

8. Recommendations

Taking into account that the Payment Services Directive is not yet transposed in all Member States, and its national rules will not enter into force until November 2009, and also taking into account the very recent adoption of the eMoney Directive, it should be noted that it is difficult to make general recommendations with respect to EU e-payment legislation.

Clarification of the scope of the eMoney Directive – As indicated throughout this document, the scope of articles 1.4 and 1.5 of the new eMoney Directive (relating to limited networks and value added services) is unclear, especially in relation to newly developing services (such as online platforms and virtual worlds). These articles must therefore be clarified, because the current rules will lead to much legal uncertainty for many emerging online payment services.

Add a new waiver scheme – We recommend to introduce an additional waiver scheme. Each waiver would automatically apply on an EU-level, and would consist of a mere notification duty (similar to the notification duty for internet access providers\textsuperscript{123}), whereby e-payment providers would be exempted from (part of the, or ideally all) financial regulations in the Payment Services Directive and eMoney Directive. However, in order to strike balance with consumer interests, this waiver scheme would only apply when the individual account held by each user, stores a maximum value of 150 EUR.

Limiting this waiver scheme to a maximum stored value of 150 EUR significantly reduces the possible negative impact in case of fraud by the issuer, security breaches or other situations which could lead to a loss of the stored value. As such, the benefits of e-payment, which allows cheap and quick transactions, will most likely outweigh the risks entailed by the waiver regime. In this context, this waiver scheme must require payment operators to take all necessary measures to prevent customers from using multiple accounts, so as to avoid a bypass of the 150 EUR limit and to avoid an increased financial risk for customers.

Such a waiver scheme would be particularly relevant for telecom operators to the extent the value stored on their prepaid cards is limited to 150 EUR. As such, they would no longer be subject to the provisions of the eMoney Directive for typical mobile payments such as the purchase of parking tickets or ringtones via SMS\textsuperscript{124}. Considering that online e-payment systems have become very successful in countries that

\textsuperscript{123} See note 60

\textsuperscript{124} See section 3.2.3 with respect to value added services and mobile payments
did not apply strict regulatory rules (such as Japan), we are convinced that this new waiver scheme will significantly foster private initiatives to create new e-payment systems.

**Voluntary accreditation** – While we think a strict regulation of all e-payment service providers cripples the uptake of e-payment services (hence our recommendation to add another waiver scheme), we think it could nevertheless be useful to introduce a voluntary accreditation system for e-money issuers in order to enhance consumer trust. By joining such an accreditation system, e-money institutions would assure consumers that the use of their e-money is safe and that transactions are secured in accordance with certain standards. Voluntary accreditation also entails a type of self-control, as members of an voluntary accreditation system will usually be reluctant to interact and trade with a member that fails to comply with any applicable standards and codes of conduct.

**Supervise online payment providers that process important transactions** – Services and systems which imply considerable financial transactions, must be subjected to a supervisory authority.

For example, in 2008, Second Life had over fifteen million users who collectively spent more than twenty million dollars in the virtual world every month. If such substantial amounts of e-money are being put into circulation, it is recommended that the issuers be supervised and controlled, and subject to a variety of consumer and privacy related obligations. There has, indeed, already been a bankruptcy of an “in-world” financial institution of Second Life in 2008.\(^{125}\)

To the extent the individual accounts of such services and systems only allow storage of a value of maximum 150 EUR, these services would need to be subject to our proposed additional waiver scheme.

**Mutual recognition for all waivers** – The current principle of mutual recognition for waivers must be reversed, so that waivers for e-payment providers will be mutually recognised across all EU Member States (unless in specific cases).

**Privacy implications** – Some types of e-payment schemes imply significant privacy and data protection related issues, in particular RFID technology based applications. Conversely, other schemes (including disposable prefunded cards and gift cards) can guarantee the user’s privacy and even anonymity, while still being easy to use in both the online and offline environment. The creation of such prepaid cards should therefore be further encouraged and stimulated, as this technology facilitates payment and transactions, and strongly enhances consumer trust.

**Online escrow services** – Online financial escrow services equally enhance consumer trust, as they ensure a correct transaction between buyer and seller, through a trusted third party. The development of such escrow services should therefore be stimulated, so as to increase their use and acceptance, and lower the transaction costs involved. As such services are particularly relevant for important financial transactions, it is recommended that they are subject to control and supervision (unless their involvement would be limited to transactions below a certain threshold), to the extent they do not fall within the scope of the Payment Services Directive.

**Merge** – As pointed out in section 3.3.2, we recommend to merge the Payment Services Directive and the eMoney Directive.

---

Chapter 8
Electronic contracting

1. Historic evolution

Electronic commerce in its early stages consisted of digital transactions between and among businesses and individuals. With the development of the Internet and the increased number of dot com companies, e-commerce became the use of the Internet to conduct business. Initially emerging from the Electronic Data Interchange (EDI) several major steps and changes have occurred to get it to its current point.

EDI – The first step came from the development of EDI, which is a set of standards developed in the 1960’s to exchange business information and do electronic transactions. While at first there were several different EDI formats that businesses could use, in 1984-1985 the ASC X12 standard became stable and reliable in transferring large amounts of transactions.

Web – The next major step occurred in 1992, when Mosaic, the first "point and click" internet browser – was made available. Mosaic was quickly adapted into a downloadable browser, Netscape, which allowed easier access to e-commerce. Christmas of 1998 also became a major milestone for e-commerce: American internet provider AOL, for example, had sales of 1.2 billion USD over the 10 week holiday season from online sales.

E-commerce – With the development of new technologies and business models, the Internet continued to grow as a very powerful technology for the development of e-commerce. The European e-commerce market was worth 106 billion EUR in 2006 (although 70% of the turnover was concentrated in the UK, Germany and France). Between 2004 and 2008, the percentage of individuals who had ordered goods and services over the Internet for private use in the past year in the EU rose from 22% to 34%. In 2008, 32% of individuals in the EU had ordered online in the past year. However, there is a significant variation across EU Members States in the level of e-commerce.

M-commerce – With the popularity of mobile phones and smartphones on the rise, mobile data and Internet services are following the same pace. Text messages have become the universal mobile data service for the masses, because it does not require special downloads or configuration as it is already embedded in over 98% of all cell phones. In relation to mobile Internet there are more than 40 million active monthly users in the U.S. alone. By 2013, it is expected that 125 million Europeans will use mobile Internet services. Moreover, at a worldwide level, there are 800 million users of Web-capable devices.

128 J. WEISMAN, Ibid.
129 Ibid.
131 Ibid.
132 www.cellsigns.com/industry.shtml
133 www.ecommercetimes.com/story/66795.html
134 www.forrester.com/ER/Press/Release/0,1769,1203,00.html
handsets. This mobility trend is further accelerated by the popularity of modern smart phones (such as iPhones and BlackBerrys), which are fully internet-enabled.

The future? – While mobile applications are the current trend, the next trend may be "intelligent" software and "smart agents", which enter into transactions on behalf of their human owner, within the limits specified by their owner.

2. Electronic contracting in the eCommerce Directive

This section 2 provides a description and analysis of the regime established in Articles 5.1, 9, 10 and 11 of the eCommerce Directive.

2.1. Background

Fragmentation – By the end of last century, during the golden era of the Internet, "a clear divergence in Member States’ approaches to e-commerce and e-contracting was developing. Some countries such as Germany had already forged ahead with new permissive legislation. Others, such as the UK, were lagging behind mired in the process of consultation". This was the perfect scenario to justify a Directive covering e-contracting issues in order to reduce the level of uncertainty, internet users' fears, and the lack of cross-border harmony. Moreover, as e-commerce would help to promote the Single Market goals, it was important to guarantee that local laws on e-contracting would not create barriers to cross border transactions. In fact, prior to the Directive, twelve Member States did not have clear legislation on the legal status of an electronic contract.

Initial proposal – In its Proposal for the Directive, the European Commission had identified "specific obstacles restricting the possibility of concluding on-line contracts across frontiers", especially because "[p]articular acts performed by the parties with a view to concluding electronic contracts may result in considerable legal uncertainty as to the conclusion of the contract. In particular, the same act of clicking on the "OK" icon may have different legal implications in different Member States (does it constitute acceptance of an offer to provide a service or a customer's offer to contract?) and can give rise to uncertainty as to the time when the contract was concluded (the time of receipt or of sending the acceptance?). This major divergence between the national legal systems, linked to the specific nature of the technological context, results in uncertainty in cross-border contractual relations – particularly for consumers – and is inimical to the development of the trust which is necessary for electronic commerce (one party may consider, on the basis of his own legal system, that the contract has been concluded while the other party, on the basis of his national rules, believes that he is not yet bound)."

Moreover, the Commission had also noted that "some formal requirements prevent contracts from being concluded electronically, or result in a considerable lack of legal certainty as to their lawfulness or

---

135 www.ecommercetimes.com/story/66795.html
136 Ibid., pp. 67-92
137 In its original French version: "aux inquiétudes de l'internaute", J. BERLEUR and Y. POULLET, "Réguler Internet", Études 2002/11, Tome 397, p. 472
validity. This may take the form of requirements which obviously rule out electronic contracts, (for example, a requirement that a contract be drawn up on paper), or more frequently, difficulty arising from the interpretation to be given to requirements such as "in writing" (i.e. on paper), "in a durable medium", "an original". Such legal uncertainty clearly works against on-line transactions; some Member States are therefore considering amending their rules and the courts have already given rulings on this matter. At Community level, the recent proposal for a Directive on electronic signatures does not deal with formal requirements other than signature”.

The Community, nevertheless, had already been involved in regulating electronic commerce for decades. In 1987, the TEDIS Electronic Data Interchange (EDI) programme was established to encourage the use of EDI in trade. Directive 98/34/EC and Directive 98/48/EC, both adopted in 1998, provided further procedures for the provision of information in the field of technical standards and rules on information society providers. Those Directives imposed on Member States the obligation to ensure that the standards of national bodies were compatible with the Commission’s standards and that they did not create barriers to the functioning of the Internal Market.

Other Directives related to e-commerce – The Distance Selling Directive, when implemented in 1997, did not regulate any distance e-commerce issues. It was originally tailored to regulate distance transactions concluded via catalogues, fax machines, and telephones. Other legal aspects regarding electronic trade before implementation of the eCommerce Directive were regulated in the Data Protection Directive 95/46 and the Electronic Signatures Directive 99/93.

2.2. Electronic contracting under the eCommerce Directive

2.2.1. Basic requirements

Article 5, 10 and 11 impose several basic contracting requirements for online service providers. Following the implementation of this Directive at a national level, service providers quickly adapted their websites to comply with these requirements. Thus, complying with the requirements of this Article did not originate major issues for website owners.

Information duty – In order to protect customers, article 10 holds that online service providers must provide information on the technical steps which customers have to follow in order to conclude a contract, how to correct input errors, and to provide information on codes of conduct, contract terms and

---

140 Council decision introducing a communication network community programme on trade electronic data interchange system (OJ 1987 L 285/1) and following decision (OJ 1997 L208/1)


143 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data


general conditions, prior to entering into the contract. Most of these obligations can, however, be deviated from for non-consumers.

Article 10 is complemented by paragraph 1 of article 5, which holds that a set of general information (such as the name and geographic address of the service provider) must also be provided by the service provider, even when the service provider does not enter into a contract.\(^{146}\)

**Harmonisation of contract rules** – Article 11 introduces an innovative method for formation of e-contracts. Unless otherwise agreed by parties who are not consumers, the e-contract will be concluded through the placing of an "order" by the recipient of the service, followed by an acknowledgment of the receipt of the order by the service provider. Moreover, the service provider has to make available to the customer effective and accessible technical means allowing for the correction of errors. If, however, the contract is executed exclusively by exchange of electronic mail or equivalent individual communications, the service provider does not need to make available a means for correction of errors or to acknowledge receipt of the order.

2.2.2. **Characteristics of the electronic contracting regime**

The electronic contract regime is characterised by the following principles.

**Equivalence** – Pursuant to the general principle set forth in paragraph 1 of article 9, contracts made by electronic means shall be valid. In other words, save for the few exceptions (which are also set forth in article 9), anything which can be achieved through written documents must be in law achievable through electronic documents.\(^{147}\) The provisions of this article are complemented by the Electronic Signatures Directive, which ensures the legal recognition of legal signatures.\(^{148}\)

The regime set out in paragraph 1 of article 9 does not apply to the contract types listed in paragraph 2 (such as real estate contracts, contracts requiring court involvement and family law contracts). It is not the purpose or intention of the Directive to have this list of exceptions remain unaltered for an unlimited period of time. According to paragraph 3, Member States must inform the Commission every five years of the reason why they would consider it necessary to maintain the category of "contracts requiring by law the involvement of courts, public authorities or professions exercising public authority" (article 9.2.b).

**Removal of obstacles for the use of e-contracts** – Article 9.1 establishes that Members States shall ensure that their legal system allows for contracts to be concluded by electronic means. For this purpose, they must remove any legal requirements that could create obstacles for the use of electronic contracts or deprive them of legal effectiveness or value.

Pursuant to paragraph 34 of the recitals, the examination of the legislation must be made in a systematic way and should cover all the stages and acts of the "contractual process" (including publicity, negotiation, offer, acceptance, registration, amendments, invoicing and archiving).\(^{150}\) This means that, by

---

\(^{146}\) Proposal for a European Parliament …, p. 22


\(^{148}\) According to article 5.1 of the Electronic Signatures Directive, a "qualified electronic signature" attached to electronic data shall have the same status as a written signature on a paper document.

\(^{149}\) The only change to the wording of this Article 9.1 from its first draft to the final draft was the elimination of the reference to "legislation". This change was intended to prevent common law Member States from using their common law principles of contract to achieve meet the equivalence principle without the need to enable legislation. Notwithstanding this change during the drafting process, according to Andrew D. Murray, the United Kingdom, a common law Member State, decided not to directly implement Article 9, thereby failing to fully implement this Article – See A. MURRAY, *Ibid.*

\(^{150}\) *Ibid.*, p. 201
way of example, Member States would have to amend a provision in their civil code requiring that certain contracts must be handwritten. However, according to paragraph 37 of the recitals, only legal obstacles have to be removed; practical obstacles do not have to be removed.

Information about the procedure of formation – "In order to ensure a high standard of fair trading and consumer protection" article 10 paragraph 1 imposes "extensive requirements" on the service provider (unless contractually agreed otherwise with customers that are not consumers). Service providers must also inform their customers of any codes of conduct the service provider has subscribed to, and how these codes of conduct can be consulted electronically. The purpose of this provision is to inform the customer of certain rules the service provider will comply with, particularly if those rules may have an impact on the customer's expectations.

The concluded contract – Prior to placing the order, service providers must inform customers on whether the contract will be filed by the service provider, and whether the concluded contract will be accessible by the service recipient.

Contractual terms and general conditions – Service providers must provide customers with the contractual conditions in a way that allows the customer to store and reproduce (print) them. The Directive does not establish any limit on the length of these conditions or on its content. Moreover, it does not provide for any difference between what should be included in the order and acknowledgement of receipt, vis-à-vis the contractual terms and general conditions.

The term "order" – Due to the "turbulent path" of article 11 during the drafting process, the title of this article and its paragraph 1 make reference to the term "order". The use of this term was the result of the consensus that the parties involved in the legislative process were able to achieve. This concept of "order" is a neutral term that avoids any reference to the concepts of offer and acceptance. According to GOBERT and MONTERO, the term "order" should be understood in a broad sense, irrespective of the online service it relates to, provided that from the "order" it is clear that the recipient wants to enter into an electronic contract with the service provider.

Acknowledgment of the receipt of the order – Without undue delay, the service provider must acknowledge the receipt of the order. The acknowledgment of the order has to be made by electronic means. It is not clear from the wording of the Directive if the immediate display of the acknowledgment of the receipt on the service provider’s website shall suffice to meet this requirement, or if it is required to send an e-mail.

---


152 For instance, contracts that have to be executed before a third party, such as contracts before a public notary - D. GOBERT and É. MONTERO, "Les contrats conclus par voie électronique", p. 207

153 Comments to Article 10, p. 6, Proposal for a European Parliament ...


155 M. DEMOULIN, "Information et transparence sur les réseaux" in Le Commerce Électronique sur les rails?, Bruylant, Brussels, 2001, p. 124

156 This process is explained in detail in A. MURRAY, Ibid.

157 D. GOBERT and É. MONTERO, Ibid., p. 258

158 Article 11, paragraph 1, first bullet

159 D. GOBERT and É. MONTERO, Ibid., p. 258, consider that these are alternative means of acknowledgment, although most of the service providers use both e-mail and display on a webpage for each order.
Moment of the “order” and “acknowledgment of receipt” – The second bullet of paragraph 1 of article 11 establishes a sort of “delivery” rule to determine the exact moment in which the order and acknowledgement of receipt occur. The order and/or receipt shall be deemed to be received when the parties to whom they are addressed are able to access them. In other words, it is the moment when the message “enters the circle” of the addressee that is relevant. In the case of an e-mail, the moment such message arrives at the mail server of the addressee’s e-mail address, the message will be deemed as received at that moment. This rule is particularly significant, as it is also applicable to electronic contracts concluded exclusively by exchange of electronic mail or by equivalent individual communications.

2.3. **Issues linked to the electronic contracting regime**

This section 2.3 highlights some of the issues related with and resulting from the electronic contracting regime deserving of further analysis.

2.3.1. **Formalities in articles 10 and 11**

The contracting requirements laid down in article 10.1 (transparency obligations), 10.3 (contract terms) and 11.2 (input errors) evidence the legislator’s “cold feet”: the legislator was afraid that consumer interests could be harmed during the online ordering procedure because customers were not familiar with online procedures, and therefore imposed basic requirements on the online service provider.

While these concerns may have been valid at the time the eCommerce Directive was adopted, they have now either become evident (tools to avoid input errors), have become a stumbling block for new technologies and business models (allowing to store terms and conditions), or merely lead to increased compliance costs (describing the technical steps of the contracting process).

Furthermore, it should be recognised that the consumer protection aspirations of articles 10 and 11 partially duplicate the existing rules of the *consumer acquis*. Abolishing article 10 and 11 would therefore not lead to less consumer protection.

---

For example, article 10.3 requires the service provider to make available the contractual terms and conditions. Articles 4 and 5 of the Distance Selling Directive have the same goal.

Similarly, article 10.1.d) requires the service provider to specify in advance which languages are offered for the conclusion of the contract. The concern expressed by the eCommerce Directive (avoiding that a website would be offered in one language, while the accompanying contract would be offered in a different language) is also tackled by the Unfair Commercial Practices Directive (e.g., article 7).

2.3.2. **Article 5 of the eCommerce Directive**

Article 5 holds that “In addition to other information requirements established by Community law, Member States shall ensure that the service provider shall render easily, directly and permanently accessible to recipients of the service and competent authorities: (…) (c) the details of the service provider, including his electronic e-mail address, which allow him to be contacted rapidly and communicated with in a direct and effective manner”

On 16 October 2008, the European Court of Justice ruled that the eCommerce Directive requires online service providers to offer a form of communication that permits the customer to contact the service provider rapidly and in a direct and effective manner. This form of communication must be offered before

---

the contract is formed, and must be offered in addition to an e-mail address. This case, the only EU-level case regarding the electronic contracting provisions of the eCommerce Directive, highlights a fundamental flaw of the eCommerce Directive.

Background facts – The defendant, Deutsche Internet Versicherung ("DIV"), is an automobile insurance company operating exclusively online. Through its website, DIV provided its postal address and e-mail to its website visitor, but no telephone number. Instead, an online enquiry template was offered which had a response time of 30-60 minutes; a telephone number was only provided after a contract was concluded. The German Federation of Consumers’ Associations brought an action based on Article 5.1 of the eCommerce Directive, alleging that the Directive requires DIV to provide a telephone number even before the contract was concluded.

The ruling – The ECJ held that Article 5.1(c) of the Directive had to be interpreted as meaning that "a service provider was required to supply to recipients of the service, before the conclusion of a contract with them, in addition to its electronic mail address, other information which allowed the service provider to be contacted rapidly and communicated with in a direct and effective manner. That information did not necessarily have to be a telephone number, it might be in the form of an electronic enquiry template through which the recipients of the service could contact the service provider via the Internet, to whom the service, provider replied by electronic mail except in situations where a recipient of the service, who, after contacting the service provider electronically, found himself without access to the electronic network, requested the latter to provide access to another, non-electronic, means of communication." In addition, the European Court of Justice stated that "in exceptional circumstances" where a recipient of the service, after making contact by electronic means with the service provider, is deprived of access to the Internet (e.g., due to a journey, holiday or a business trip), communication by an enquiry template can no longer be regarded as effective within the meaning of article 5.1.c of the Directive. The service provider must then provide "access to a non-electronic means of communication," even if that client initially entered into contact with the provider through electronic means.

According to the ECJ, the requirements of the "direct and permanent" means of communication were not sufficiently met by an e-mail address and, as such, online vendors must also display either a telephone number or, alternatively, a web response form that is answered in 30-60 minutes – not by an automated responder, but by a human being.

Evaluation – Offering only an e-mail address does not comply with the E-Commerce Directive’s disclosure requirements even when the service provider maintains very high levels of availability, both on its website and via the communication channels it offers to its customers through its website.

Instead of promoting digitalisation and use of electronic services, this ruling takes a step back, by assuming that the Internet is less available and less efficient than a telephone line or a mobile phone. The ECJ approach is to have more personal service, instead of electronic templates, and to guarantee to consumers an important level of service. But not all e-stores, particularly small web-shops, have those resources. Some e-stores are owned, managed and supplied by a single individual. They use the

162 Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV
163 see para [40] C-298/07 Bundesverband [2008]
164 see para [39] C-298/07 Bundesverband [2008]
Internet because of its reach and availability. This means that they could be receiving a visit on their website at 2:00 a.m. from a client in New Zealand.

Essentially, online service providers are now forced to provide 24/7 call centres to deal with requirements of the ECJ ruling. The ECJ obviously focused on consumer protection, without taking into consideration the fact that requiring additional direct contact with a human being creates additional costs for any enterprise which provide services online – not to mention SMEs and individuals acting as service providers. Moreover, the ruling was not very clear and created additional uncertainty on how service providers should be organised in order to comply with the ruling.

2.3.3. Unclear structure

Both paragraphs 1 (basic information requirements) and 2 (conveying codes of conduct) of article 10 include an exception for B2B contracts whenever the parties have agreed otherwise. However, paragraph 3 (making available T&C) does not contain a similar exception: no specification is made as to whether the "recipient" to whom the contract terms are to be provided is a consumer (B2C) or a business (B2B). It is not clear why this is the case.

2.3.4. Language requirements

According to article 10.1(d), service providers are required to provide recipients with information on "the languages offered for the conclusion of the contract". The question arises whether this requirement is relevant (or even whether this requirement has ever been relevant), because it is very uncommon for a website to be in a particular language, while the contractual terms are in another language. Therefore, this provision seems to result in a redundancy. Only in the event that the language of the contents on the website viewed is different from the language offered for the conclusion contract should service providers provide this information.

2.3.5. Confirmation step

Although in most legal systems contracts are formed through the exchange of offers and acceptance, the eCommerce Directive introduces a third step in contract formation – confirmation. Accordingly, a contract is concluded only when the customer has received an electronic acknowledgement of his order from the service provider. Pursuant to article 11, if a service provider fails to send a confirmation to the consumer issuing acknowledgment, no contract is formed.

The central principle behind the prior information requirements provided for in article 10 of the Directive is to establish the confidence of consumers and businesses in e-commerce, which is again a sign of the legislator's "cold feet" in the area of contracting. Consumers will only be willing to use electronic commerce if they are convinced that it is as safe and reliable as conducting transactions on the traditional market.

Hence, in the words of MURRAY, "it quickly becomes clear that article 10 is not a formation of contract provision at all, but rather a consumer protection provision embedded into the contract formation rules."

2.3.6. Execution of contracts via new devices

Articles 10 and 11 establish a regime which is mandatory for all electronic contracts entered into with consumers, and that may be briefly explained as follows: information such as the technical steps for

---

\[165\] Article 11 of the eCommerce Directive
Conclusion of the contract, technical means to identify and correcting input errors and the terms and conditions of the contract (in a way that allows the service recipient to store and reproduce) is made available to the recipient of the service. The recipient will then agree with the offer and place the order. The service provider must then acknowledge receipt.

**Procedure with a typical pc** – It is very easy to imagine an individual (recipient of the information society service) in front of a computer screen going through the steps for conclusion of the contract and the terms and conditions, then clicking "OK" to accept the terms and conditions and storing them in the computer hard drive and, finally, receiving an e-mail with the acknowledgment of receipt of the order placed. To have this process properly executed, it would be necessary to have a screen large enough to allow for the reading of the terms and conditions, a mouse to click on the "OK" button of the terms and conditions, a hard drive to store all of this information and an e-mail account to receive the acknowledgement of receipt.

**New technologies** – Today, several new online services are being made available to the public, including services targeted to companies, through the use of SMS or instant messaging.

*For example, while waiting at a bus stop for a bus, it is possible to request a service from the bus company providing information on when the next bus is due to arrive at such bus stop (a fee is charged for this service). This service is delivered upon sending an SMS to a number provided by the bus company. Such service is also an information society service pursuant to Directive 98/34 amended by Directive 98/48[^166], and for this reason it must comply with the requirements of articles 10 and 11.*

**Limitations of SMS** – SMS services have certain technical limitations in opposition to the user experience of accessing information through a browser on a computer screen. For instance, an SMS only allows 160 characters per message. The length of the majority of the terms and conditions for any service would take up more than 160 characters, or even ten times more. Should the recipient have to receive 10 SMS messages on his/her mobile phone before accepting any service, he would most likely not enter into the contract.

In addition to the number of messages, it is also important to consider size and design limitations of the devices, proving to be too bothersome for the consumer to read long texts on such devices. Accordingly, it is not very likely that the consumer will read all of this information, at least while in the process of formalising the contract[^167].

**Ease of use** – Like in most consumer-related services, consumer adoption and use shall only occur if the service is useful and easy to use. The bus stop example is a prime example of how important it is to have simple solutions. The same line of reasoning applies to the provision of information society services via PDAs or smart phones[^168], instant messaging services, *"and in the future – who knows?"[^169].*

**Technology neutral?** – With the increase in the number of mobile phones[^170], more services will be launched at a global scale[^171]. The question arises whether the current regime is still adequate for all online services, including those that exist and/or will exist in the future.

[^166]: Preamble, and paragraphs 34 of eCommerce Directive
[^168]: Website owners make available versions of their websites prepared to be viewed in PDAs or smartphones.
[^170]: There are over 3 billion mobile phones worldwide. This means that over 40% of the world’s population carries a mobile phone, far more than use a computer or have access to the internet. In many developed countries, mobile phone penetration
The eCommerce Directive claims to take a *technology neutral* approach. In fact, in several of its provisions, the Directive makes reference to "electronic means" without ever specifying the device to be used by service recipient. This is indeed the correct approach in order to promote innovation.

However, the Directive is not as "technology neutral" when it comes to establishing the steps for concluding contracts by electronic means. The required contractual steps and the entire legal structure seems conceived as if all customers would sit in front of a computer screen. This "contractual process" is very difficult to implement for mobile services.

These constraints are far from being a surprise. In November 2000, GSM Europe, the European interest group of the GSM association, wrote a letter to the Commission stressing the "necessity to take into consideration the specificities of m-commerce enablers such as mobile handsets" when implementing the Directive at national level. Moreover, the Commission, in a 2004 document, had already noted that the information requirements on the Distance Selling Directive were implicitly based on computers as the main technology to provide Internet access.

### 2.3.7. Storage and reproduction of contract terms and general conditions

Article 10.3 establishes that the online service provider must make available to the customer the terms and conditions, in order to allow him to store and reproduce them. The relevant web page will have to be prepared and configured in such a way that the recipient at "his place" may adequately print or store them.

Technological development and change in consumer behaviours have made this provision outdated. Websites play a much less central role in today's consumer web experience. Consumer behaviour was recorded in The Yearbook of Consumer Law (2008) and evidenced that, upon being questioned on whether they read the terms and conditions made available to them when contracting online, 43% of consumers said they "sometimes" read them, 29% "always" read them and 28% of consumers never do.

Such a provision clearly calls into question the form of click-wrap agreement, when the agreement is displayed in a separate window from which it cannot be downloaded, copied or printed. Furthermore, a significant number of service recipients use mobile phones to access online services, which make the storage of contract terms and conditions barely feasible. Some of these mobile equipments do not allow...
– or have limited capabilities – to store information which is made available on a web-page (including when such webpage is prepared to meet the requirements of article 10.3). Moreover, most of the mobile devices are not prepared to interface with printers to carry out printing jobs.

2.3.8. Length of terms and conditions

As pointed out above, most consumers do not read a service provider’s terms and conditions. Still, the terms and conditions often contain important and extensive exclusions of liability of which end-users are not aware.

This observation is likely at least partially linked to the length of the contractual terms and conditions.

For example, the terms and conditions of Apple iTunes encompass about 23 pages when printed; those of Amazon and Dell each about 15 pages; those of Facebook about 8 pages.

The eCommerce Directive does not restrict the length of the contractual terms and conditions used by an online service provider. Although the issue of lengthy contractual terms and conditions is not limited to the online environment — they equally exist in the offline environment — it must be recognised that offline terms and conditions are typically limited to a single page (often in a small font, printed on the back of an invoice) as it would be burdensome to provide a separate bundle of paper with terms and conditions. Conversely, the unlimited space available on websites seems to incentivise lawyers to make the terms and conditions overly long. Also, many lawyers seem to suffer from "cold feet" in the online context, so that many unnecessary legal provisions are nevertheless included.

However, lengthy terms and conditions are difficult to reconcile with the fast-moving and multi-tasked online environment, and are also difficult to apply to minors. Expecting a customer (particularly a minor) to read twenty pages before a service can be used, is exaggerated. We therefore recommend the Commission to adopt sector-specific, concise templates of terms and conditions, and to incentive service providers to use these templates. An interesting idea would also be to create a set of "boiler plate" standard clauses, whereby the actual terms and conditions of a service provider would only need to list clauses that deviate from the boiler plate standard clauses. This would drastically reduce the length of terms and conditions.

Preferably, the use of such templates would also be integrated in trustmarks.

3. eSignatures

Directive 1999/93/EC on a Community framework for electronic signatures (eSignatures Directive) aims to ensure a basic legal recognition of electronic signatures within the EU, and allow the free flow of electronic signature products and services cross border.

---

178 The typical use of "legalese" expressions is another issue.
179 See, for example, the Belgian version at www.apple.com/legal/itunes/befr/terms.html
180 See, for example, the UK version at www.amazon.co.uk/gp/help/customer/display.html?ie=UTF8&nodeId=1040616
181 See, for example, www.euro.dell.com/content/topics/topic.aspx/emea/topics/footer/terms?c=uk&l=en&s=gen
182 See www.facebook.com/terms.php?ref=of
183 See our recommendation in Chapter 13 - self regulation
Legal recognition – As the Commission noted in its Report on the operation of the eSignatures Directive, the first objective has been achieved by the transposition of the Directive into the legislation of the Member States. By implementing the general principles of the Directive, all Member States legally recognise e-signatures. As such, the objectives of the Directive have already been largely fulfilled at this moment.\textsuperscript{186}

Cross-border use – However, a legal and technical analysis of the practical usage of electronic signatures shows that the objective of (cross-border) use of e-signatures has not yet been achieved.\textsuperscript{187} Service providers have little incentive to develop a multi-application electronic signature and prefer to offer solutions for their own services. As a result, today’s e-signature market consists of isolated islands of e-signature applications, where certificates can only be used for one single application.\textsuperscript{188} This lack of technical interoperability has been the main obstacle for market acceptance of e-signatures. In turn, the lack of market acceptance further decreases the incentive for service providers to develop new and multi-application e-signatures. In other words, a classic "chicken-and-egg" situation.

Action Plan – The Commission has acknowledged the need for mutually recognised and technically interoperable e-signature solutions, and has therefore adopted an Action Plan on e-signatures, which aims to offer a comprehensive and pragmatic framework to achieve interoperable e-signatures.\textsuperscript{189}

- With respect to qualified electronic signatures and advanced electronic signatures based on a qualified certificate, the main obstacle for cross border use lies in the lack of trust in e-signatures originating from other Member States. At present, it is often difficult to obtain information regarding the status of the certification service provider, or to verify the quality of the signature (as regards its advanced or qualified nature).

To facilitate this validation process, the Commission will compile a "Trusted List of Supervised Qualified Certification Service Providers" at a European level. In addition, it will further update the list of generally recognised standards for e-signature products.\textsuperscript{190}

- With respect to advanced electronic signatures, Member States have used very diverse technical solutions with different security levels.\textsuperscript{191} Similar to qualified e-signatures and advanced e-signatures based on a qualified certificate, the main challenge lies in the fact that receiving parties must be able to easily validate advanced electronic signatures, and to trust their legal value or security level.

To avoid multiple validation efforts in Member States, the Commission proposes to delegate these verification and validation tasks to a centralised or distributed validation service mechanism. The available options for establishing such a mechanism will be examined through a feasibility study.\textsuperscript{192}

We welcome this Action Plan: with such initiative, the Commission is taking the necessary steps to further encourage and facilitate the use of e-signatures. As the main obstacles for widespread use of e-signatures are of a practical and technological nature rather than a legal nature, it is indeed necessary to

---

\textsuperscript{186} Ibid., p. 9-10
\textsuperscript{188} Report, p. 7
\textsuperscript{189} Action Plan, p. 4
\textsuperscript{190} Ibid., p. 7-8
\textsuperscript{191} Article 2.2 of the eSignatures Directive defines advanced electronic signatures in a generic way. Member States had more discretion as to which advanced electronic signature solutions they would accept.
\textsuperscript{192} Action Plan, p. 8-9
take measures which can simplify the technical validation and verification of e-signatures in practice. By doing so, the Commission has taken a first step to deal with the "chicken-and-egg" problem described above.

**Long-term validation** – A second reason for the reluctance to implement e-signature applications is that the archiving of electronically signed documents is often considered too complex and too uncertain\(^{193}\). This is caused by the fact that the validity of certificates is usually limited in time. Indeed, the rapidly evolving technologies for certificates do not allow certificates to have a long-term validity.

The expiry of such certificates also entails the expiry of e-signatures based on these certificates. This problem can be bypassed by resigning the document with a new certificate each time the previous certificate expires, which is, however, a laborious procedure. The expiry of certificates and e-signatures undermines the concept of e-archiving, as the advantages thereof do not seem to outweigh the disadvantages. The issue of long-term validation of e-signatures therefore currently remains unresolved, and also requires to be addressed on a technical level rather than from a legal perspective.

4. E-invoicing

4.1. Introduction

All companies would like to cut back costs by 80% and reduce the average cost of 30 EUR of processing a paper invoice. Needless to say, in pursuit of these results, businesses are now looking at e-invoicing\(^{194}\).

It is estimated that more than 30 billion paper invoices are sent each year in Europe. The adoption of e-invoices would deliver potential savings of 243 billion EUR per annum in Europe, according to the Corporate Action on Standards (CAST) project from the European Association of Corporate Treasures\(^{195}\). In addition to the costs reduction, there are other significant benefits associated with the use of e-invoices. Such benefits include\(^{196}\) better customer services, jobs with less routine and better environment\(^{197}\). These benefits also align with the goals set out in the Lisbon Agenda, to allow Europe to become the most competitive and dynamic knowledge-based economy in the world.

---

\(^{193}\) Report, p. 8  
\(^{195}\) See E-Invoicing 2008, published by the Euro Banking Association and Innopay (available at www.abe-eba.eu; www.innopay.com), p. 55, section 5.2. In this section it is also mentioned that the University of Hannover has potential savings of nearly €135 billion per year  
\(^{197}\) Ibid. It is estimated that the energy and raw material needed for producing of the relevant paper, printing, enveloping, distributing and recycling 20 billion invoices would correspond to the following savings per year in the event of replacement of e-Invoices: 400 000 tons of paper; 2700 tons of ink; 160 million liters fuel; 1432 GWH energy and 15 million trees - www.i2010conf.si/P2-Harald.pps - 588, 5, Slide 5
4.2. The Electronic Invoicing Directive

4.2.1. Electronic invoicing before the Directive

"The invoice is probably the most important document in commercial trade", according to a 1999 PWC Report\(^{198}\). With the Single Market as an ultimate goal, a simplification and a harmonisation of the national VAT legislation on invoice requirements was deemed to be necessary in those days. For instance, some Member States like Germany, Greece, Luxembourg and Portugal\(^{199}\) did not recognise paperless electronic invoices as proper invoices for VAT purposes.

EDI – In relation to the technologies used, EDI\(^{200}\) and e-invoice delivery over the Internet by means of e-mail attachments were the systems used. However, both EDI and the use of e-mails were not treated in the same way by the Member States. In some Members States (like Belgium, France, Italy and Spain) the use of the EDI standards was mandatory, while in others (Austria, Denmark, the Netherlands, Sweden and the UK) EDI appeared to be the a de facto standard.

The same type of inconsistency among Member States existed in relation to the possibility to attach e-invoices to e-mails: Austria, Denmark, Finland, Ireland, Italy, Sweden and the UK were the only Member States allowing this. This inconsistency between Member States – of which the above mentioned cases are only an example – represented a significant barrier for the Single Market goals and for the development of electronic commerce.

It was clear then, as it is today, that new technologies can provide more security and offer more information, in a form easier to utilise than paper invoices, all this with lower production and storing costs for businesses. The European Commission recognised these concerns in a proposal of Directive\(^ {201}\): "the development of electronic commerce has made it necessary to establish a legal framework for the use of electronic invoicing to enable tax administrations to continue to perform their controls". This proposal was later amended and approved by way of Directive 2001/115/EC\(^ {202}\) (hereinafter called the "eInvoicing Directive"). Directive 2001/115/EC was eventually replaced by Directive 2006/112/EC\(^ {203}\) (the "Invoicing Directive"), although no relevant changes were made to the provisions on electronic invoices.

4.2.2. Invoicing under the eInvoicing Directive

Under the eInvoicing Directive, traders in Europe have to comply with one set of VAT rules for all the invoices it issues, irrespective of the place of taxation of the goods or services being sold. This Directive establishes the following regime for Member States to implement:

\(^{198}\) "Study on the requirements imposed by the Member States, for the purpose of charging taxes, for invoices produced by electronic or other means" by PriceWaterHouseCoopers, available at http://ec.europa.eu/taxation_customs/taxation/vat/key_documents/reports_published/index_en.htm

\(^{199}\) Ibid. "Study on the requirements imposed…", Section 4.2, p. 33

\(^{200}\) Additional information on EDI is available on p. 30 of "Study on the requirements imposed…"


- A list of mandatory items that must be mentioned on each invoice (such as name and address of the seller, date of issuance, number of the invoice, applicable VAT rate, etc.).

- Electronic Invoices – Traders have the right to issue invoices valid for VAT purposes both in paper or electronic by trades. They may use electronic invoicing on the condition that the authenticity of the origin and integrity of the content of the invoice are guaranteed. Pursuant to the Directive, those guarantees can be ensured by way of advanced electronic signatures, Electronic Data Interchange (EDI), or by any other method accepted by a specific Member State.

- Place of storage – Traders have the freedom to choose the place and method of storage of invoices (they may store invoices on-line in a Member State other than the country where it is established for VAT purposes).

- Outsourcing – Traders have the freedom to outsource invoicing operations to a third party or to his customer (i.e. self-billing).

Notwithstanding all the efforts of the Commission in preparing a directive that would allow for a significant harmonization and the benefits of this Directive, the wording of several provisions allowed for an open interpretation by Member States while implementing it. This has led to a lack of harmonization:

- Content of the invoice – Several Member States’ national VAT legislation contained provisions establishing requirements which go beyond the mandatory contents of an invoice set out in the Directive. For instance, in Hungary it was required to include an invoice page number as well as the total number of pages.

- Summary statement on paper for EDI – In certain national legislations, entities using EDI have to issue a paper summary document (for instance, Portugal, Greece or Hungary), while in other legislations there was no such requirement.

- Electronic signatures – Among other Member States, Greece and Germany required the electronic signature to be based on a qualified certificate, through means of a secure-signature creation device. For other countries, like Sweden and the United Kingdom, an advanced electronic signature would suffice.

- Signature by legal entities? – While electronic invoices do not need to be signed in order to be valid, electronic signatures can be used in the context of electronic invoices, as a means to secure the authenticity and integrity of an electronic invoice. Both functions of an electronic signature (signing and ascertaining security) should be clearly distinguished, although they both use the same technologies. It should not come as a surprise, however, that the dual role of electronic signatures has led to confusion regarding the question of whether a natural person should necessarily be involved in creating an electronic invoice. In those Member States that require an invoice to be secured by a qualified electronic signature for security reasons, it is often (wrongly) assumed that these qualified electronic signatures can only be placed by natural persons. This interpretation

204 See, particularly, the conclusions from "CompTIA EU Electronic Invoicing and VAT compliance requirements Publication", 2005, from CompTIA – The computer Technology Industry Association – www.comptia.org

205 See article 229 of the eInvoicing Directive

206 Even though it is acceptable to argue that only a natural person can place a qualified electronic signature to sign an electronic document (because only natural persons can place a traditional handwritten signature on a paper document), nothing prevents a legal person from placing a qualified electronic signature to secure an electronic document such as an invoice. The latter use of a qualified electronic signature is merely for security reasons, and — despite its name — does not fulfill the function of a traditional handwritten signature. As mentioned, this opinion is not shared by all commentators.
completely defeats one of the most essential purposes of electronic invoices, i.e. to allow invoices to be generated more efficiently by avoiding unnecessary human interactions.

- **Place of storage** – Not all Member States have established the same storage requirements. By way of example, in Belgium storage must be in electronic form and guarantee full on-line access, while the same is not applicable in Hungary.

This situation has led to a scenario of lack of harmonization with legal uncertainty. Any company involved in cross-border electronic invoicing has to comply with a (slightly or significantly) different regime for each of the Member States with which it was doing business, which increases the invoicing costs substantially, due to the increase in complexity of the relevant IT system. The increase in direct and indirect costs not only applies to companies doing cross-border trade, but also to companies offering electronic invoicing services, software solutions or auditing e-invoicing services.

It should be noted that the aforementioned discrepancies only concern issues that are addressed by the eInvoicing Directive. Other issues (such as the time of storage of data and verification of certificates) are also not harmonized, thereby contributing to the legal uncertainty and increase of costs, and creating additional barriers to cross-border trade.

---

**Practical example: delegated signing of e-invoices.** A leading European e-invoicing service provider developed a new e-invoicing system that would allow customers to send raw invoice data from its enterprise systems to the service provider’s central e-invoicing platform. The service provider's platform would then convert the raw data into a PDF file that was signed with the service provider's qualified signature. This PDF file – which constitutes the invoice for legal purposes – would then be sent to the recipient selected by the customer.

When the service provider performed a legal compliance audit of this system, it was revealed that assessing the legal compliance of this system with the rules of the eInvoicing Directive was difficult, because the authenticity of the origin of the invoice did not result directly from the advanced (or even qualified) electronic signature that was applied to the PDF file (which referred to a certificate of the service provider). In addition, although the service provider's end-to-end workflow was very secure, the integrity of the content of the invoice did not only result from the use of an advanced or qualified electronic signature, but also from secure communications between the service provider and the customer, as well as extensive audit trails. For these reasons, it was difficult to assess that "the authenticity of the origin and the integrity of their content are guaranteed "by means of” an advanced electronic signature, even though the service provider's platform was innovative and at least as secure as platforms that rely on EDI methods to secure invoices.

---

4.3. **A moving target**

4.3.1. **The EEI Report**

As previously noted, the current electronic invoicing framework is on the move.

In July 2007, the European Commission Informal Task Force on E-invoicing completed its report on Electronic Invoicing (hereinafter the "EEI Report") 207. This report highlighted the fact that Electronic

---

Invoicing "penetration and adoption" in Europe to be limited, irrespective of the fact that several cases have evidenced that the use of electronic invoices may lead to significant savings.

The EEI Report identified three levels of barriers for electronic invoicing:

- **Standardisation** – A significant number of technical specifications for electronic invoicing are currently in use. Unfortunately, none of these specifications are a perfect fit for the mass-market. According to the report, further standardisation work is necessary to decrease the need for costly integration and improve interoperability between existing European standards and solutions. An international e-invoice standard should also be developed. A common international (ISO) European Electronic Invoice standard would also avoid the need for interim European standards, which will be costly to amend or replace in the longer term.

- **Trust and Operational** – Risks associated with the electronic exchange, automated processing and storage of invoices will have to be reduced. Whether an invoice is sent in paper form or via electronic means has no bearing upon the level of trust between the trading partners involved. It is to be expected that business and financial controls will be applied for an e-invoice, as they would for its paper equivalent.

- **Legal** – E-invoicing lies at the crossroads of several areas of legislation (mainly VAT, accounting, payment, authentication, company transparency and data retention). This adds complexity and uncertainty to the implementation of any e-invoicing solution for both the supplier and buyer, as well as for the vendor or the service provider. Moreover, there is currently no certification of e-invoicing solutions in place, or indeed harmonised legal or administrative practices between Member States.

The EEI Report therefore endorsed the creation of an EEI Steering Committee with the purpose of harmonizing approaches in order to establish an "umbrella EEI Framework".

Following publication of the EEI Report, and as per the recommendations set out therein, the Commission has appointed a group of experts with a mandate to prepare a European e-invoicing Framework by the end of 2009. One of the tasks of the Expert Group is to identify those shortcomings in the regulatory framework for e-invoicing at Community and Member State level that prevent the Community economy exploiting its full potential.

### 4.3.2. The Mid-Term Report

On 27 January 2009, the Expert Group released its Mid-Term Report.

In order to help remove the barriers to massive adoption of electronic invoices, the Mid-Term Report sets several initial recommendations and identifies priorities.

This Report calls for the "principle of equal treatment of paper and electronic invoices with no distinction between invoicing carried out on a domestic or on a cross-border basis within the EU."

The Report suggests that it is not advisable to place additional demands on "electronic invoices as they generally are..."
more secure and less prone to fraud than paper invoices. In the same paragraph, it is also mentioned that "the threshold to electronic invoicing must be lowered and be unified especially in the VAT auditing dimension". This is indeed a sound position, which aligns with the increased convergence of the online and offline environment, and constitutes a message to all stakeholders towards the massive adoption of electronic invoice.

4.3.3. The new proposal

Following the recommendations of the Expert Group and an open consultation, the Commission published its "Proposal for a Directive amending Directive 2006/112/EC on the common system of value added tax as regards the rules on invoicing". In the proposal, the Commission notes that in order to promote e-invoicing, the proposal aims to eliminate the barriers to e-invoicing by removing the differences between electronic invoices and traditional paper invoices. Accordingly, a new article 218a holds that "Member States may not impose on taxable persons any obligations or formalities, other than those laid down in this Chapter and Chapter 4, in relation to the issue or storage of invoices, irrespective of whether the invoices are sent or made available by electronic means or sent on paper."

Taking into account the many issues that plague the current e-invoicing legal framework, we fully endorse this proposal and strongly recommend its adoption.

5. E-archiving

5.1. Introduction

Electronic document management and electronic information transmission constitutes an extensive part of commercial and administrative activities. However, paper documents are not likely to completely disappear as electronic documents take the front seat: individuals still often fall back on the use of paper when dealing with crucial information, such as important contracts.

One of the reasons leading to the distrust in electronic documents has been identified as the lack of security on the possibilities for storing electronic documents on a longer term. Although the lack of trust in electronic documents has been pointed out as an issue when it comes to regularly using such documents as complete replacements of paper documents, one of the most difficult issues faced with regard to e-archiving refers to the cross-border context within an electronic environment.

5.2. E-archiving and EU legislation

On 27 January 2009, the Expert Group on E-Invoicing adopted its mid-term report providing for an outline of the overall progress made during the first year of the group’s mandate and represents an important step towards the final proposal of the EEI Framework. Upon publishing this report, stakeholders were invited to provide their comments and a summary was drawn. According to the

213 Mid-Term Report – Section 1.4.2, p. 7
217 Feedback on Comments Received on the Mid-Term Report of the Expert Group on E-Invoicing, 6 April 2009
218 Ibid.
summary of the comments received, some respondents specifically called for more clarity and harmonisation of archiving requirements.\textsuperscript{219}

Diverging implementation of the rules governing e-archiving hinder the use of electronic invoices. Although the issuer was given the prerogative to choose the place of storage of electronic invoices\textsuperscript{221}, for example, some Member States have imposed additional conditions concerning notification requirements to tax authorities and periods and terms of storage.

For example, France allows storage outside of its national borders, but only in countries that have signed mutual assistance agreements. Conversely, Germany only allows storage in other Member States\textsuperscript{222}.

Reference to e-archiving within E-Commerce at the EU level is found in the eInvoice Directive, as well as in the eCommerce Directive itself:

- In the absence of a set of rules and requirements specifically governing archiving in the EU, a reference to transmission and storage of invoices “by electronic means” is found in the eInvoice Directive. This Directive has provided that “transmission and storage of invoices ‘by electronic means’ means transmission or making available to the recipient and storage using electronic equipment for processing (including digital compression) and storage of data, and employing wires, radio transmission, optical technologies or other electromagnetic means”\textsuperscript{223}.

- In addition to e-invoices, e-archiving also applies to other elements of e-contracting. The eCommerce Directive sets forth that contract terms and general conditions provided to a recipient must be made available in a way that allows him to store and reproduce them\textsuperscript{224}. Furthermore, an additional reference to archiving is found in article 10.1.b of this Directive, requiring service providers to provide service recipients with information on whether “the concluded contract will be filed by the service provider and whether it will be accessible”.

5.2.1. The eInvoice Directive

The invoice, in terms of legal reality, is one of the most important documents in business processes. It holds references relating to the customer, products delivered and services rendered. Invoices must be archived and presented to auditors to support balance sheet entries and provide internal records of transactions\textsuperscript{225}.

Audit efficiency – Electronic document archives enable quick access to information; therefore, they allow a significant increase in audit efficiency of benefit to both tax authorities and businesses. However, although there remains a lack of standardization in e-invoicing practice, and irrespective of the significant efforts currently being employed, it is important that businesses in Europe can choose the e-invoicing technologies, business control framework and processes that better suit their particular circumstances.

\textsuperscript{219} Contributions to the consultation came from six different Member States, with an additional five replies from representing bodies at the EU or global level.

\textsuperscript{220} Feedback on Comments Received on the Mid-Term Report of the Expert Group on E-Invoicing, 6 April 2009


\textsuperscript{222} European Invoicing Final Report 2007

\textsuperscript{223} Ibid., article 2(2) paragraph 3(e)

\textsuperscript{224} Article 10(3) of Directive 2000/31/EC

\textsuperscript{225} Mid-Term Report of the European Commission Expert Group on Invoicing, 27 January 2009
Imposing limited options for e-invoice implementation is not only counterproductive for businesses, but also for the European economy.\(^{226}\)

**Authenticity of the archiving** – According to article 2.2.d of the e-Invoice Directive, every taxable person shall ensure that copies of invoices issued by himself, by his customer, or in his name and on his behalf, by a third party, and all invoices which he has received are stored. The authenticity of the original and integrity of the content of the invoices as well as their readability must be guaranteed throughout the storage period.

**Place of storage** – The electronic data may be stored in any EU member State under the condition that there is online access to the electronic data. Moreover, the data can be stored outside the EU territory, but only under the additional condition that the third country guarantees the storage of invoices according to the European data protection rules. Each Member State has the possibility to opt out if there is no mutual assistance agreement with the third country. Several Member States (such as Germany) do not agree on storage outside the European Union territory. In contrast, Estonia allows storage outside the EU. Some Member States demand prior notification to the national tax authorities.\(^{227}\) Nevertheless, as mentioned above, the electronic invoices can be stored on any medium provided that it guarantees the integrity, authenticity and readability of the invoices.

5.2.2. **The eCommerce Directive**

The invoice is not the only important document in the audit trail. Other relevant documents include purchase orders, transport documents, delivery notifications and remittance advices.\(^{228}\) Therefore, these other elements of e-contracting also need to be duly archived.

Article 10.1.b of the eCommerce Directive holds that information on whether "the concluded contract will be filed by the service provider and whether it will be accessible" must be provided to service recipients. Additionally, article 10.3 of this Directive holds that "contract terms and general conditions provided to a recipient must be made available in a way that allows him to store and reproduce them".\(^{229}\) All of these documents need to be auditable and accessible. In order to ensure this, they must be properly archived.

Article 10 of the eCommerce Directive aims to provide transparency as well as consumer protection in on-line transactions.\(^{230}\) For purposes of this section on e-archiving under the electronic contracting regime, article 10.1.b and 10.3 are of particular importance whereby the service provider must inform the recipient of whether the "concluded contract will be filed by the service provider" and additionally that "contract terms and general conditions provided to the recipient [of the service] must be made available in a way that allows him to store and reproduce them".

---

\(^{226}\) Code of Practice on Electronic Invoicing in Europe, 24 March 2009

\(^{227}\) EEI final report

\(^{228}\) *Ibid.*, at p. 5

\(^{229}\) Article 10(3) of Directive 2000/31/EC


\(^{231}\) With reference to Article 10(1) of the eCommerce Directive where information requirements are between the "service provider" and the "recipient of the service"
Service providers tend to keep copies of their concluded electronic transactions\textsuperscript{232} for their record keeping and in the event of any future dispute. Accordingly, in view of this practice, service providers are better poised than consumers to maintain adequate archiving IT systems.

5.3. Requirements

Readability – The eInvoice Directive requires a guarantee of the readability of the electronic invoices during the storage period. An invoice is considered readable if all components of the corresponding record and optional electronic signatures may be retrieved and viewed on screen or printed in a way to be understood by a person.

Format and duration of storage – Member States can impose conditions on storage. They can opt for storage of the original format as well as storage of data guaranteeing the authenticity of the original and the integrity of the content. Member States like Belgium, Cyprus, France, Denmark, Hungary, Iceland, Latvia, Lithuania, Malta, Portugal, Slovakia, Slovenia, Spain and Sweden have imposed the requirement that invoices must be received in original format. Some, however, do not impose this requirement for issued electronic invoices, such as Cyprus, France, Ireland and Portugal\textsuperscript{233}.

Period of storage – The duration of storage is not harmonised at the European level. Member States are to determine the period for which invoices must be stored by taxable persons relating to goods or services supplied in their territory\textsuperscript{234}. Electronic archive records need to be stored for five years in Denmark, seven years in the UK and ten years in Germany\textsuperscript{235}. The average period is ten years. The Code of Practice on Electronic Invoicing has provided a guideline for storage whereby the audit trail maintained by businesses must be accessible for six years\textsuperscript{236}.

6. Digital evidence

6.1. Introduction

New technologies have exponentially increased the creation of electronic documents within organisations. More than 3 trillion of e-mails are sent in the world every year. More than 90% of the documents in an organisation are electronic and less than 30% are finally printed.

The use of the digital means and the virtual environment is not exempt from dishonest use and traditional evidence is moving from paper support to a virtual environment. As more and more transactions from the commercial world, government and private individuals exist only in digital form, the only way in which someone can prove that something has happened – or has failed to happen – is via digital evidence\textsuperscript{237}.

\textsuperscript{232} M. DEMOULIN, “Information et transparence sur les réseaux” in Le Commerce Électronique sur les rails?, Bruylant, Brussels, 2001, p. 121

\textsuperscript{233} Electronic Invoicing challenges In Europe, the Computer Technology Industry Association

\textsuperscript{234} eInvoice Directive

\textsuperscript{235} See www.efstechnology.com/pdfs_whitepapers/e-invoicing_whitepaper.pdf

\textsuperscript{236} See Code of Practice on Electronic Invoicing in Europe, 24 March 2009. One of the core principles includes "Auditability: Businesses must be able to demonstrate and explain their administrative and control capability. Businesses must maintain an audit trail, including the underlying transaction data and any relevant supporting documentation and data, which must accessible towards external auditors, both statutory and tax. Accessibility must be ensured for six years."

In this context, management procedures and admissibility criteria are undergoing changes with regard to traditional evidence\textsuperscript{238}.

The importance of digital evidence grows proportionally to the growth of e-commerce in the European Union. The gap between domestic and cross-border e-commerce is widening, however. 71\% of consumers have indicated that a major inhibiting factor to their cross-border purchases are cross-border enforcement and redress while 39\% of consumers think that it is harder to resolve problems such as complaints, returns, price reductions, or guarantees when purchasing from providers located in other EU countries\textsuperscript{239}. Therefore, having to present electronic data in possible disputes is a very common scenario.

Between September and November of 2003, the open consultation on legal barriers in e-business took place. Among the reported cases was the question of legal validity of various types of electronic documents used in commercial transactions\textsuperscript{240}. It was noted that the legal recognition of the various types of electronic documents used in business processes is not always ensured. This is, inevitably, a matter of great concern for companies – trade documents and receipts are not always legally recognised in electronic format by competent authorities\textsuperscript{241}.

Companies, as well as individuals, need to know how to precisely turn electronic data into evidence that is unimpeachable in terms of reliability. Transaction records, business records, e-mails, and any and all other records must be turned into evidence. Among other things, digital evidence may include e-mails, webpages, word processing files, data bases stored in memories of computers and servers (located in the users’ facilities or some other place that user is not aware of and can only be accessed via a URL\textsuperscript{242}), magnetic disks, optical disks and flash memory\textsuperscript{243}.

Computer systems have back-up procedures, even if only to enable rapid recovery after a disaster. Back-up archives prove to be extremely important sources of evidence as they can show if "live" files have been tampered with and can provide data which has been deleted from the "live" system\textsuperscript{244}. However, this does not solve the problem of customers wishing to present evidence in case of a dispute; servers and server software are provided by the service provider, leaving the customer in a more vulnerable position.

\textbf{6.2. (Non-)existing legal framework}

The legal framework in the European Union does not provide any specific regulation on digital evidence. Across the European Union, legislation by Member States varies. Each Member State regulates e-evidence basically by analogical interpretation of existing rules of traditional evidence. Currently, the legal domestic rules of Member States differ as well as the case law on this matter.

\textsuperscript{238} I. FREDESVINDA, "The Admissibility of Digital evidence in Court (A.E.E.C.): Fighting against High-Tech Crime—Results of a European Study"


\textsuperscript{240} Commission Staff Working Paper, Legal barriers in e-business: The results of an open consultation of enterprises

\textsuperscript{241} \textit{ibid.}, at p. 17

\textsuperscript{242} Uniform Resource Locator: an address of a web page, ftp site, audio stream or other Internet resource


\textsuperscript{244} \textit{ibid.}, p. 23-24
**Hurdles created** – The lack of a relevant legal framework for digital evidence in the European Union is a major impediment for efficient cross-border use of digital evidence. The lack of uniformity and legal criteria causes domestic regulations to very often be burdensome and poorly regulated (for instance, a lack of measures related to the authenticity of evidence or the right to data protection). Additionally, unsatisfactory and diverging jurisprudence along with the lack of relevant technical infrastructure creates further obstacles. As a result, this creates difficulties in proving the authenticity, readability, integrity and origin of electronic data, as well as the legal validity of digital evidence\(^\text{245}\).

**AEEC project** – In November 2005, a group of European multidisciplinary experts started to set out the different methods by which digital evidence is adduced in the courts of sixteen member states under the Admissibility of the Digital evidence (A.E.E.C.) project. European judges, lawyers, prosecutors, law enforcement bodies which were interviewed consider that a European legal framework on e-evidence is necessary because it will help with the legal national development of the issue and further help to develop legislations concerning e-evidence in a uniform way, especially when considering the transnational character that this type of evidence has. Moreover, it would facilitate the international cooperation between judges since, within the same country and under very similar cases there is diverging case law and a lack of homogeneity of criteria\(^\text{246}\).

As a result of the findings of the A.E.E.C. project, procedural standards were not found to include any specific procedure regulating the collection, preservation, and presentation of digital evidence in court. Nonetheless, investigators have observed how countries usually apply by analogy the general rules and procedures for the traditional evidence: 48 percent of the rules analysed contemplate procedural processes that can also be applied for digital evidence\(^\text{247}\).

Interestingly, the deep legislative review conducted under the A.E.E.C. project in sixteen Member States\(^\text{248}\) showed that there is not even an accepted definition "digital evidence". However, there are some precepts referring to "digital evidence" in some way.

For example, the Finnish legal Proceedings Code refers to "deeds that support action"\(^\text{249}\) meaning both the digital support and the paper support. A more direct reference was found in the Police & Criminal Evidence Code of the United Kingdom: "evidence is all information contained in a computer"\(^\text{250}\).

In the majority of European countries there are several definitions of e-evidence, separate for civil and criminal law, etc\(^\text{251}\). The different legislation of the European countries\(^\text{252}\) does not establish any specific definition on e-evidence, nor does it specifically regulate digital evidence. Instead, digital evidence is regulated through the analogical interpretation of traditional evidence.


\(^{246}\) The need of a European legal framework concerning Digital evidence (I. FREDESVINDA, Strategic Development Manager, CYBEX)

\(^{247}\) I. FREDESVINDA, o.c.

\(^{248}\) Austria, Belgium, Denmark, Finland, France, Germany, Greece, Holland, Ireland, Italy, Luxembourg, Portugal, Romania, Spain, Sweden, and the United Kingdom.

\(^{249}\) Legal Proceedings Code of Finland. Chapter 17, Section 11b

\(^{250}\) Police and Criminal Evidence Act, PACE

\(^{251}\) The admissibility of digital evidence in the Courts, CYBEX initiative

\(^{252}\) Study was undergone of the legislation currently in force in each of the following countries: Austria, Belgium, Denmark, Finland, France, Germany, Greece, Holland, Ireland, Italy, Luxembourg, Portugal, Romania, Spain, Sweden, and the United Kingdom
7. Conclusions

1. The eCommerce Directive has fulfilled its role of initiating cross-border electronic contracting, by imposing the principle of equal treatment of electronic contracts, by removing the legal obstacles for the use of electronic contracts, and by harmonising important aspects of electronic contracting. Nevertheless, some issues have surfaced.

2. Articles 10 and 11 impose several basic contracting requirements for online service providers. While article 10 describes the requirements to be met before the conclusion of the contract (which concern primarily information duties), article 11 describes the ordering procedure. While these requirements were answers to valid concerns at the time the eCommerce Directive was drafted, they have now either become too evident, have become a stumbling block for new technologies and business models, mainly lead to increased compliance costs and/or overly protect consumers. Furthermore, they discriminate against the offline contracting process, which is free from formalities in most cases and in most Member States. Moreover, the eCommerce Directive does not deal with real issues nowadays, such as unreadable and lengthy terms and conditions.

3. The eSignatures Directive has reached its first objective of requiring all Member States to legally recognise e-signatures. However, it has not succeeded in getting companies and consumers to actually use electronic signatures on a large scale in a day-to-day context. Major hurdles include a lack of technical interoperability and market acceptance. We therefore welcome the Commission’s Action Plan on e-signatures, which aims to offer a comprehensive and pragmatic framework to achieve interoperable e-signatures.

An unresolved issue remains the long-term validation of e-signatures. This issue also requires to be addressed on a mainly technical level rather than from a legal perspective.

4. Electronic invoicing also suffers from insufficient market adoption. Contrary to the eSignatures Directive, however, the current legal framework is at least partially responsible. The current eInvoice Directive is plagued by a lack of harmonisation, legal clarity (e.g., whether legal entities can sign invoices), diverging Member State implementations (e.g., whether qualified or advanced electronic signatures are required) and unnecessary discrimination against electronic invoices. However, the proposal for a new eInvoice Directive seems to resolve these issues.

5. The legal framework in the European Union does not provide any specific regulation on digital evidence. Across the European Union, legislation and case law by Member States in this area varies. Each Member State basically regulates e-evidence by analogical interpretation of existing rules of traditional evidence.

8. Recommendations

8.1. Article 5 of the eCommerce Directive

The European Court of Justice ruled that when a recipient of a service, after contacting the service provider by electronic means, is either on a journey, holiday or a business trip, and therefore deprived of access to the Internet, communication by an enquiry template can no longer be regarded as “effective” within the meaning of article 5.1.c of the Directive. The service provider would have to provide “access to a non-electronic means of communication”. Ultimately, the ECJ ruled that the requirements of the “direct and permanent” means of communication were not sufficiently met by an e-mail address and, as such,

online service providers must also display either a telephone number or, alternatively, a web response form that is answered in thirty to sixty minutes.

The focus of the ECJ was on consumer protection and failed to take into account that not all service providers have large business models that would allow for a permanently accessible telephone line at any time of day. Moreover, the ruling was not very clear and created additional uncertainty on how service providers should be organised in order to comply with the ruling.

In order to avoid any further (mis)interpretations of the wording in this provision, and to make this provision technology-neutral, we recommend to change article 5.c to "those electronic contact details of the service provider that are appropriate considering the nature of the information society service considered".

8.2. Article 9.2 of the eCommerce Directive

The purpose of article 9 of the eCommerce Directive is to require Member States provide equivalence for e-documents in all contractual matters, except those listed as exceptional in section 9.2. The exceptions in article 9.2 should be further analysed and reconsidered in the short term, as the Directive was drafted at a time where technologies were not in place that could offer the same level of security as the "traditional" offline solutions. If the exceptions in this provision are not removed, the message conveyed is that electronic contracting is only adequate for minor transactions. In the medium and long term, these exceptions should be removed as Member States become increasingly digitalised and trust grows in the use of technology.

Real estate – The "badge of formality" already referred to and associated to written documents may subsist with adequate implementation of technology. Real estate transactions often require that a notary be present. This third party adds to the "badge of formality" required by those involved in such transactions. However, the continued development of technology for online notarisation will likely mitigate this (e.g., the use of e-Notary applications in Estonia).

Involvement of the courts – As technology develops, and assuming that Member States will follow the current tendencies of digitising their public services, courts will likely go digital as well. As in the case of Portugal’s e-Government project, the submission of documents to the court may be done through electronic means. Therefore, in the long term we recommend this exception be removed.

Contracts of suretyship – This consumer protection provision was the result of considerable lobbying as there was a concern that if security agreements were digitised, the degree of formality which is necessary to communicate to consumers the gravity of the agreement they are entering into would be removed. Given the nature of this exception, it is recommended for the medium term that this exception be removed. A short term recommendation is not considered necessary as the inclusion of this exception in article 9.2.c.

Family and succession – Although this exception may just have been included as an act of respect for family, as technology develops and Member States digitise, family and succession services will be available electronically (divorce certificates, wills, etc.). It is recommended for the medium term that this exception be removed.

255 EULIS – European Land Information System at www.eulis.eu/countries/profile/estonia
8.3. **Article 10 of the eCommerce Directive**

The eCommerce Directive lays down minimum information standards required for electronic contracts in article 10. This provision aims to provide transparency, as well as consumer protection in online transactions, by requiring service providers to provide service recipients with the information therein. However, the wording and structure of this provision calls for further analysis and must undergo some adjustments in order to ensure it is coherent and in line with today’s reality.

**Removing article 10** – Preferably, we recommend to simply delete article 10, as its requirements have become either too evident, have become a stumbling block for new technologies and business models, mainly lead to increased compliance costs, and partially duplicate the protection measures found in other consumer directives.

When this drastic solution is not viable, we recommend to at least incorporate the following changes.

**Article 10.1.b**

The service provider must inform the recipient of "whether or not the concluded contract will be filed by the service provider". According to the wording in this information requirement, it is clear that the service provider is not required to file a copy of the concluded contract. In other words, "whether or not" indicates that it is the service provider’s prerogative to either file or not store the contract. It is common practice for service providers to keep copies of their concluded electronic transactions for their record keeping; there may be a future dispute.

In light of this common practice, service providers are better poised than consumers to maintain adequate archiving IT systems. In order to align this information requirement with the consumer protection nature of the provision, it is recommended that in the short term the wording of this provision be changed so as to require the service provider to inform the recipient that the contract has been filed and additionally inform on where it can be accessed.

**Article 10.1.d**

This provision requires service providers to provide recipients with information on "the languages offered for the conclusion of the contract". This provision, clearly drafted to ensure consumer protection, results in a redundancy. That is, when a consumer visits a website, the language of the website is most likely to be the language of the contract. This is the result of common practice for online activities. Only in the event this is not the case should service providers be required to inform recipients that the language offered in their website is not the language the contract is available in. Therefore, it is our recommendation that this provision be amended so as to require service providers to inform recipients on the languages offered, only in the event that the contract is offered in a different language.

**Article 10.2**

Paragraph 1 of this provision sets forth that the information requirements therein shall be given by the service provider to service recipients "clearly, comprehensibly and unambiguously… except when otherwise agreed by the parties who are not consumers". Paragraph 2, however, also sets forth an information requirement to provide information on "any relevant codes of conduct" to which the service provider has subscribed. In fact, both paragraphs 1 and 2 include exception on "when otherwise agreed by the parties who are not consumers". It is therefore not clear why the information requirement on codes of conduct was not included in the list of information to be provided in paragraph 1. In fact, codes of conduct, when followed by the service provider, proves to be an important piece of information that enlightens the (potential) service recipient on the rules the service provider follows.

It is therefore recommended that the information requirement in article 10.2 on codes of conduct be included in the list of information in paragraph 1 of this provision so that this information is also provided "clearly, comprehensibly and unambiguously".

**Article 10.3**

As noted in the preceding paragraph, both paragraphs 1 and 2 of article 10 include an exception to B2B contracts whereby the information requirements therein will not be applicable "when..."
otherwise agreed by the parties who are not consumers”. Although article 10 is an evident consumer protection provision, the choice was made to expressly make reference to this exception. This was not done, however, in paragraph 3 of this provision. As it is not clear, when compared to the preceding paragraphs in the provision, whether the requirement on “contract terms and general conditions provided to the recipient must be made available in a way that allows him to store and reproduce them” is applicable to consumers (B2C) or businesses (B2B), or whether this is a general requirement applicable to both, it is recommended that this paragraph be amended so as to clarify this.

Length of terms and conditions – We recommend the Commission to adopt sector-specific, concise templates of terms and conditions, and to incentive service providers to use these templates. An interesting idea would also be to create a set of “boiler plate” standard clauses, whereby the actual terms and conditions of a service provider would only need to list clauses that deviate from the boiler plate standard clauses. This would drastically reduce the length of terms and conditions. Preferably, the use of such templates would also be integrated in trustmarks.

8.4. Article 11 of the eCommerce Directive

Removing article 11 – As is the case with article 10, we recommend to simply delete article 11. However, when this solution is not viable, we recommend to at least incorporate the following changes.

Technology dependence – As the "contractual process" in the eCommerce Directive is very difficult to implement for mobile services, and may not be suitable for future technologies, it is our recommendation for the long term that the specifics of these technologies and the services they offer be taken into consideration as they may need to be governed by a separate legal framework.

Removing the confirmation requirement – Pursuant to article 11, if a service provider fails to send a confirmation to the consumer issuing acknowledgment, no contract is formed. This formality discriminates against electronic contracts, and should be removed, or at least made compatible with business models and technologies other than traditional webshops.

8.5. E-invoicing and e-archiving

E-Invoices – Taking into account the many issues that plague the current e-invoicing legal framework, we fully endorse the Commission’s new eInvoice Directive proposal. We strongly recommend its adoption.

E-archiving – As one of the most important documents in business transactions, invoices must be duly archived. Given the narrow relationship between e-archiving and e-invoicing, it is recommended for the short term that the pending Final Report of the Expert Group include harmonisation rules on e-archiving in addition to e-invoicing.

8.6. Digital evidence

Given the lack of certainty caused by the absence of a legal framework for digital evidence in the EU and the diverging rules applicable to e-discovery and e-evidence within the Member States, it is our recommendation for the short term that digital evidence be an issue of priority and the object of further study and analysis. These studies should identify the applicable rules governing digital evidence in the Member States as well as identify the necessary steps towards eliminating the current cross-border related issues.

257 See our recommendation in Chapter 13 - self regulation
In the medium term, we recommend to harmonise the digital evidence rules within the EU, because such harmonised legislation on digital evidence currently constitutes the "missing link" in the spectrum of legal instruments relating to e-contracts. All other steps found in a typical contractual process are already covered by other Directives (from the ordering process to the signature of the order and the invoicing process).
9. **Net neutrality**
# Table of contents

Chapter 9 Net neutrality ......................................................................................................................2  
1. Introduction........................................................................................................................................2  
2. The concept of net neutrality ..............................................................................................................3  
   2.1. Introduction ..................................................................................................................................3  
   2.2. Technical background ....................................................................................................................5  
3. Overview of neutrality interferences .................................................................................................7  
   3.1. Introduction ..................................................................................................................................7  
   3.2. Blocking ......................................................................................................................................7  
   3.3. Degradation ..................................................................................................................................11  
   3.4. Prioritisation .................................................................................................................................11  
   3.5. Access-tiering ...............................................................................................................................12  
   3.6. Restrictions on equipment and applications ..............................................................................14  
4. Network neutrality as a policy principle? ..........................................................................................15  
5. Existing net neutrality rules in Europe ...............................................................................................17  
   5.1. National level ...............................................................................................................................17  
   5.2. European level .............................................................................................................................18  
6. Net neutrality in the United States ......................................................................................................24  
   6.1. History .......................................................................................................................................25  
   6.2. Current policy ..............................................................................................................................26  
   6.3. Proposed legislation .....................................................................................................................26  
7. Applying existing legal solutions to neutrality interferences ..............................................................28  
   7.1. Blocking .......................................................................................................................................28  
   7.2. Degradation ..................................................................................................................................32  
   7.3. Prioritisation ..................................................................................................................................36  
   7.4. Access-tiering ...............................................................................................................................37  
   7.5. Unreasonable restrictions on equipment and applications .......................................................38  
8. Summary and overview ......................................................................................................................39  
9. Blocking illegal content ......................................................................................................................40  
10. Recommendations ...........................................................................................................................45  
   10.1. Anticipating net neutrality interferences? ...................................................................................45  
   10.2. Obligation to inform .....................................................................................................................47  
   10.3. Minimum service levels ...............................................................................................................47  
   10.4. Extended powers for national regulatory authorities ...............................................................48  
   10.5. Blocking illegal content ...............................................................................................................48  

This study was commissioned by the European Commission's Information Society and Media Directorate-General, in response to the invitation to tender OJ 2007/S 202 244659 of 19/10/2007. The study does not, however, express the Commission's official views. The views expressed and all recommendations made are those of the authors.
Chapter 9
Net neutrality

1. Introduction

a. VoIP, short for "voice over Internet protocol", is a transmission technology that allows voice telephone calls through the Internet. VoIP services are viewed as a competitive threat by telecom operators, because they enable virtually free telephone calls between Internet-connected devices, and telephone calls to landlines at drastically reduced prices. However, in 2007, UK telecom operators Orange and Vodafone removed the VoIP capability of all Nokia N95 cell phones sold by them in the UK, in what was criticised in the press as "a desperate move by the network operators to defend their voice revenue". More recently, Deutsche Telekom AG publicly stated in April 2009 that it was considering to prevent its customers from using Skype (a popular VoIP program) on the popular Apple iPhone smart phone.

b. In December 2007, national UK broadcaster BBC launched its "iPlayer" video platform. The service, which allows users to access video content from their pc, television or mobile phone, quickly gained a large audience, with more than 42 million programmes accessed in the first three months after its launch. However, the success of the iPlayer service lead to a surge in traffic for streaming video and complaints of network congestion. Ofcom, the UK telecom regulator, estimated that the costs of the broadband capacity required to support the iPlayer could in aggregate be up to £831 million over 5 years. Various UK network operators argued that the BBC should contribute to the cost of network upgrades caused by the iPlayer. Some even threatened to restrict access to the service.

c. In December 2008, the Italian Competition and Markets Authority imposed an administrative fine of 90.000 euros on Tele2 Italia, because the access provider had restricted access to certain websites and peer-to-peer applications using filtering technology, without informing its customers thereof. The Authority based its decision on the rules of unfair commercial practices, stating that the fact that consumers were not informed of the filtering must be considered deceptive. According to the Authority, consumers require such information to make an informed decision about whether to use the services in the first place.

d. In May 2009, the Belgian government launched a controversial, new anti-gambling bill. In its effort to reduce unhealthy gambling activities of its citizens, the Belgian government proposed to license a maximum of only a handful of online gambling operators that also have an offline presence in Belgium and meet the strict quality requirements of the bill. The bill also proposes to install a system to force internet access providers to block access to illegal gambling sites. While the bill is contested by the European Commission (on competition grounds), the Belgian government is determined to adopt the bill and protect its citizens against illegal gambling.

1 See www.theregister.co.uk/2007/04/18/n95_crippled/
3 See http://www.ofcom.org.uk/research/tv/bbcmias/ondemand/bbc_ondemand
4 See www.ispreview.co.uk/news/EElyAAlvAENaLVckY.html
5 Decision of the Italian Authority of Competition and Market (L’autorità garante della concorrenza e del mercato) of 18 December 2008. See www.agcm.it/agcm_it/BOLL/BOLLETTE.NSF/0ef77801432af6d1c1256a6f004d522a/1ee325f636386f8c12575430094883eb/$FILE/48-08.pdf, p. 103
The cases above illustrate that network operators can be inclined to interfere with the dataflow on the Internet for a variety of reasons. They can use their power as gatekeepers over the Internet to restrain access to competing services, prioritize their own services at the expense of their competitors, charge online service providers a premium to guarantee fast delivery of their content, or restrict the use of certain applications on their network.

Claims for "network neutrality" — "net neutrality" in short — can be seen as a reaction to the possible influence network operators could exert on their users. Net neutrality itself has been labelled as the public policy principle that all like Internet content must be treated alike and move at the same speed over the network. Although some see net neutrality as a "solution waiting for a problem" or a problem which only exists in the United States, the cases above illustrate that net neutrality issues have already emerged, also in the EU. The importance of the Internet warrants a profound debate on the way the Internet is governed and controlled, and what policy principles should apply.

This chapter therefore aspires to provide guidance in this debate.

2. The concept of net neutrality

This section provides a general overview of the substance of the net neutrality debate. It also gives a short introduction to the technical underpinnings of the Internet, insofar as relevant for the clear understanding of the issues and solutions discussed in this report.

2.1. Introduction

"messages received from any individual, company, or corporation, or from any telegraph lines connecting with this line at either of its termini, shall be impartially transmitted in the order of their reception, excepting that the dispatches of the government shall have priority"

— Section 3 of the Pacific Telegraph Act of June 16th 1860

Network neutrality is the public policy principle that all like Internet content must be treated alike and move at the same speed over the network. Although the transmission of data over telecommunications networks has since long been the subject of regulation, the net neutrality has become much more relevant in the last decade due to the everyday dependence on the Internet and the ever-growing amount of data being sent over the Internet. Generally, this data is transmitted on a best-efforts basis, regardless of what type of data is transmitted. In other words, the network is "neutral" towards the data passing through it, and does not discriminate between different types of data.

Coping with insufficient capacity — The growth of data traffic could confront network operators with a demand for network capacity which exceeds the available network capacity. Obviously, one way to deal with this discrepancy between supply and demand, is by investing in additional network capacity. Once

---

8 L. LESSIG and R.W. MCCHESNEY, o.c.
9 Hereafter, the shortened term "net neutrality" will be used to refer to network neutrality.
10 This has to be nuanced for two reasons. Firstly, the availability of some services is better in some places due to technical reasons. Secondly, large parts of the Internet cannot be accessed by some, because of government censorship.
11 Some stakeholders have therefore argued that the content providers responsible for the additional dataflow should contribute to these investments (Digital Britain interim report, January 2009, p. 22.
sufficient network capacity is again available, the issue will disappear. This solution does not trigger any
net neutrality issues, although such issue may arise when third parties would pay for the investments
and their network traffic would subsequently be prioritised over other network traffic.

Alternatively, network operators could avoid network congestion and the ensuing degradation of service
by manipulating the network dataflow. For example, advanced "deep packet inspection" technology
allows network operators to identify the type of data that is transmitted over the network, as well as its
content, and to discriminate between packets of data on the basis of this information\(^\text{12}\). This information
can then be used to shape Internet traffic\(^\text{13}\), which enables network operators to control the flow of data
over a network, giving the transfer of some data packets priority over others. Accordingly, the transfer of
data would no longer be "neutral".

**Gaining network control** – Techniques such as traffic shaping can also serve other purposes than
remedying network congestion. Access providers can use their position of Internet gatekeeper to block or
degrade content providers that are unwilling to pay for the transport of their content over the network,
regardless of any concerns over network congestion. Likewise, access providers can hinder access to
certain services in order to protect their economic interests. For example, an access provider could block
VoIP traffic on its network in order to protect its fixed or mobile telephony business.

Although access providers have an ideal position to interfere with Internet content, they are not the only
stakeholders who have an interest in such practices. For example, intellectual property owners are
reacting against copyright infractions by directing themselves at access and content providers. Public
authorities are also increasingly focusing on regulating Internet content, as exemplified by the initiatives
in various Member States to implement "blacklists" to block access to unwanted websites. All these
initiatives involve, to some extent, measures that interfere with net neutrality.

**Arguments pro and contra** – Proponents of net neutrality argue that it is the neutrality of the Internet
which ensures that the Internet remains a free and open technology that fosters innovation and
competition\(^\text{14}\). The preservation of free speech rights on the Internet has also been cited as a reason for
mandating net neutrality\(^\text{15}\). Net neutrality opponents, however, argue that legislation on net neutrality is
unnecessary, will stifle investments in new broadband services\(^\text{16}\), will result in higher prices\(^\text{17}\) and lower
quality of service, and will limit consumer choice\(^\text{18}\).

Both sides offer good arguments to the debate. In this chapter, we will try to identify the various issues
that can be grouped under the net neutrality denominator, and consider whether these issues pose a
problem in the European context.


\(^\text{13}\) Network Working Group, An Architecture for Differentiated Services, [tools.ietf.org/html/rfc2475#section-2.3.3.3](http://tools.ietf.org/html/rfc2475#section-2.3.3.3).

\(^\text{14}\) See, for example, L. LESSIG and R.W. MCCCHESNEY, Id; T. BERNERS-LEE, Net Neutrality: This is serious,

\(^\text{15}\) [http://voices.washingtonpost.com/shortstack/2009/10/antievil_free_speech_in_the.html](http://voices.washingtonpost.com/shortstack/2009/10/antievil_free_speech_in_the.html)

\(^\text{16}\) [www.washingtonpost.com/wp-dyn/content/article/2006/02/06/AR2006020601624.html](http://www.washingtonpost.com/wp-dyn/content/article/2006/02/06/AR2006020601624.html)

\(^\text{17}\) [www.ft.com/cms/s/a0/8d00c0df8-9ece-11dd-98bd-000077b07658.html](http://www.ft.com/cms/s/a0/8d00c0df8-9ece-11dd-98bd-000077b07658.html)

At the outset, it needs to be noted that the net neutrality issues in the EU are not an exact replica of the issues identified in the United States, where the net neutrality debate has started and is more extensively discussed for historic reasons.  

2.2. Technical background

To understand some of the concepts used in this report, as well as the net neutrality debate as a whole, it is necessary to understand some of the technical underpinnings of the Internet. This section 2.2 therefore sketches the technical background which is required to follow the discussions elaborated upon in the remainder of this chapter.

Interconnection of networks – The Internet consists of a large number of interconnected networks. When a consumer contracts with an Internet access provider, he becomes part of that access provider's network. The access provider's network is in turn connected to other parts of the Internet, which are typically interconnected through so-called "backbone providers". The sum of all these connected networks is called the Internet.

This decentralised structure implies that there is no "master network" that exerts control over all other networks. Instead, several networks are connected to each other, either directly or by way of intermediaries. As a result, no single access provider has control over the Internet. Access providers can act as "gatekeepers" towards their own customers, but not towards the customers of other access providers.

TCP/IP – To communicate, the computers in the network need to be able to communicate with one another, through a set of predefined communications. These protocols define a common language and a set of rules and procedures that enable devices and systems to communicate. The fundamental structure of the Internet uses a combination two protocols: the Transmission Control Protocol (TCP) and the Internet Protocol (IP), jointly referred to as the TCP/IP protocol. From a net neutrality perspective, the design of the TCP/IP protocol brings the important implication of packet switching and the end-to-end principle.

Packet switching – The TCP/IP protocol relies on packet switching technology, which is a network communications method that groups all transmitted data into blocks of data, called packets. These packets are then transmitted independently, can pass multiple intermediate "routing points" and are then assembled back into the original message at the recipient's end. As the network capacity is shared on a "packetised" basis, many communications can occur simultaneously across the network, with millions of packets from a theoretically unlimited amount of parties being transmitted at the same time.

Compared to circuit switching — a network paradigm in which a dedicated circuit is set up between two endpoints, allowing only a limited number of connections per line, with a fixed bandwidth per connection — packet switching allows cheaper network connections, as a theoretically unlimited amount of parties...
(instead of a fixed amount) can join the network. However, packet switching also introduces the possibility of net neutrality issues, as network congestions can occur when too many packets are flowing through the network at the same time.

**Packet inspection** – Each packet that is sent across the network contains a *data section* (containing the actual data being sent) and a *header section* (providing information about the source and destination of the packet, similar to how the envelope of a postal letter contains the destination address and the address of the sender). Network devices will necessarily inspect the header section of a packet to determine where the packet needs to be sent. The header section can, however, also be used by access providers to filter network traffic, for example by giving lower priority to data originating from certain senders, or by blocking data sent to specific targets.

An access provider can also filter packets on the basis of their data section, a technology called "deep packet inspection". Compared to filtering on the basis of the header section, filtering on the basis of the packet section is much more advanced and far-reaching, as the actual content of the data is being analysed. While deep packet inspection has been used for several years to maintain the integrity and security of networks (e.g., to search for viruses, spam and other threats), it is now also used to shape network traffic or to gather useful statistics about the network usage of each subscriber. Such new uses of highly contested, as they raise privacy and net neutrality issues.

**End-to-end principle** – The end-to-end principle is one of the central design principles of the Internet. The principle counsels that "intelligence" in a network must be located at the ends of the network, i.e., the devices and applications connected to the network. Rather than build into the network a complex set of functionality, the end-to-end network philosophy pushes complexity to the applications and devices that run on the network, rather than the network's core. In such design, the network infrastructure is sometimes referred to as "dumb pipes", as the network's only function is to transfer data through the network, without having the ability to interfere with the dataflow. Proponents of net neutrality argue that the end-to-end design of the Internet encourages innovation in applications for the network, because it avoids disables the network owner from interfering with the opportunity of innovation within the network. As such, it implies a principle of non-discrimination among applications and content. Abandoning this principle would bring with it the risk that the incentive to create innovate applications will diminish or disappear.

**Domain name blocking** – In addition to the way packets travel of over the Internet, it is also important to describe the way domain names functions on the Internet. In order to avoid that human beings would have to remember IP-addresses (e.g., "147.67.136.2") in order to access a certain website (e.g., "www.europa.eu"), the domain name system (DNS) was introduced, which translates each human-readable domain name to a corresponding internet address. The DNS is a hierarchical system, where a few central name servers distribute and delegate translation requests to lower-ranked servers. When the translation of a domain name is blocked at the level of one of the central servers, the website under that domain will appear blocked for most users — except for those users who would happen to know the IP-address of the domain, or who would use alternative name servers. The hierarchical nature of the DNS is

---

26 See Office of the Privacy Commissioner of Canada, *What is deep packet inspection?*, available at dpi.priv.gc.ca
29 L. LESSIG, *o.c.*, p. 111-112
30 M. A. LEMLEY, L. LESSIG, *o.c.*, p. 6
therefore an easy and attractive (although not perfect) instrument to block access to unwanted content, which avoids the need to perform expensive or difficult deep-packet inspection.

3. **Overview of neutrality interferences**

This section 3 provides an overview of the different actions (“neutrality interferences”) of access providers that can qualify as a breach of net neutrality.

Note that the legal solutions to counter these net neutrality interferences are not discussed in this section 3, but are instead discussed in section 7 below.

3.1. **Introduction**

This chapter subdivides net neutrality issues — called “neutrality interferences” in the remainder of this report — into five distinct categories.

The first category, **blocking**, refers to the situation where access providers block the transmission of certain data over the network. The second category, **degradation**, deals with slowing down the transmission of certain content. The third category, **prioritisation**, is the opposite of degradation and refers to a better treatment of certain traffic. The fourth category, **access-tiering**, relates to the case where access providers offer content providers different quality of service at different prices. The last category deals with access providers that impose **unreasonable restrictions** on running certain applications and connecting certain equipment.

3.2. **Blocking**

A first type of traffic interference that can be applied by an access provider, is the blocking of access to certain content. Blocking can be achieved by shaping the traffic using techniques such as **deep packet inspection** or by modifying DNS servers. In principle, an access provider can only exert control over the content requested by its own customers, without being able to manipulate the network operations of other access providers. Access providers can have various motives for blocking:

- they might block the transmission of data to eliminate **competition**;
- they can choose to block the transmission of data because of the **high costs** associated with the data transfer; and
- they might block the transmission of data because the data itself is **illegitimate**.

Each of these motives will be examined in greater detail hereafter.

**Blocking for reasons of competition** – One of the reasons an access provider may try to block data from one or more online content providers is because the service provider would offer a service that competes with a service provided by the access provider (e.g., online video rental services). By blocking the competing service, the access provider could leverage its presence at the content level and gain a monopoly over its customers for that service. For the same reason, an access provider could choose to

---

31 This classification is also used by P. VALCKE, L. HOU, D. STEVENS and E. KOSTA, Legal Analysis of Network Neutrality under EU Competition Rules and the Regulatory Framework for Electronic Communications, ssrn.com/abstract_id=1246642.

32 See section 2.2 above

33 by P. VALCKE, L. HOU, D. STEVENS and E. KOSTA, o.c., p. 7
block an entire class of data (e.g., VoIP traffic), thus eliminating all the content providers that depend on that class of data.

For example, in April 2009 Deutsche Telekom AG announced that it was considering to prevent customers from using Skype, a popular Voice over Internet Protocol program, on the popular iPhone smartphone. Skype can be used to call other users for free over a wireless Internet or a cellular network, and thus competes with the services of classic cellular operators.

Instead of blocking one service provider, such as Skype, an access provider could, for example, block the transmission of VoIP data, thereby affecting customers’ ability to use the services of all VoIP service providers. This type of blocking already takes place, both in Europe and the United States, where telecom provider Madison River Communication was sanctioned by the Federal Communications Commission for blocking VoIP traffic. In June 2009, Deutsche Telekom announced that it would allow VoIP applications to run on its network, albeit at an additional cost to consumers.

It is often argued that competitive pressure would deter access providers from blocking data for this reason. Although such a scenario would indeed seem unlikely on the basis of neo-classic economic theory, research shows that blocking may yield benefits, even if an access provider does not have a monopoly position. By excluding a competing service provider, the access provider can not only increase its profits in the (complementary) market of that service provider, but can also increase its secondary revenues (e.g., advertising revenues), due to the logic of pricing in the advertising markets.

Based on this theory, issues could arise even in a market that is considered competitive. Even if there is a threat that end-users would move to rival access providers who do not block any online services, various costs and obstacles (e.g., changing the e-mail address) may prevent consumers from actually switching. This conclusion is supported by the observation that some European telecoms operators are indeed planning to restrict VoIP services on their mobile networks.

Blocking due to high costs – In some cases, access providers have argued that the cost of carrying the content of certain content providers is too high. They argue that the success or the nature of certain content provider’s services can result in such a high bandwidth use that it is no longer justified to carry the content without some form of compensation.

An example is the case of BBC’s multimedia and video platform iPlayer, which saw more than 42 million programmes accessed in its first three months, leading to complaints of network congestion by network operators and even threats to restrict access to the service.

---

34 See http://online.wsj.com/article/SB123868309907582515.html
35 Users are charged for access to the network and, depending on the subscription type, for the amount of data traffic.
36 See the Orange, Vodafone and Deutsche Telekom cases.
37 The decision, which was the first enforcement of net neutrality by the FCC, can be consulted online at http://hraunfoss.fcc.gov/edocs_public/attachmatch/DA-05-543A2.pdf
38 www.gomonews.com/deutsche-telekom-lifts-mobile-voip-ban-but-charges-users-extra
40 F. CHIRICO, I. VAN DER HAAR and P. LAROUCHE, o.c., p. 29
44 www.ispreview.co.uk/news/EElyAAlytENalVVckY.html
Another example are the alleged contractual restrictions imposed by AT&T on Apple, which prohibit content-hogging applications from being provided over the 3G network. This restriction is applied worldwide through Apple’s policy on third party applications that can be installed on the iPhone through its “App store”.

This argument is part of a wider discussion between access and content providers that boils down to the question of how control over bandwidth as well as content can be valorised. On the one hand, access providers are looking for models in which they can charge content providers for carrying their content.

An executive of British Telecom stated that BT “can't give the content providers a completely free ride and continue to give the customers the [service] they want at the price they expect”. However, referring to its iPlayer video platform, the BBC has stated that it does not believe that it should pay access providers for the delivery of its content, which only makes up a small percentage of total Internet traffic in the UK.

On the other hand, content providers are exploring the possibility to charge access providers for access to their content.

For example, in the United States, the sports site ESPN360.com charges access providers for the right to give their subscribers access to ESPN360 content. This has led to protest of the American Cable Association, which claims that Internet video content providers are charging ISPs wholesale access fees to their sites “at discriminatory rates, terms and conditions”.

Although it is unclear at the moment what the outcome of this discussion will be, it is likely that these evolutions will have a considerable impact over time on the content users can access over the Internet. Therefore, close attention should be paid to the development of these new potential revenue models.

Blocking illegitimate content – An access provider may also have incentives (or be ordered) to block access to a content provider because the content breaches the law.

For example, in February 2008, a Danish court ordered access provider Tele2 to block access to the contested filesharing website The Pirate Bay. More recently, in August 2009, a Dutch court ordered all Dutch access providers to block access to the same site.

Alternatively, instead of blocking access to all the content of a specific content provider, an access provider could also block specific web pages or files, leaving the rest of the content accessible.

The eCommerce Directive’s special liability regime for online intermediaries encourages access providers to take down (possible) illegal content on its systems on their own initiative, in order to avoid liability. Access providers will also block access to illegal content upon receiving notice of the presence of illegitimate content.

---

45 See, for example "Apple weigert iPhone applicatie Uitzending Gemist", available at tweakers.net/nieuws/62265/apple-weigert-iphone-applicatie-uitzending-gemist.html. Despite the fact that Dutch telecom operator T-Mobile recommended Apple to approve a third application for watching Dutch time-shifted television shows, Apple allegedly refused this application because it operated through the 3G network.

46 See www.out-law.com/page-10109


48 See www.theregister.co.uk/2008/02/05/ifpi_pirate_bay_denmark/

49 It concerned a decision given in default, as the Pirate Bay was not represented. At the time of writing (September 2009), The Pirate Bay announced to initiate appeal proceedings to reverse the decision.

50 More often than not, the subject of blocking illegal content is not treated under the header of net neutrality. This is due to the fact that it is usually not the access provider itself who takes the initiative to block the content. For the purpose of completeness, we will deal with this subject under the same header.
of the illegal information by a third party, in order to avoid liability. In addition, some access providers voluntarily participate in projects that are aimed at blocking unwanted content.

The CSAADF (Child Sexual Abuse Anti Distribution Filter), which is developed within the framework of the EU sponsored CIRCAMP project, is a filtering system aimed at blocking access to material involving sexual abuse of minors. Since there is no legal obligation to implement the system, effective implementation of the CSAADF filtering system requires cooperation and agreements with internet access providers.

More recently, some European Member States have taken steps to implement obligatory blacklists. Such a system usually entails a list of "forbidden websites" drafted by the government. Internet access providers offering their services in the Member State are obliged to prevent access to sites on the list.

For example, in June 2009, the German Bundestag enacted a law which obliges ISP’s to restrict access to websites on a list composed by the Federal Office of Criminal Investigation. The scope of the law is limited to child pornography. The content of the list is supervised by a committee of experts, which will verify "at least every quarter, on the basis of spot checks" whether the websites on the list fall within the scope of the law.

While these blacklists usually aim to block links to illegal content (mainly child pornography), they have also been found to list content for which the illegal nature was, at least, contestable. This was, for example, the case in Finland, where a leaked list with hundreds of blacklisted domains turned out to block access to a site criticising Internet censorship. In a similar example, an Australian blacklist that was leaked on the Internet contained amongst others an anti-abortion site, a dentist clinic, gay sites, gambling sites, euthanasia activist sites, an astrologer’s blog and the website that leaked the information itself. China’s intense filtering of websites that contain politically undesirable content counts as a third example.

Although most initiatives focus on child pornography and material that promotes hatred and terrorism, there is a fear that the scope of filtering mechanisms will surpass the strictly necessary. Therefore, these initiatives have been followed with caution by rights groups, which argue that such filtering systems are at odds with the strong European tradition of democratic processes and commitment to free expression.

In Belgium, law enforcement and the administration of justice are also in the process of composing a blacklist. Although access providers would only be obliged to restrict access to a website if they receive a court order, the scope of the system is likely to be broader than that system recently enacted in Germany. Besides content involving sexual abuse of minors, it would also encompass content that offends public decency, and possibly even illegal gambling websites.

Finally, we want to point out that filtering network traffic to remove spam, viruses and other types of malware, could also be considered a type of blocking. However, provided that it concerns genuine

---

51 See section 3 of Chapter 6 - liability of online intermediaries
52 See http://circamp.eu
54 See paragraph nine of the German law
55 See https://wikileaks.org/wiki/797_domains_on_Finnish_Internet_censorship_list_including_censorship_critic_2008
56 See http://wikileaks.org/wiki/Western_internet_censorship:_The_beginning_of_the_end_or_the_end_of_the_beginning
57 See, for example, http://opennet.net/research/regions/europe
58 See the third example in the introduction of this chapter
protection, we do not qualify this type of blocking of data as a type of net neutrality interference in the remainder of this report.

3.3. Degradation

Concept – A second major type of traffic interference is traffic degradation. Instead of outright blocking traffic, an access provider could degrade access speeds to content to such a level that users would be less inclined or even refrain from using the content, effectively attaining the same result as with blocking.

Certain online services are particularly sensitive to such degradation. For example, VoIP services are delivered in real time, and are therefore time-sensitive and could be made unusable by degrading the quality with which they are transferred over the network. When the traffic for such online services is sufficiently degraded, this could have the same practical effects as blocking these services.

Two major types of degradation can be distinguished: degrading specific content (data from a certain content provider or certain class of data), and degrading all content (by giving priority to preferred content).

a) Content from a specific type or content provider – A first reason why an access provider would degrade content from a specific type or content provider, is similar to the reasons described for blocking such content. An access provider may perform such degradation to strengthen its competitive position, by promoting its own competing services. The competing services must not necessarily be provided online: an access provider could also degrade the transmission of video-related traffic in order to relax the competition against its own separate television or telephone services.

A second reason for degrading specific content, is bandwidth management, i.e. tweaking network traffic in order to avoid network congestion, or to allow time-sensitive services to get priority over other services.

An access provider could, for example, opt to degrade peer-to-peer traffic and consumer video network traffic, in order to allow its customers to use VoIP services without hiccups during network peak hours.

A recent example is Dutch access provider UPC, which limits the speed of peer-to-peer traffic as well as Usenet access when Internet traffic reaches peak levels, but does not clearly advertise these limitations. Users reported that data traffic is capped at up to 1/3 of the original speed59.

b) Degrading all content – In the second type of degradation, an access provider degrades all content, in order to give priority to preferred content without having to upgrade its network infrastructure.

For example, by presenting itself as “the fastest peer-to-peer provider” or “the best provider for YouTube addicts”, an access provider could try to target at a niche public. However, to our knowledge, no provider has yet degraded content in such way, so this remains a merely theoretical example for the time being.

3.4. Prioritisation

Prioritisation is the counterpart of degradation. Prioritisation entails that an access provider deliberately prioritises the delivery of certain data, at the detriment of other data. Prioritisation requires discriminatory effects: when these are not available, the actions of an access provider would rather qualify as “access-tiering”, discussed in the section 3.5 below.

Prioritisation according to the source of the data – In a first scenario, the access provider prioritises its own content, or the content emanating from specific third parties. As the other content is slower to access, there is once again the issue of a possible competitive advantage for the access provider.

Alternatively, access providers can discriminate in favour of their own data through the way in which they manage customer bandwidth. Most access providers impose some form of Internet traffic limitations on their customers\(^{60}\). By not applying these limitations when customers access the content (e.g. movie collection) of the access provider, providers of similar content services are being disadvantaged.

Prioritisation according to the type of data – The second scenario, prioritisation of a certain class of content, is less likely to pose problems. An access provider could choose to prioritise VoIP traffic over other content, because such traffic is very time sensitive. Without prioritisation, Internet based telephony services could be severely disturbed when the network is congested. Such network practices seem legitimate and should not by hindered by legislation. This position was also adopted by the Commission. Commissioner Reding stated that “openness for innovation sometimes cannot exclude legitimate network management practices”\(^{61}\).

Difference with degradation – Although prioritisation of some content and degradation of other content will often be applied together (particularly in a congested network), this is not necessarily the case. Some content could be degraded, while all other content would remain at the same bandwidth. Prioritisation and degradation are therefore independent of each other.

### 3.5. Access-tiering

#### 3.5.1. What is access-tiering

**Concept** – Another recurring theme in the net neutrality debate is the subject of access-tiering (also called guaranteeing "quality-of-service" / QoS). This concept refers to the practice of giving bandwidth priority, at a price independent from Internet access fees to applications, service and content providers that are willing to pay for quality of services. By auctioning or selling lanes, access providers would be able to extract additional revenue from application and service providers\(^{62}\).

Access-tiering is closely linked to managing network congestion. Without access-tiering, data is routed through the network using a best-efforts approach. The best-efforts approach implies that bottlenecks in the transmission path or network congestion will lead to data packets being held, rerouted or dropped on a random basis\(^{63}\). By implementing access-tiering, access providers would no longer transmit data on a best-efforts basis, effectively moving away from net neutrality.

In principle, when there is no scarcity in capacity, there should not be much difference between best-efforts transmission and transmission with access-tiering, as the network capacity allows to support both priority and non-priority traffic. However, when the network of an access provider that has implemented access-tiering becomes congested, delivery of packets from content providers who have paid for priority will be delivered at the expense of the packets of the non-paying providers, who will experience

\(^{60}\) Such limitations usually take the form of so-called "fair use policies" or fixed bandwidth caps over a given timespan.


\(^{62}\) KOCSIS and DE BIJL, o.c., section 2.1.

\(^{63}\) CHIRICO, VAN DER HAAR and LAROCHE, o.c., p. 43
interruptions in the delivery of their content. In particular VoIP traffic, which relies heavily on the timely delivery of packets, could be severely disrupted by the use of access-tiering.

**Differences with other issues** – Access-tiering does not imply an intention to discriminate, as every service provider who pays the requested price, can get priority on the network. Actions of access providers that do imply discriminatory intent, would rather qualify as *prioritisation*.

Access-tiering must also be distinguished from the degradation of (almost) all content\(^\text{64}\): in the latter case, content providers cannot pay for priority delivery of their content.

Access-tiering must also be distinguished from the prioritisation of data\(^\text{65}\), as access-tiering implies that every content provider who is willing to pay for it can receive premium treatment for its content.

### 3.5.2. Feasibility of access-tiering

Contrary to blocking, degrading and prioritising data, applying access-tiering is not always possible for access providers.

Access providers can only act as gatekeepers towards their own customers, but not towards the customers of access providers that have their own network\(^\text{66}\). While network architectures such as "Diffserv" and "IntServ" make it possible to engage in access-tiering in a small network, these techniques are much harder to apply on the scale of the Internet, since the access provider needs to control the entire transmission path, from source to endpoint ("end-to-end").

Access-tiering can therefore only be implemented by an access provider when it has end-to-end control over the entire transmission path. Although this situation is not very common, it can occur in the following two situations\(^\text{67}\):

- one access provider could gain control over the entire transmission process. Such a scenario could, for example, materialise at Member State level;
- access providers and backbone providers could cooperate in order to offer end-to-end quality-of-service ("QoS") guarantees to their customers.

### 3.5.3. Economic analysis of access-tiering

When approaching access-tiering from an economic perspective, the issue could be seen as a mere matter of supply and demand. An access provider sells the best quality of service to content and application providers with the highest willingness to pay\(^\text{68}\). The differences in treatment are then essentially a form of product differentiation.

As noted by the European Commission, product differentiation is generally considered to be beneficial to the market, so long as users have the choice to access the transmission capabilities and the services they want\(^\text{69}\). In addition, in a competitive market, consumers could easily switch between access

---

\(^{64}\) discussed in section 3.3  
\(^{65}\) discussed in section 3.4  
\(^{66}\) See 2.2, Technical Background  
\(^{67}\) CHIRICO, VAN DER HAAR and LAROCHE, o.c., p. 47-48  
\(^{68}\) J. G. Sidak, A Consumer-Welfare Approach to Network Neutrality Regulation of the Internet, ssrn.com/abstract=928582, p. 69  
\(^{69}\) This view was adopted by the Commission. See commission staff working document SEC(200è) 1472, p. 92
providers, possibly providing disincentives to proceed with access-tiering. However, this supposes that switching costs are sufficiently low to persuade consumers to switch.

As noted by CHIRICO et al., not much economic analysis is available on the welfare effects of access-tiering. In literature, some authors stress that access-tiering would not be beneficial to consumers, leading to a loss of innovation in the field of time-sensitive applications, increased transaction costs and a loss of consumer welfare. Opponents of access tiering argue that, particularly in a market with insufficient competition or significant switching costs, access-tiering will likely result in detrimental effects.

Lawrence Lessig described this problem by stating that “by effectively auctioning off lanes of broadband service, this form of tiering will restrict the opportunity of many to compete in providing new Internet service. For example, there are many new user generated video services on the Internet, such as Google Video, YouAre.TV, and YouTube.com. The incentives in a world of access tiering would be to auction to the highest bidders the quality of service necessary to support video service, and leave to the rest insufficient bandwidth to compete. That may benefit established companies, but it will only burden new innovators.”

3.6. Restrictions on equipment and applications

3.6.1. Concept

The final category of net neutrality issues is imposing restrictions on the use of certain applications and/or equipment by its users.

There can be various reasons for restricting the use of certain equipment or applications. A first reason could be that access providers or their affiliates may want to charge users additional fees for the use of such applications or equipment.

In 2001 in the United States, many providers put restrictions on the use of Virtual Private Networks, a technology that allows users to connect to their work network through a secure connection.

A more recent example is that several telecom operators specify in the terms & conditions for cell phone data subscriptions that users are prohibited from using their cell phone as a device to connect their personal computer to the Internet (so-called “tethering”), because such use would strain the network and would undermine the attractiveness of dedicated Internet connection subscriptions for personal computers. Although, to our knowledge, no telecom operator has yet effectively blocked such use, it is not a merely theoretical example, considering that telecom operators have already prepared their legal conditions for such move, and that the software of some devices (such as Apple’s iPhone) only allows tethering for certain telecom operators that have pre-approved tethering on their network.

In July 2009, the US Federal Communications Commission launched an investigation against computer maker Apple, because the company had rejected an iPhone application that allows users to make VoIP calls using a wireless network connection. Since this application would allow iPhone

---

76 J. G. Sidak, A Consumer-Welfare Approach to Network Neutrality Regulation of the Internet, ssrn.com/abstract=928582, p. 69


73 Apple’s response to the FCC questions can be consulted at www.apple.com/hotnews/apple-answers-fcc-questions/
users to make calls over the Internet instead of over the mobile telephony provider’s network, suspicions have arisen that Apple has blocked the application in consultation with AT&T, the sole telecommunications provider allowed to distribute the iPhone in the US.

Restrictions could also be placed in order to dissuade users from using competing services.

An access provider that offers television services to its customers could block the use of set-top boxes giving access to digital television content.

Finally, restrictions could be imposed on customers because the equipment or applications burdens the network, or threatens to cause congestion.

3.6.2. Methods of implementation

On a technical level, the restrictions could be enforced by blocking the dataflow from the unwanted equipment or applications. Such restrictions would qualify as blocking of a certain class of data.

Besides outright blocking specific applications, access providers could also place other restrictions on the use of applications, such as placing a cap on the maximum amount of application-related data that will be transferred over the network.

Such approach has, for example, been suggested as a possible action against the BBC iPlayer video platform.

Access providers can also contractually impose restrictions on their customers, without enforcing these restrictions with technical means. The use of the restricted application would then qualify as breach of contract.

An example of such a situation can be found in the restriction imposed by the German branches of T-Mobile and Vodafone on the use of VoIP and instant messaging applications. The use of these applications on these operators’ cellular network is prohibited, but currently, the companies do not engage in blocking.

4. Network neutrality as a policy principle?

European Commissioner Viviane REDING identified the openness of the Internet as one of the key principles related to the future of the Internet. In a speech in 2008, she stated:

"we will only be able to reap the full social and economic benefits of a fast moving technological landscape if we manage to safeguard the openness of the Internet. Openness is one of the key ingredients that made the Internet so successful as an innovation place, and we have to make sure that it is not compromised."

This was repeated in several other speeches:

"[P]rioritising some traffic means restricting the rest and it will be essential to remain vigilant as regards the impact this has on competition. The European Commission attaches high importance to preserving the open and neutral character of the net in Europe, in the interest of fair competition and tangible consumer benefits. (...) [T]here are many reasons for being very

---

74 See 3.2, Blocking
75 See www.independent.co.uk/news/business/news/Internet-groups-warn-bbc-over-iplayer-plans-461167.html
76 See http://online.wsj.com/article/SB123868309907582515.html
77 V. Reding, SPEECH/08/473, Net Neutrality and Open Networks – Towards a European Approach, Copenhagen, 30 September 2008
vigilant with regard to new threats to net neutrality, as they can arise in the course of market and technology developments.”

The notion of openness is vague, but should be seen in the context of the history and architecture of the Internet. The fact that there is no single gatekeeper to the network, and the “neutral” treatment of transmissions, can at least in part be seen as one of the reasons for the success of the Internet and the innovation that it has made possible, resulting in a large variety of content, applications and services.

The openness of the Internet is also a crucial condition for continued innovation on the Internet. This has been recognised by the European Commission, which identified net neutrality as one of the three key areas where it is necessary to ensure that openness remains preserved. All net neutrality issues described above (blocking, degradation, prioritisation, access-tiering and unreasonable restriction on the use of equipment and applications), imply to some extent restrictions on this openness.

However, it has been noted that openness for innovation should not exclude legitimate network management practices. Indeed, certain actions that would strictly qualify as a breach of net neutrality are not necessarily harmful, and could – on the contrary – simply result in a better quality of service for end-users. Consequently, any interventions aiming at guaranteeing net neutrality need to respect a balance between the interest of consumers and undertakings in having an Internet that supports innovation and competition, and the interest of access providers in delivering high quality service, at a price that allows them to recover investments in network infrastructure.

On this basis, we recommend the application of the following principles:

- access providers should allow their users to send and receive lawful content of their choice, to use services and run applications of their choice, and to connect hardware and use software of their choice that do not harm the network;
- if restrictions do apply, access providers should inform their users about these restrictions before selling network access subscriptions;
- access providers have the right to engage in legitimate bandwidth management in case of network congestion and when non-discriminatory bandwidth management is required for the smooth delivery of content or services; and
- regulators should monitor access providers, and intervene when their actions are discriminatory or harmful for competition or innovation.

In the remainder of this chapter we will identify the national and European legislation that can be applied to the net neutrality issues, analyse gaps in the existing legal framework, and suggest remedies based on the principles formulated in this section.

---


80 V. REDING, SPEECH/08/473, 30 September 2008

81 The prioritisation of time-sensitive traffic in times of network congestion would be an example of such a case.

82 This principle is based on the network neutrality guidelines formulated by the Norwegian Telecommunications Regulator (See www.npt.no/KnowBase/Content/109604/Guidelines%20for%20network%20neutrality.pdf), which has in turn looked at the Federal Communications Commission Policy Statement of 23 September 2005 (See http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-05-151A1.pdf). Both documents are dealt with in greater detail below.
5. Existing net neutrality rules in Europe

This section 5 provides an overview of existing legal instruments relating to (or having an impact on) the net neutrality debate, at both the national and the European level.

Note that this section 5 only provides an overview of the legal instruments that could be applied to counter neutrality interferences. It does not actually investigate to which extent each legal instrument can be effectively applied to each of the neutrality interferences identified in section 3. The application of this legislation to the specific net neutrality problems is discussed in section 7.

5.1. National level

European Union – No European Member State has yet enacted rules that specifically aim to enforce net neutrality. Up until now, the debate does not seem to be high on the national political agendas. It seems plausible that this can, at least in part, be attributed to the fact that the discussion is currently taking place at the European level, within the framework of the telecommunications package reform.

In the United Kingdom, for example, net neutrality legislation has been explicitly dismissed by the Department for Culture, Media and Sport and the Department for Business, Enterprise and Regulatory Reform. In their "Digital Britain" report of January 2009, it is stated that "the Government has yet to see a case for legislation in favour of net neutrality". It is argued that allowing network operators to offer guaranteed service levels to content providers in exchange for increased fees could lead to differentiation of offers and promote investment in higher-speed access networks. The report therefore states that, unless the national regulator would find some access providers to have significant market power — which would justify intervention on competition grounds — traffic management will not be prevented.

Norway – In 2006, Norway (a member of the European Economic Area) was confronted with a dispute relating to net neutrality, when broadband provider NextGenTel decided to limit the bandwidth available to the website of NRK (the Norwegian state broadcaster), which the operator said was generating excessive traffic caused by its subscribers streaming free Internet TV.

In response, network neutrality guidelines were drafted in 2009 by the Norwegian Post and Telecommunications Authority, in collaboration with Internet service providers, content providers, consumer protection agencies and industry organisations. The guidelines are derived from the US FCC policy statement (see section 6.1).

In these guidelines, the Norwegian regulator establishes the three network neutrality principles. According to these principles, Internet users are entitled to an Internet connection with a predefined capacity and quality, that enables them to send and receive content of their choice, use services and run applications of their choice, and connect hardware and use software of their choice that do not harm the network. The principles also entitle Internet users to an Internet connection that is free of discrimination with regard to type of application, service or content or based on sender or receiver address.

It should be noted, however, that the guidelines do not have a formal legal status, and cannot be used as a basis to issue sanctions.

84 See http://minimba.eventscope.co.uk/templates/000210/view1.html
85 See www.npt.no/IKnowBase/Content/109604/Guidelines%20for%20network%20neutrality.pdf.
5.2. European level

As is the case with the national level, no specific European legal instruments deal with the issue of net neutrality.

Even so, some existing legal instruments can be used to deal with some of the issues that are part of the net neutrality debate. In particular, EU competition law may serve a role here for access providers that have a dominant position.

The net neutrality debate has also surfaced as part of the wider issue of regulating telecommunications services. Existing telecommunications regulation provides some tools – such as the significant market power regime – that may be applicable to net neutrality issues.

5.2.1. General competition law

Article 82 – A considerable number of possible neutrality interf erences can be used to eliminate or reduce competition. Consequently, such anti-competitive behaviour may be sanctioned under general European competition law. Anti-competitive behaviour by a single access provider will under certain conditions allow to be dealt with under article 82 EC Treaty, which states that "any abuse by one or more undertakings of a dominant position within the common market or in a substantial part of it shall be prohibited as incompatible with the common market insofar as it may affect trade between Member States". In addition, since the competition laws of most Member States are closely in line with European competition law, similar provisions will apply in case of abuse of a dominant position that is limited to the national market.

Dominant position – A significant hurdle in the application of article 82 and its national equivalents to net neutrality interferences is that it requires a dominant position within the common c.q. national market, or in a substantial part of it. Dominance is a position of substantial economic power, held for a period of time by a firm over its competitors, customers and/or suppliers in the market, which enables the firm to impede effective competition. Its assessment requires an ex post economical analysis, taking into account the product market, geographic market and the so-called "temporal factor".

Evaluation – The criterion of the dominant position may present difficulties in practice to tackle net neutrality issues at the European level. Due to early regulatory intervention, the EU retail market is fairly competitive. The introduction of local "loop unbundling" in 2000 aimed at enhancing competition, ensuring economic efficiency and bringing maximum benefit to users. This enhancement of competition makes it less probable that an access provider would be found to have a dominant position on the retail market, which would in turn rule out the application of article 82 to net neutrality issues. However, in such case, national competition law could still apply.

---

86 i.e. blocking, degrading, prioritising and placing unreasonable restrictions on the use of certain applications
89 The temporal factor is the estimated time for which a certain undertaking may dominate the market.
92 According to the Q3 ECTA Broadband Scorecard, 44% of all DSL lines are supplied by competitors of the incumbent. See www.ectaportal.com/en/basic650.html
The "local loop" connects a user to a DSL telecommunications provider infrastructure. Since the telecommunications infrastructure was typically owned by the incumbent, these local access networks were one of the least competitive segments of the liberalised telecommunications market. Local loop unbundling forced incumbents to share the infrastructure with competitors.

5.2.2. Significant market power regime


The Framework Directive establishes a procedure which allows the relevant national regulatory authorities to determine whether a specific telecommunications market is competitive. If it determines that such a market is not effectively competitive, the national regulatory authority must define undertakings with significant market power (“SMP”) on that market. The definition of SMP is identical to the standard definition of "dominance", as determined and repeated by the European Court of Justice. The principles to be used by national regulatory authorities to determine whether an undertaking has SMP, are set forth in the "Commission Guidelines on market analysis and the assessment of significant market power under the Community Regulatory Framework for electronic communication networks and services".

The Access Directive and the Universal Service Directive set forth a number of obligations which can be imposed by the national regulatory authority on undertakings which are considered to have SMP on a specific market. The Commission has the possibility to define trans-national markets, in which case the national regulatory authorities must coordinate their efforts. In contrast to European competition law,

93 DSL (digital subscriber line), is a technology that allows data transmissions over the telephone network.

94 Regulation (EC) No. 2887/2000, recital 4

95 There was no similar intervention for cable-based Internet services.


102 Article 16 Framework Directive

103 Article 16.4 Framework Directive


105 Article 15.4 Framework Directive

the SMP regime allows national authorities greater flexibility to deal with national circumstances, using
tools which are tailored to the telecommunications sector, thus rendering the regime potentially more
useful to deal with net neutrality interferences. Also, while the analysis of dominance in general EU
competition law occurs ex post, the presence of SMP is analysed ex ante by the national regulatory
authorities.

**Relevant market** – In assessing whether an undertaking has SMP, the "relevant market" in which an
undertaking operates must first be determined. When making this assessment, national regulatory
authorities must take into account the list of relevant markets identified by the Commission. This list
does not include retail broadband markets, which implies that national regulatory authorities that want to
regulate a market under SMP rules need to pass a three criteria test. These criteria are as follows:

- the market must have high and non-transitory entry-barriers;
- the market does not tend towards effective competition within the relevant time horizon; and
- the application of competition law alone would not adequately address the market failure(s) concerned.

These criteria pose significant difficulties to national authorities that want to regulate the retail broadband
market. Thus far, no national regulatory authorities have submitted their retail broadband market to the
three criteria test, so that the application of the SMP regime to net neutrality issues might at this point be
rather theoretic.

**Possible obligations to be imposed** – If a national regulatory authority would succeed in proving that a
relevant market is not effectively competitive, it can identify undertakings with SMP within that market and
impose specific regulatory obligations.

The first set of obligations applies to the relationship between network operators. The Access
Directive (articles 9 - 13) lists a number of obligations that can be imposed on companies with SMP in
their relations with other market players. These obligations include transparency, non-discrimination,
separate accounting, mandatory access, and cost-oriented pricing. Some argue that the transparency
obligation and the non-discrimination obligation, which can be imposed with respect to price and non-
price dimensions of access, are suited to deal with net neutrality issues. However, the lack of inclusion
of retail broadband markets in the list of relevant markets identified by the Commission, and the fact that
the regulatory remedies under the Access Directive are confined to regulating the relationship between

---

107 As mentioned above, the relative competitiveness of the European telecom market makes it improbable that an access
provider would be found to have a dominant position on the retail market, which would in turn rule out the application of
article 82 to net neutrality issues. In such case, national competition law could still apply.
108 See recital 34 of EC 2002
within the electronic communications sector susceptible to ex ante regulation in accordance with Directive 2002/21/EC of the
European Parliament and the Council on a common Regulatory Framework for electronic communications networks and
services, O.J. L 344/65
within the electronic communications sector susceptible to ex ante regulation in accordance with Directive 2002/21/EC of the
European Parliament and the Council on a common Regulatory Framework for electronic communications networks and
services, O.J. L 344/65
111 P. VALCKE, L. HOU, D. STEVENS and E. KOSTA, o.c., p. 14
the Pipe, You Call the Tune: The Net Neutrality Debate and Its (Ir)relevance for Europe”, CEPS, 2008, available at
ssrn.com/abstract=1291027, p. 23;
network operators casts serious doubt upon these arguments\textsuperscript{113}.

A second set of obligations can be applied to the relationship between the SMP-company and its end-users. These obligations are set forth by articles 17 - 19 of the Universal Service Directive, and include applying retail price cap measures, measures to control individual tariffs, measures to orient tariffs towards costs or prices on comparable markets and obligations regarding the provision of a minimum set of leased lines. Regardless of the problems surrounding market definition, these tools seem ill-suited to deal with net neutrality issues.

**Evaluation** – In the context of dealing with net neutrality issues, the application of the SMP regime has the same shortcoming as general EU competition law: the regime cannot be applied to market players who are not dominant on the relevant market. In addition, in their current form, the regulatory remedies available under the Access and Universal Service Directives seem to be of limited use in dealing with net neutrality issues. It should be noted that at the time of writing, updates to the regulatory framework are being discussed between the Parliament, the Commission and the Council.

5.2.3. **The general interconnection regime**

In addition to the measures available under the SMP regime, article 5 of the Access Directive grants national regulatory authorities the power to impose interconnection obligations on undertakings that control access to end-users, to the extent such is necessary to ensure end-to-end connectivity\textsuperscript{114,115}.

Article 5 of the Access Directive is primarily designed to deal with situations where network operators would deny other operators access to their networks. However, the wording of article 5 assigns a considerable amount of discrentional power to national regulatory authorities to handle national circumstances in order to ensure end-to-end connectivity, as it refers to “undertakings that control access to end-users”. The Access Directive does not define this concept, but it seems suitable for dealing with at least some of the neutrality interferences, particularly because recital 6 refers to the case where “network operators were to restrict unreasonable end-user choice for access to Internet posts and services” as an example of a situation in which the obligation of article 5, 2° (a) could apply.

Consequently, the general interconnection regime might be of use in resolving neutrality interferences. However, it should be taken into account that the general interconnection regime was not specifically designed to deal with net neutrality, and that at least some amount of interpretation by national courts would be required to bring the issues described above under the scope of the regime. Consequently, in view of the sometimes limited clout of the national regulatory authorities, it is not unlikely that the use of the interconnection regime in resolving net neutrality interferences will be limited in practice.

\textsuperscript{113} P. VALCKE, L. HOU, D. STEVENS and E. KOSTA, o.c., p. 14

\textsuperscript{114} Article 2 (b) Access Directive defines interconnection as “the physical and logical linking of public communications networks used by the same or a different undertaking in order to allow the users of one undertaking to communicate with users of the same or another undertaking, or to access services provided by another undertaking. […]”

\textsuperscript{115} Article 5, 2° holds: “In particular, without prejudice to measures that may be taken regarding undertakings with significant market power in accordance with Article 8, national regulatory authorities shall be able to impose: (a) to the extent that is necessary to ensure end-to-end connectivity, obligations on undertakings that control access to end-users, including in justified cases the obligation to interconnect their networks where this is not already the case: […]”
5.2.4. **Universal Service Directive**

**Current legislation** – One of the goals of the Universal Service Directive is to ensure "the provision of a defined minimum set of services to all end-users at an affordable price."\(^{116}\). However, the scope of the universal service obligation is **limited to fixed telephony services** and does not include broadband services, which makes it unsuitable to deal with net neutrality issues. The same applies to the consumer protection rules laid down in this Directive. For example, the Directive imposes an obligation to inform consumers of the "services provided, the service quality levels offered", an obligation which could be useful in a net neutrality context. However, in view of the limitation of the scope of to "providers of access to public telephone networks", in its current form, the Directive is ill-suited to deal with net neutrality interferences\(^ {117}\). Although a review of the scope of Universal Service Directive in 2005 concluded that there was no need to extend the scope of the Directive to broadband services, the Universal Services has been cited as one of the legal instruments that, with the necessary modifications, could play a central role in regulating net neutrality\(^ {118}\)\(^ {119}\).

**Review of the Universal Service Directive** – In its 2006 review of the EU Regulatory Framework for electronic communications networks and services, the Commission acknowledged the need for a fundamental reflection on the role and concept of universal service in the 21\(^{st}\) century. In particular, the fact that many of the provisions in the Universal Service Directive are linked to traditional telephone services was deemed to require modernisation\(^ {120}\).

If approved, the proposed amendments to the Universal Service Directive will make it a more suitable instrument to deal with net neutrality issues\(^ {121}\). The proposal contains updated provisions relating to information, transparency and quality of service\(^ {122}\). The updated provision regarding **information** obliges access providers to include information on conditions limiting access to and/or use of services and applications, minimum service quality levels and measures taken to limit and manipulate the flow of data over their network in their contracts\(^ {123}\). With regard to **transparency**, access providers will be obliged to inform customers about changes to conditions limiting access to and/or use of services and applications and procedures put into place to measure and shape traffic\(^ {124}\). In addition, the national regulatory

\(^{116}\) Recital 4 Universal Service Directive  
\(^{117}\) Article 20, 3\(^{(b)}\) Universal Service Directive  
\(^{118}\) COM (2005) 203, Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions on the Review of the Scope of Universal Service in accordance with Article 15 of Directive 2002/22/EC  
\(^{119}\) A. RENDA, o.c., p. 32  
\(^{120}\) COM (2006) 033, Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions on the review of the EU Regulatory Framework for electronic communications networks and services.  
\(^{121}\) At the time of writing, the proposal has been approved with amendments in the second reading by the European Parliament and is awaiting second reading by the Council.  
\(^{123}\) Proposed article 20 of the Universal Service Directive  
\(^{124}\) Proposed article 21, 3 of the Universal Service Directive
authority are granted the power to impose minimum quality of service requirements on access providers\textsuperscript{125}.

### 5.2.5. Roaming Regulation

In June 2009, the existing Roaming Regulation was amended in order to further lower consumer prices and develop the market for cross-border telecoms services\textsuperscript{126}. The Roaming Regulation states that there should be no obstacles to the emergence of applications or technologies which can be a substitute for, or alternative to, roaming services, such as WiFi, Voice over Internet Protocol (VoIP) and Instant Messaging services\textsuperscript{127}. Although the Regulation does not contain any concrete obligations to treat data indiscriminately, Information Society Commissioner Viviane Reding has threatened to brandish the Roaming Regulation in order to prevent telecoms operators from blocking alternative communication services on their mobile network\textsuperscript{128}.

### 5.2.6. Data Protection Directive and ePrivacy Directive

Actively monitoring the actual network traffic of individual users (particularly with technologies such as deep packet inspection\textsuperscript{129}) may infringe both the Data Protection Directive and the ePrivacy Directive, unless prior consent is obtained from the individual users:

- Article 5.1 of the ePrivacy Directive requires Member States to ensure the confidentiality of communications and traffic data, and to prohibit listening, tapping, storing and other kinds of interception and surveillance without the user’s prior consent. The only exception relates to the technical storage of traffic data that is necessary for the conveyance of communications.

  Analysing the details of a user’s traffic data for purposes such as packet shaping may be considered to infringe this article 5.1, as such analysis is not necessary for conveying communications in many situations\textsuperscript{130}.

- Article 7 of the Data Protection Directive requires data controllers to rely on one or more lawful grounds to process personal data. Considering that personal data is interpreted in a very broad way\textsuperscript{131}, traffic data may also constitute personal data. Consequently, access providers will require a lawful ground to process traffic data.

\textsuperscript{125} Proposed article 22, 3 of the Universal Service Directive


\textsuperscript{128} Document E-3125/09EN of 7 June 2009, answer by Viviane Reding on behalf of the Commission on a written question, see www.euractiv.com/29/images/Answer%20from%20Reding_tcm29-184143.doc

\textsuperscript{129} See section 2.1 above

\textsuperscript{130} A similar issue was also raised by the voluntary Japanese guidelines for packet shaping: see www.jaiipa.or.jp/other/bandwidth/guidelines_e.pdf, p. 5.

\textsuperscript{131} See Chapter 4 - privacy and data protection, with respect to the interpretation of the Data Protection Directive. The ePrivacy Directive also considers the recording of communications to be processing within the meaning of Directive 95/46/EC: see recital 23.
Although the legal ground of "necessity for the performance of a contract with the data subject" (article 7.b) is suitable for the normal processing of traffic data, this legal ground may not be suitable for activities such as deep packet inspection, which are not necessary for performing the contract with the data subject (i.e., the subscriber).

Another possible legal ground for processing may be the necessity for the "legitimate interests" pursued by the access provider (article 7.f). However, reliance on this article requires that the legitimate interests of the access provider are not overridden by the fundamental rights and freedoms of the data subjects. In general, data protection authorities are hesitant to allow reliance on this article in borderline cases. When technologies such as deep packet inspection would be used for mere economic purposes, then the fundamental rights and freedoms of the data subjects could arguably take precedence over the mere economic interests of the access provider. Reliance on article 7.f as a lawful ground for activities such as deep packet inspection may therefore be problematic, particularly when taking into account that a user’s actual traffic data may perhaps also be considered to include "sensitive data," for which article 7.f cannot be used at all.

Consequently, the only lawful ground that is guaranteed to be legally sound in this context, is the unambiguous, prior consent of the data subject (article 7.a).

Article 10 of the Data Protection Directive requires the access provider to duly inform users of the traffic inspection that is being applied by it. However, the Data Protection Directive does not indicate how this information should be provided in practice (through a privacy policy, prominent notice, in the general terms & conditions, ...).

It should be noted that not all net neutrality interferences are problematic according to the Data Protection Directive and ePrivacy Directive. For example, when the access provider would block data by simply closing one or more "ports" on its network, or modifying its DNS servers, then no user traffic data actually needs to be inspected, so that the confidentiality and data processing concerns outlined above would not apply. The same would generally apply to any technology which does not actually inspect a user’s data.

6. Net neutrality in the United States

This section discusses how the case law and legislation of the United States deal with the topic of Net Neutrality.

132 See also Opinion 118 of Working Party 29 on privacy issues related to the provision of email screening services (available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp118_en.pdf), which investigates when access providers can lawfully inspect email traffic. The Working Party argues that such inspection is allowed for anti-virus and anti-spam purposes, as such inspection could fall under (1) the "legal obligation" (article 7.c) lawful ground of the Data Protection Directive, because article 4 of the ePrivacy Directive requires access providers to guarantee the safety of their network; and (2) the "necessity for performance of a contract with the data subject" (article 7.b) lawful ground, as subscribers contractually expect email traffic without viruses / malware. Conversely, the Working Party is of the opinion that, without the prior consent of the subscriber, access providers cannot engage in filtering, storage or any other kind of interception for purposes of screening emails for detecting other predetermined content (such as general illegal material).

133 E.g. the IP address of a website dealing with medical or religious issues.

134 for example when the interference would be limited to the communication path between the access provider and a service provider.
6.1. History

The net neutrality debate has its origins in the United States, and is closely connected with the local market situation. Although authors had written about net neutrality before, the debate only began in earnest in 2005, after the Supreme Court’s decision in the "Brand X" case, which has had a significant impact on the American market situation.

Brand X case – In Brand X, the Supreme Court overturned a federal court decision that forced cable companies to act as a common carrier, sharing their infrastructure with Internet service providers such as Brand X. Inspired by the Brand X decision, the Federal Communications Commission (FCC) levelled the playing field by also exempting DSL from common carrier regulations. As a result, contrary to the situation in the EU, broadband unbundling rules are nonexistent in the United States. In the United States, the market for broadband is mainly divided between cable and ADSL services, with the former taking up 53 percent of the market, and the latter accounting for close to 34 percent of the market.

2005 FCC policy statement – As a reaction to concerns that these evolutions could lead to closed broadband networks, the FCC adopted a non-binding policy statement in 2005, which contains four principles aimed at ensuring “that providers of telecommunications for Internet access or Internet Protocol-enabled (IP-enabled) services are operated in a neutral manner.” To encourage broadband deployment and preserve and promote the open and interconnected nature of the public Internet, consumers are entitled to:

- access lawful Internet content of their choice;
- run applications and use services of their choice (subject to the needs of law enforcement);
- connect lawful devices of their choice that do not harm the network; and
- competition among network providers, application and service providers, and content providers.

The principles laid down in the policy statement were used as a guideline by the FCC in merger approvals. On October 31, 2005, the FCC approved the mergers of SBC Communications with AT&T, and Verizon with MCI. Each of the merged companies agreed for two years to conduct business in a manner that complies with the principles set forth in the FCC’s Internet policy statement, in which the FCC claimed jurisdiction to enforce provisions regarding neutral Internet access. In addition, the president of the United States Telecom Association, who counts AT&T and Verizon among its more than 1200 member companies, has pledged in a Senate testimony that consumers will continue to visit any legal website without being blocked, without their service being impaired or degraded.

---

136 Supreme Court of the United States, National Cable & Telecommunications Association et al. v. Brand X Internet Services et al., June 27, 2005
141 See the Senate testimony at http://commerce.senate.gov/public/_files/McCormick061306.pdf.
6.2. Current policy

Up until today, net neutrality remains a debated topic in the US. In August 2008, reports that cable access provider Comcast was interfering with file-sharing traffic led to a decision of the FCC in which Comcast was ordered to stop this practice. Comcast complied with the decision, and replaced the existing traffic control mechanisms with a “bandwidth agnostic” system. It also lodged an appeal on the grounds that FCC lacks the authority to enforce any ruling on Comcast. The outcome of this appeal is expected to determine the FCC’s position in the US net neutrality debate. In August 2009, Julius Genachowski, the FCC chairman, confirmed the FCC’s intent “to keep the Internet free of increased user fees based on heavy Web traffic and slow downloads.”

Following this statement, in October 2009, the FCC adopted a notice of proposed rulemaking which adds two additional principles to the ones contained in its 2005 policy statement. According to the notice, access providers also have to:

- treat lawful content, applications, and services in a nondiscriminatory manner; and
- disclose information concerning network management and other practices in order to ensure that users and service can enjoy the benefit of net neutrality of the other principles.

It should be noted that the FCC’s policy principles are without prejudice to “reasonable network management.” However, the FCC has been criticized for the ambiguity of its definition of reasonable network management.

The FCC policy statement proposes to codify its six policy principles into law. At present, these principles do not have the status of binding rules, although the FCC has stated that it will “incorporate the above principles into its ongoing policymaking activities.”

6.3. Proposed legislation

Several bills have been proposed with regard to net neutrality on the federal level, but none have yet been enacted into law.

May 2006 bill – For example, on 16 May 2006, republican politicians introduced the “Internet Freedom Preservation Act”. The bill explicitly aims to amend the Communications Act of 1934 in order to ensure net neutrality, and imposes several obligations on broadband providers. Besides a general obligation not to interfere with the use of the broadband service by its users, the text imposes upon broadband providers the obligation to refrain from obstructing a user from attaching any device to the network and to...

---

143 The original traffic management system only interfered with traffic using the bittorrent protocol, a set of instructions for transferring data (such as the TCP/IP or the VoIP protocol) that is used for peer-to-peer file sharing. The new system aims to manage bandwidth use regardless of the used protocol.
146 See FCC notice of proposed rulemaking, nr. 135. “Reasonable network management consists of: (a) reasonable practices employed by a provider of broadband Internet access service to (i) reduce or mitigate the effects of congestion on its network or to address quality-of-service concerns; (ii) address traffic that is unwanted by users or harmful; (iii) prevent the transfer of unlawful content; or (iv) prevent the unlawful transfer of content; and (b) other reasonable network management practices.”
147 See www.sfgate.com/cgi-bin/article.cgi?f=/g/a/2009/11/03/urnidans002570F3005978D8885257963005E0F76.DTL
148 See FCC notice of proposed rulemaking, nr. 30 and 88
allow the offering of lawful content, applications, or services. Prioritisation is only allowed based on the type of content, applications, or services and the level of service purchased by the user, and cannot be charged for. The bill never made it to the Senate.

**February 2008 bill** – Another bill, entitled the “Internet Freedom Preservation Act of 2008” was introduced on 11 February 2008. It aimed “to establish broadband policy and direct the Federal Communications Commission to conduct a proceeding and public broadband summit to assess competition, consumer protection, and consumer choice issues relating to broadband Internet access services, and for other purposes.” The bill seeks – amongst others – to amend the Communications Act of 1954 with a section dealing with broadband policy. The first point of the proposed broadband policy states that it is the policy of the United States:

> “to maintain the freedom to use for lawful purposes broadband telecommunications networks, including the Internet, without unreasonable interference from or discrimination by network operators, as has been the policy and history of the Internet and the basis of user expectations since its inception”

However, this bill was also not enacted during the session of Congress in which it was introduced, and thus never became law. There is speculation that future bills could make it into law, as the current administration seems to have a more favourable opinion towards net neutrality, but opposition to the bills stays significant.

**July 2009 bill** – On July 30, 2009, democratic politicians introduced the “Internet Freedom Preservation Act of 2009.” The underlying idea of the bill is that access providers have an economic interest to discriminate in favour of their own services, content and applications, and that a network neutrality policy is essential to ensure that the Internet’s services remain open. The bill, which would amend the Communications Act of 1934, imposes several new obligations on Internet Access Services Providers, including the obligation not to block, interfere with, discriminate against, or degrade the ability of a user to engage in lawful activity on the Internet. In addition, access providers would be prohibited from charging additional fees for accessing specific Internet content or services, and are obliged to allow users to connect non-harmful devices to the network. If enacted, the bill would allow any US Internet user to file a neutrality complaint with the FCC and receive a ruling within 90 days.

**October 2009 position** – It was mentioned above that, in October 2009, the FCC issued two new net neutrality principles and proposed to codify its six policy principles into law. In accordance with the notice of proposed rulemaking, stakeholders have the possibility to submit comments and reply-comments until March 5, 2010. As the adoption of open Internet and net neutrality rules has been stressed as a top priority by the Obama administration, final rules could be in place somewhere in the

---

149 The full text of the bill can be consulted at www.publicknowledge.org/pdf/s2917-109.pdf.
151 The full text of the bill can be consulted at thomas.loc.gov/cgi-bin/bdquery/z?d110:H.R.5353:
153 See, for example, www.reuters.com/article/marketsNews/idINN1337119020081113?rpc=44
154 See http://euobserver.com/19/27859.
155 The full text of the bill can be consulted at www.publicknowledge.org/pdf/111-hr3458-20090731.pdf.
157 Proposed section 12 (h) 2 of the Internet Freedom Preservation Act of 2009.
158 See Section 6.1.
159 FCC notice of proposed rulemaking, p. 1.
second half of 2010\textsuperscript{160}. However, several issues – such as the ambiguity of the definition of "reasonable network management" – will likely be the subject of much discussion.

7. Applying existing legal solutions to neutrality interferences

This section 7 applies the European legal framework outlined in section 5.2 above to the net neutrality issues discussed in section 3, identifies gaps in the existing framework and formulates policy recommendations.

As the existing legal instruments are applied to each of the neutrality interferences, this section 7 mimics the structure of section 3.

7.1. Blocking

The first neutrality interference that will be studied, is the blocking of data of one or more content providers\textsuperscript{161}. As explained above, an access provider may have several reasons for blocking the dataflow on its network. The access provider may, for example, want to block the data of a content provider because it offers a competing service, or because the data of this content provider takes up too much bandwidth (leading to high costs for the access provider). The access provider may, for similar reasons, also consider blocking an entire class of data.

**Competition law** – A first remedy for those cases where a content provider's data is blocked because the access provider offers a competing service, may be found in EU and national competition law.

Competition law prohibits a dominant undertaking from discriminating in favour of its subsidiary on the market\textsuperscript{162}. This would, for example, be the case when a dominant access provider would block a video hosting website that competes with its own video content platform. This has been explicated by the European Commission in its Notice on Access Agreements in the telecommunications sector\textsuperscript{163}.

However, since art. 82 and its national equivalents only prohibit discrimination taking place on the "relevant market" concerned, dissimilar treatment among different relevant markets will not qualify as an abuse\textsuperscript{164}. Consequently, depending on the market definition, competition law might not provide a solution if an entire class of data (such as VoIP traffic) is blocked, although such an action would result in the blocking of all content providers handling that type of data.

**Essential facilities doctrine** – In principle, competition law can also be applied outside discrimination cases, for example when an access provider blocks a content provider's data because of the high bandwidth consumption. The "essential facilities doctrine" \textsuperscript{165} – which does not have a formal legal basis but was established by case law – does not allow a company with a dominant position in the provision of an essential facility, to refuse other companies access to that facility without objective justification\textsuperscript{166}. The

\textsuperscript{160} See for example www.wired.com/epicenter/2009/03/obama-nominates and www.broadcastingcable.com/article/277425-Obama_Committed_to_Network_Neutrality.php

\textsuperscript{161} Please note that the subject of blocking of illegal content is dealt with below. See section 9.

\textsuperscript{162} CHIRICO, VAN DER HAAR and LAROUCHE, o.c., p. 31-32

\textsuperscript{163} Notice of 22 August 1998 on the application of the competition rules to access agreements in the telecommunications sector, O.J. C 265/2, para. 126.

\textsuperscript{164} P. VALCKE, L. HOU, D. STEVENS and E. KOSTA, o.c., p. 7

\textsuperscript{165} P. VALCKE, L. HOU, D. STEVENS and E. KOSTA, o.c., p. 5

network of an access provider could indeed be seen as an essential facility for content providers, who need the network to bring their content to their customers.

In the Microsoft case, the Court of First Instance rephrased the conditions that need to be fulfilled to apply the essential facilities doctrine\textsuperscript{167} \textsuperscript{168}:

- the refusal must relate to a product or service that is indispensable to the exercise of a particular activity on a neighbouring market;
- the refusal excludes any effective competition on the neighbouring market;
- the refusal cannot be objectively justified.

It is unclear whether these three criteria will be fulfilled in cases where an access provider blocks data from one or more specific content providers.

The first condition seems to be met: the market of Internet content services and the market of retail broadband services are \textit{neighbouring markets}, and the provision of access to the broadband service is \textit{indispensable} for the content provider to deliver its services.

It is less clear, however, whether the second condition (excluding effective competition) is met: due to the competitiveness of the European market, it will be hard to establish that the access provider's blocking will exclude any effective competition on the neighbouring market\textsuperscript{169}. It is equally unclear whether an access provider can demonstrate that the refusal can be objectively justified\textsuperscript{170}. Since this criterion has been narrowly interpreted in the past, mostly being confined to security reasons and protecting the integrity of the services at hand, it has been argued that a refusal could be deemed justified if it is necessary to protect against threats such as malware or DoS attacks\textsuperscript{171}. Consequently, it is unclear whether the essential facilities theory can be used to remedy blocking without the intent to discriminate a subsidiary on the content market. Furthermore, it should – again – be borne in mind that there are currently few network operators that have a dominant position on the internal market, so that even when the three conditions would be met, they can only be used against a few dominant network operators.

\textbf{SMP regime} – It was noted above that the application of the SMP regime is fraught with difficulties, as the retail broadband market is not recognised by the European Commission as one of the relevant markets on which the SMP regime can be applied\textsuperscript{172}. However, if the retail broadband market would be identified as constituting a relevant market, or national regulatory authorities manage to pass the three criteria test, the regime could also be used to deal with blocking.

A first measure that can be imposed under the SMP regime when an SMP access provider blocks data to discriminate, is set forth by article 10, 2° of the Access Directive. This article allows authorities to impose obligations of non-discrimination in relation to interconnection and/or access. This article might thus be applied to force an access provider to provide access to one or more content providers.

\textsuperscript{167} ECJ, Case T-201/04 Microsoft vs. The Commission, 17 September 2007.

\textsuperscript{168} With regard to the supply of an intellectual property right, an extra condition needs to be fulfilled. In addition to the three criteria described above, the refusal must also prevent the appearance of a new product for which there is a potential demand.

\textsuperscript{169} CHIRICO, VAN DER HAAR and LAROUCHE, o.c., p. 38; P. VALCKE, L. HOU, D. STEVENS and E. KOSTA, o.c., p. 5-6

\textsuperscript{170} P. VALCKE, L. HOU, D. STEVENS and E. KOSTA, o.c., p. 6

\textsuperscript{171} A. RENDA, o.c., p. 21

\textsuperscript{172} See 5.2.2, Significant market power regime
However, as pointed out above, it is unclear how this would work in practice, as the primary purpose of article 10, 2° is to regulate the relationship between network operators.

In addition, article 12 of the Access Directive allows authorities to give third parties access to specified network elements and/or facilities of an SMP access provider, when not allowing access would not be in the end-users interest. While this article might also be relevant to deal with net neutrality issues, it is characterised by the same issues as article 10, 2°.

**Universal Service Directive** – The information obligation in the current Universal Service Directive is limited in scope (it only applies to public telephony services) and unfit to efficiently deal with the blocking of specific service providers. The wording of the proposed amendment to article 20 of the Universal Service Directive – which obliges access providers to inform their users of “conditions limiting access to and/or use of services and applications” – is better suited to deal with such cases of blocking.

**Other measures under the telecom framework** – Article 5 of the Access Directive allows national regulatory authorities to impose obligations on undertakings that control access to end-users, including in justified cases the obligation to interconnect their networks were this is not already the case. The application of article 5 does not require the presence of SMP, and could therefore be useful to counter data blocking situations involving access providers without an SMP position. It should be noted, however, that there are no known cases where article 5 was applied to such cases.

**Roaming Regulation** – Recital 40 of the Roaming Regulation states that there should be no obstacles to the emergence of applications or technologies which can be a substitute for, or alternative to, roaming services, such as WiFi, Voice over Internet Protocol (VoIP) and Instant Messaging services. The specific situation in which VoIP traffic is being blocked by access providers falls under the situation described in the consideration. However, it remains to be seen whether the wording of the Regulation (“should be no obstacles”) is strong enough to allow dealing with these net neutrality violations. In addition, the Roaming Regulation focuses on the use of public mobile communications when travelling within the Community, and does not specifically address limitations to VoIP services on the national market.

**Data protection legislation** – When a user’s actual traffic data is inspected by an access provider to block access (particularly using technologies such as deep packet inspection), then the Data Protection Directive and the ePrivacy Directive may be considered to be breached when the access provider does not obtain the prior consent of the subscriber. However, whether these Directives can be used against blocking issues, depends on the actual technology that is used by the access provider. Furthermore, the consent of the subscriber may have been obtained by the access provider through its general terms & conditions, in which case the Data Protection Directive and ePrivacy Directive will also be of little use against blocking issues.

### 7.1.1. Evaluation and conclusion

European and national **competition law** can be used to deal with the situation in which a dominant undertaking would block data from a content provider in order to favour an affiliated content provider. It is less clear whether competition law will apply in case an entire class of data is blocked.

---

173 See 5.2.2, Significant market power regime
174 Article 20, 2, b of the Universal Service Directive
175 Whether or not general terms & conditions are suitable to obtain a user’s freely given, specific and informed consent, is another issue, dealt with in Chapter 4 - privacy and data protection.
It is also unclear whether the essential facilities doctrine could be used to deal with situations where a dominant undertaking would block data for other reasons than to favour an affiliate.

The Roaming Regulation may serve as a yardstick to prevent telecoms operators from blocking alternative communication services on their network. However, since the problem of blocking is only addressed in general terms in the recitals, it is unclear whether the Roaming Regulation will prove to be an effective instrument to deal with net neutrality infractions.

Articles 10 and 12 of the Access Directive can also be used (interconnection and/or access obligations), although the fact that the retail broadband markets is not listed in the guidelines on market analysis poses a significant hurdle for national regulatory authorities that want to intervene. In addition, the lack of application in practice to net neutrality problems makes it difficult to conclude that articles 10 and 12 can indeed be used to counter blocking situations.

The same is true for the application of article 5 of the Access Directive (obligations on undertakings that control access to end-users), even though article 5 does not require the identification of retail broadband markets as a condition for regulation.

The Commission has stated that "the competitive markets together with the current provisions on access and interconnection, should [...] be sufficient to protect "net freedoms" and to offer a suitably open environment for both European consumers and service providers". However, as shown above, the application of existing rules to access providers with a position of dominance or significant market power is not without problems. Therefore, it can be concluded that although some legal instruments could be useful to deal with net neutrality problems, their usefulness might prove to be rather theoretical in practice, as these legal instruments were not primarily created to deal with net neutrality issues and are often too limited in scope.

Finally, for some traffic inspection technologies that can be used by the access provider to block content, the Data Protection and ePrivacy Directive may also be used to counter blocking issues, under the condition that the consent of the subscriber has not been obtained. The Data Protection Directive also requires access providers to duly inform their subscribers of any actual inspection of the user's traffic, which would qualify as personal data.

7.1.2. Recommendations

Preventing and resolving blocking issues – The fairly limited, yet increasing number of (publicly known) cases in which access providers have been shown to engage in blocking warrants a cautionary approach. At present, it is unclear whether free market competition will force access providers to refrain from net neutrality infractions. Therefore, access providers should be encouraged to adhere to the net neutrality principles mentioned in section 4, while national regulatory authorities gather more data on existing net neutrality interferences. However, in case the currently proposed updates to the telecommunications package would prove to be insufficient to prevent cases of blocking, it should be considered in the short term to strengthen the existing legal framework to deal with these issues.

Information duty – In section 4 above, we recommended that if restrictions do apply, access providers should inform their users about these restrictions before the user has subscribed to the Internet access.


177 For example, in August 2009, The German access provider Telefónica O2 announced that it will allow customers with a mobile Internet package total access to VoIP services at no extra charge. See www.gomonews.com/deutsche-telekom-lifts-mobile-voip-ban-but-charges-users-extra
In line with this principle, we recommend that measures must be taken to ensure that users are properly informed about restrictions before buying internet access subscriptions. (The same measure will also be proposed for the other neutrality infringements discussed below).

While the current legal instruments do provide some legal ground to oblige internet access providers to properly inform their customers, these existing rules may not be sufficiently clear and/or compelling.178 However, an adequate set of rules has already been proposed in this regard by the European Commission within the framework of the reform of the telecommunications package. The current proposal amends article 20 of the Universal Service Directive, which obliges network operators to inform users on the services provided, including in particular:

"information on any other conditions limiting access to and/or use of services and applications, where such conditions are allowed under national law in accordance with Community law." 179

**Powers of authorities** – It should also be envisaged to extend (or clarify) the powers of national regulatory authorities in order to allow them to easily investigate whether blocking occurs, and to intervene in cases where blocking is deemed discriminatory or harmful for competition or innovation — irrespective of the presence of significant market power.

### 7.2. Degradation

#### 7.2.1. Degradation and the law

**Degradation specific data** – In section 3.3, a distinction was made between two types of degradation. The first type – degradation of content of a specific type or content provider – is appropriate for the application of article 82 EC Treaty and its national equivalents. Competition law prohibits dominant undertakings from "applying dissimilar conditions to equivalent transactions with other trading parties, thereby placing them at a competitive disadvantage". Consequently, competition law will apply if a (wholly or partly) degraded content provider can point to an online service provider who provides similar services that has not been degraded by the access provider.

In addition, the non-discrimination obligation in the **SMP regime** may apply. Article 10, 2° Access Directive allows national regulatory authorities to impose obligations of non-discrimination in relation to interconnection and/or access. However, as long as the relevant markets are not defined, national regulatory authorities will need to complete the three stage test, which poses significant difficulties.180

Also, under the proposed amendment of article 20 **Universal Services Directive**, access providers will have to inform customers of "conditions limiting access to and/or use of" online services.181 In comparison with the initially proposed wording (which referred to an obligation to inform consumers of any limitations

---

178 For example, article 10 of the Data Protection Directive does not specify how access providers should provide information to their users, or which level of detail should apply.


180 See 5.2.2, Significant market power regime

181 Proposed Article 20, 1, b of the Universal Service Directive
which apply to the use of these services\textsuperscript{182}), the currently proposed wording places only a limited burden on the access provider. It can therefore be regretted that the proposed article 20 has been altered in a way that creates a grey area, while the original wording was suited to reach the goal of informing customers.

\textit{For example, it is clear that capping the end-users’ maximum speed of file transfers performed with a files sharing program qualifies as a limitation applying to the use of this service (and would therefore have been within the scope of the initially proposed wording). However, the question arises whether this also constitutes a “condition limiting the use of such a program”, since even at a reduced speed file transfers remain possible. Access provider may therefore have no clear obligation to inform their customers in such cases.}

Furthermore, under the proposed update to the \textbf{Universal Services Directive}, access providers will have to inform their consumers about the \textit{minimum service quality levels offered}, such as the time for the initial connection and other quality of service parameters defined by the national regulatory authorities\textsuperscript{183}. However, it remains to be seen whether access providers will feel obliged to advertise their degradation on the basis of this article without intervention of the national regulatory authorities.

In addition, article 22.3 of the amended \textbf{Universal Services Directive} will allow national regulatory authorities to impose minimum service requirements on access providers. As such, the directive will provide an additional tool to safeguard net neutrality in case an access provider were to degrade the speed of a specific service below a certain level, and that level is deemed unacceptable by a national regulatory authority.

Consideration 40 of the \textbf{Roaming Regulation}, which states that there should be no obstacles to the emergence of applications or technologies which can be a substitute for, or alternative to, roaming services, covers the situation in which data transfer from a VoIP service provider is degraded to unacceptable low levels. However, absent an explicit obligation or enforcement mechanism in the Regulation, it is unclear how consideration 40 could be used to deal with net neutrality infractions.

For some traffic inspection technologies that can be used by the access provider to degrade traffic, the \textbf{Data Protection} and \textbf{ePrivacy Directive} may also be used, under the condition that the specific traffic constitutes personal data and consent of the subscriber has not been obtained. The Data Protection Directive then also requires access providers to duly inform their subscribers.

\textbf{Degrading all data} – The second category of degradation, in which a service provider degrades all data in order to give priority to his own preferred content, is less appropriate to deal with using competition law. Since art. 82 and its national equivalents only prohibit discrimination taking place \textit{on the relevant market}, service providers will need to be able to point to another service provider on the same relevant market that has not been degraded by the access provider\textsuperscript{184}. However, competition law will not apply in


\textsuperscript{184} As noted above under 3.3, according the classification of net neutrality issues in this report, degradation implies that the access provider picks its own preferred content and does not allow online service providers to pay for prioritisation.
case the degradation affects services which are situated on different relevant markets\textsuperscript{185}. For example, if the degradation is implemented in order to favour applications which are sensitive to delays, such as VoIP traffic, competition law might not apply, as the different characteristics of non-prioritised and prioritised services makes it unlikely that these services are on the same relevant market\textsuperscript{186}.

The situation with regard to the **SMP regime** is similar to that applicable to degradation of specific data. The regime only provides limited tools and is difficult to apply due to the lack of definition of a retail broadband market.

As pointed out above, the proposed amendments to the **Universal Services Directive** will make this instrument more useful in dealing with cases of degradation. Under the proposed article 20, end-users would have to be informed of the minimum service levels offered by the access provider. In addition, end-users shall have to be informed of conditions limiting access to and/or use of online services\textsuperscript{187}. Under the amended article 22.3, national regulatory authorities would be able to impose minimum service requirements on access providers which degrade their services in an excessive manner.

Consideration 40 of the **Roaming Regulation** could also apply in the situation in which all VoIP traffic is degraded. However, in view of the absence of explicit obligations or enforcement mechanisms, the Regulation seems only remotely useful.

Finally, similar to the degrading of particular content, the **Data Protection** and **ePrivacy Directive** may also be used to counter degrading issues, and to require access providers to duly inform their subscribers.

### 7.2.2. Evaluation and conclusion

As with blocking, up until now the number of publicly known cases in which access to content was degraded by the access provider is limited. However, as evidenced by for example the evolutions in Germany and the Netherlands, it is clear that this issue is not merely theoretical, in particular with respect to peer-to-peer and VoIP traffic.

The analysis above shows that with regard to the three forms of degradation, competition law can only be applied in the situation where a dominant undertaking degrades a specific content provider, or, under the conditions described above, in the situation of degradation of all data in order to prioritise some services. Furthermore, the **SMP regime and the Roaming Regulation** seem of limited use to deal with degradation. Also, whether data protection legislation can be used, depends on the nature of the traffic and how the degrading is actually performed.

Still, if traffic is sufficiently degraded, it will affect the use of services and applications. For some services — such as VoIP — even minor degradation could resort in negative effects. This is contrary to the principle formulated above that access providers should allow users to send and receive the legitimate content of their choice.

This **current lack of legal instruments to counter degradation** has been recognised by the European Commission:

\textsuperscript{185} P. VALCKE, L. HOU, D. STEVENS and E. KOSTA, o.c., p. 7

\textsuperscript{186} See for example case T-320/91, Corbeau, 19 May 1993. ECR I-1477, in which the Court found that regular and express mail are not on the same relevant market.

\textsuperscript{187} Article 20, 2°(b) Universal Service Directive, if amended in accordance with the position of the European Parliament adopted at second reading on 8 May 2009.
As for “net neutrality”, the problem also remains that the current regulatory framework does not provide [national regulatory authorities] with the means to intervene were the quality of service for transmission in an IP-based communications environment to be degraded to unacceptably low levels, thereby frustrating the delivery of services from third parties. In such an event, end-users' connectivity to services provided on the Internet (TV, telephony, Internet, etc.) could be at risk. The impact of prioritisation or of systematic degradation of connectivity could be larger on services needing real-time communications (e.g. IPTV, VoIP, in which latency is critical) and ultimately affect end-user choice\(^\text{188}\).

7.2.3. Recommendations

As is the case with blocking, we recommend that action is taken to encourage access providers to adhere to the net neutrality principles set forth in section 4. Also, action should be taken to make sure that users are duly informed about degradation of certain content or services before buying an Internet connection. The proposed amendment to article 20 of the Universal Service Directive is useful in each of the cases of degradation dealt with above. However, it does not provide a solution for the situation in which the degradation is insufficient to limit actual use of applications, while still giving the non-degraded services an unfair competitive advantage.

The Commission already proposed to introduce minimum service levels in article 22.3 of the Universal Service Directive:

> In order to prevent degradation of service and slowing of traffic over networks, the Commission may, having consulted the Authority, adopt technical implementing measures concerning minimum quality of service requirements to be set by the national regulatory authority on undertakings providing public communications networks. National regulatory authorities shall provide the Commission, in good time before setting any such requirements, with a summary of the grounds for action, the envisaged requirements and the proposed course of action. This information shall also be made available to BEREC. The Commission may, having examined such information, make comments or recommendations thereupon, in particular to ensure that the requirements do not adversely affect the functioning of the internal market. National regulatory authorities shall take the utmost account of the Commission's comments or recommendations when deciding on the requirements.

Such a measure would address the current lack of legal instruments to address degradation, and – if the minimum quality of service requirements are sufficiently high – would guarantee that users can send and receive the legitimate content of their choice. Since legislative procedures are already running, it may be possible to adopt these measures in short term.

It can also be envisaged to extend of the powers of national regulatory authorities (similar to the recommendation above for blocking). This would allow national regulatory authorities to obtain sufficient information on whether degrading is applied, and to intervene when access is not degraded below

---

minimum service levels, but is nevertheless deemed discriminatory or harmful for competition or innovation.

7.3. Prioritisation

7.3.1. Prioritisation and the law

Prioritising content of some content providers – In our classification of net neutrality issues, prioritisation implies that the access provider does not allow online service providers to pay for treating their content with priority. The essential facilities doctrine will not apply then, since online service providers have the possibility to distribute their content, although in a non-prioritised data transfer\(^{189}\).

Conversely, competition law seems suitable to deal with situations of prioritisation, at least when there is a dominant access provider that favours its own affiliate on the upstream market. Possibly, national regulatory authorities could also intervene on the basis of article 10, 2° Access Directive (non-discrimination), but as long as the relevant markets have not been defined they will need to pass the three-criteria test.

Depending on the nature of the traffic and the technology used to prioritise traffic, EU data protection legislation may also be useful\(^{190}\).

Prioritising a class of content – There seems to be no clear way to deal with the situation in which a whole class of content, such as VoIP traffic, is given priority over all other content. In order to apply article 82 EC Treaty, a content provider would have to prove a discrimination, \(i.e\). that it is treated less favourably than one of its competitors\(^{191}\). However, since entire classes of data are prioritised, such unequal treatment may be hard to prove in practice. In theory, it may be possible to apply article 10, 2° Access Directive, but national regulatory authorities will need to complete the three stage test to define the relevant market, which poses significant difficulties\(^{192}\). Also in this case, data protection legislation may be of use, depending on the nature of the traffic and the technology used.

7.3.2. Conclusions

EU competition law may be suitable to deal with the situation in which a dominant access provider prioritises access to its own affiliate on the upstream market. However, the current legal framework does not seem to allow intervention in case of prioritisation of a whole class of data without discriminatory intent, or prioritisation by an access provider without a dominant position. The application of article 10, 2° Access Directive would require the completion of the three stage test to define the relevant market. However, the lack of examples of cases in which access providers have prioritised classes of data, and the fact that such forms of prioritisation can be used to offer a better quality of service to end users, warrants a cautionary approach.

\(^{189}\) P. VALCKE, L. HOU, D. STEVENS and E. KOSTA, o.c., p. 9

\(^{190}\) However, as access providers could argue that prioritisation is actually to the benefit of subscribers, they could argue to rely on article 5.f of the Data Protection Directive to use traffic monitoring technologies without the consent of the subscriber. As described above (section 5.2.6), article 5.f requires a delicate assessment of the rights and interests of both the access provider and the subscribers. This balance may be assessed in another way for activities that are actually advantageous to subscribers, such as prioritisation and access-tiering.

\(^{191}\) P. VALCKE, L. HOU, D. STEVENS and E. KOSTA, o.c., p. 7

\(^{192}\) See 5.2.2
7.3.3. **Recommendations**

As is the case for block and degradation, we recommend in the short term to encourage voluntary adherence to net neutrality principles mentioned in section 4 and to adopt an **obligation to inform consumers of prioritisation measures** taken by the access provider. Under the updated article 20 of the Universal Service Directive, consumers will only have to be informed if prioritisation has an adverse effect on the provided services\textsuperscript{193}.

Again, the **powers of national regulatory authorities** should be extended to allow them to obtain sufficient information to detect undue prioritisation, and in order to allow intervention in cases where prioritisation is deemed discriminatory or harmful for competition, or innovation would allow for a balanced approach. This intervention should be possible irrespective of the presence of SMP.

7.4. **Access-tiering**

7.4.1. **Access-tiering and the law**

Access-tiering is the practice of giving bandwidth priority at a price independent from Internet access fees to applications, service and content providers that are willing to pay for quality of services\textsuperscript{194}.

The fact that any interested content provider can choose to apply for access-tiering has an immediate impact on the possible application of European law. Contrary to the issues of prioritisation and degradation, competition law does not offer any solutions, since the lack of discriminatory behaviour rules out the application of **article 82** EC Treaty and its national equivalents.

In addition, none of the obligations that can be imposed by **national regulatory authorities** on companies with SMP seem useful in remedying access-tiering.

It has been suggested that **article 5** of the Access Directive (which allows national regulatory authorities to impose obligations on undertakings that control access to end-users irrespective of SMP) could be applied, as excessive degradation presents a threat that is similar to blocking as regards the proper functioning of the Internet\textsuperscript{195}. However, it is far from certain that such a reasoning would be adopted by national regulatory authorities.

**Article 20, 2° and 3° of the Universal Service Directive**, which provide for the inclusion of information on "the service quality levels offered" in contracts between consumers and providers of electronic communications services providers, may be used in order to oblige access providers to inform their customers about their access-tiering practices. Again, however, it should be pointed out that article 20 was not written for this purpose, and that its scope requires some stretching in order to interpret it in this way. These issues will be resolved if the proposed amendments to the **Universal Services Directive**, which oblige access providers to inform end-users of minimum service levels and conditions limiting access to and/or use of online services, are accepted. In addition, national regulatory authorities would be able to impose minimum service requirements on access providers which degrade their services in an excessive manner.

---

\textsuperscript{193} Proposed Article 20, 1, b of the Universal Service Directive

\textsuperscript{194} See 3.5, Access-tiering

\textsuperscript{195} CHIRICO, VAN DER HAAR and LAROUCHE, o.c., p. 60
As is the case with the other net neutrality interferences, the EU data protection legislation may also be of use, depending on the nature of the traffic and the actual technology used to implement the access-tiering.

7.4.2. Conclusion

It is not clear whether the SMP regime, in particular article 5 Access Directive, can be applied to the situation of access-tiering. In addition, existing consumer information obligations are not adapted to the specific situation of access-tiering. Furthermore, as access-tiering is characterised by a lack of discriminatory conduct, competition law cannot be applied. Hence, the existing legal instruments seem ill-suited to deal with access-tiering.

However, there is considerable debate on whether significant anti-competitive problems will appear in markets. There is little evidence of anti-competitive conduct to date, and problems have typically been resolved quickly via market forces, or through quick regulatory intervention in markets where they have appeared\(^{196}\).

7.4.3. Recommendations

In the short term, we recommend to adopt an obligation to inform consumers of access-tiering measures taken by the access provider. The proposed amendment to article 20 of the Universal Service Directive will oblige access providers to inform consumers of access-tiering, but only insofar the practice limits access to and/or use of services.

Furthermore, it can be envisaged to adopt a minimum service requirement, which would cover the situation in which access-tiering would result in excessive degradation of non-prioritised services. The new proposed article 22.3 of the Universal Service Directive grants such power to the National Regulatory Authorities, under the supervision of the Commission.

In the medium term, the powers of national regulatory authorities should be extended in order to allow intervention in cases where access-tiering proves harmful for competition or innovation. This intervention should be possible irrespective of the presence of significant market power.

7.5. Unreasonable restrictions on equipment and applications

7.5.1. European Law

In most cases, networked devices are interoperable by virtue of the market mechanisms, which direct suppliers to wards open interfaces and standards, so that the market can grow for all. However, dominant players may try to use proprietary standards to lock consumers into their products or to extract very high royalties from market players, which may slow down innovation and foreclose market entry by new players\(^{197}\).

European law does not seem to cover situations in which an access provider imposes unreasonable restrictions on the use of certain equipment or applications on its customers. Although EU competition law may be applied in some cases — e.g., when a dominant access provider restricts the use of

\(^{196}\) Working Party on Telecommunication and Information Services Policies, Internet traffic prioritisation, an overview, see www.oecd.org/dataoecd/43/63/38405781.pdf, p. 5

\(^{197}\) See the “Communication on future networks and the internet”, COM(2008) 594 final, page 8
equipment\textsuperscript{198} or applications by blocking the data – such situations qualify as blocking (discussed above)\textsuperscript{199}. The European legal framework does not currently seem to offer a solution for the situation in which other restrictions, such as placing a cap on data transfer using a specific application or device, are imposed on users.

7.5.2. Conclusions and recommendations

Although abusive behaviour by dominant undertakings can be restricted by EU competition law, the legal framework does not cover restrictions imposed by non-dominant undertakings, or restrictions such as bandwidth caps. However, since measures such as placing a bandwidth cap can have legitimate reasons (such as bandwidth management or price differentiation), an overall prohibition on restricting the use of applications and equipment may not be suitable.

We therefore think that encouraging access providers to adhere to net neutrality principles – preferably using a "comply and explain" approach – and a clear information duty are sufficient to cover unreasonable restrictions on equipment. With respect to the latter, the proposed article 20.1.b of the Universal Service Directive, does seem to cover most situations in which such restrictions would be imposed.

_The contract shall specify in a clear, comprehensive and easily accessible form at least [...] the services provided, including in particular [...] information on any other conditions limiting access to and/or use of services and applications, where such conditions are allowed under national law in accordance with Community law._\textsuperscript{200}

In addition, an extension of the powers of the national regulatory authorities as described above would allow for ex post intervention when restrictions deemed discriminatory or harmful for competition or innovation.

8. Summary and overview

<table>
<thead>
<tr>
<th></th>
<th>Article 82</th>
<th>SMP</th>
<th>Current USD</th>
<th>Proposed USD</th>
<th>Roaming Regulation</th>
<th>Data Prot.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Blocking</strong></td>
<td>Applies. Dominance required.</td>
<td>10.2° and 12 AD* may apply.</td>
<td>Art 20 applies, ambiguous wording 20.1°.b. Art 22 applies.</td>
<td>No explicit obligation or enforcement.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Degrading specific data</strong></td>
<td>Applies. Dominance required.</td>
<td>10.2° AD may apply.</td>
<td>Art 20 applies, ambiguous wording 20.1°.b. Art 22 applies.</td>
<td>No explicit obligation or enforcement.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Degrading all data</strong></td>
<td>Only applies if</td>
<td>No relevant markets defined.</td>
<td>Out of scope</td>
<td>Art 20 applies, ambiguous wording</td>
<td>No explicit obligation or enforcement.</td>
<td>Depends on the actual technologies used by the access provider</td>
</tr>
</tbody>
</table>

\textsuperscript{198} \textit{E.g.,} set-top boxes for digital television, consoles giving access to a central media platform

\textsuperscript{199} See 7.1, Blocking

9. Blocking illegal content

Introductory note to this section 9: in contrast to many of the other issues dealt with in this chapter, the blocking of illegal content is not necessarily perceived as an unwanted practice to be countered by regulatory intervention. Therefore, this section will not analyse the application of existing legal instruments with a view of counteracting the blocking of illegal content, as was done in section 7.

9.1.1. Current situation

In the past years, European as well as national policy makers have taken steps to encourage the industry to adopt self-regulation mechanisms to deal with illegal content. More recently, there seems to be a trend in the Member States towards (threatening with) imposing a legal obligation on access providers to filter content that is deemed illegal. Besides the impact that such measures have on the fundamental rights of European citizens, the latter evolution is also reason for concern for other reasons, which will be dealt with in more detail below\(^\text{201}\).

European initiatives – In 2004, the Framework Decision on sexual exploitation of children enumerated a number of activities such as distribution, dissemination, transmission and making available of child

\(^{201}\) The tension between Internet censorship and fundamental rights has already been the subject of much debate. This report will not deal with the desirability of blocking content on the Internet, and the implications on privacy rights and freedom of expression, but will instead focus on the economic implications of Member State intervention in the content that can be accessed by their users.
pornography, which are to be considered illegal and have to be sanctioned by the Member States, thus paving the way for the blocking of such content. In 2006, the European Commission published its recommendation on the protection of minors and human dignity. The recommendation, which builds upon earlier initiatives, urges the audiovisual and online information services industry and other parties concerned to examine the possibility of creating filter systems which would prevent minors from accessing potentially harmful content and prevent information offending against human dignity from passing through the Internet. The scope of this recommendation shows the rather minimalist approach taken by the Commission towards the adoption of filtering systems. Already in the 1996 Green Paper, a distinction was made between, on the one hand, information that should be banned for everyone because it belonged to a general category of material that violates human dignity and, on the other hand, material that might affect the physical and mental development of minors.

However, since the EU has no competence as such to legislate on criminal matters, the primary actors in the blocking of illegal content are the Member States, who apply existing criminal laws. Given the trans-border nature of the Internet, the European Union has, through the abovementioned initiatives, played an important role in coordinating the development of policy initiatives and establishing a dialogue between industry stakeholder. In the past years the focus of illegal content blocking initiatives seems to have been shifted to the Member States. The text below provides an overview of some of the Member State initiatives with regard to the blocking of content.

**Member State initiatives** – At Member State level, more far-reaching initiatives are being taken to block unwanted content. Contrary to the European initiatives, the scope of the blocking sometimes exceeds

---


205 “Material offending against human dignity” refers to these types of material, such as violent pornography, zoophilia, and incitement to racial hatred and/or violence, which are generally prohibited in the European Union. See COM (1996) 483, p. 13

206 COM (1996) 487, p. 6


208 Although, as a general rule, neither criminal law nor the rules of criminal procedure fall within the Community’s competence, European intervention in this field is not completely excluded. In its Communication of 24 November 2005, the Commission stated its opinion that “appropriate measures of criminal law can be adopted on a Community basis only at sectoral level and only on condition that there is clear need to combat serious shortcomings in the implementation of the Community’s objectives and to provide for criminal law measures to ensure the full effectiveness of a Community policy or the proper functioning of a freedom”. See COM (2005) 583, Communication from the Commission to the European Parliament and the Council on the implications of the Court’s judgment of 13 September 2005 (Case C–176/03 Commission v Council) Brussels, 24.11.2005, 7.

209 For example, the 1996 Commission Communication on Illegal and harmful content on the Internet called upon Member States to co-operate in exchanging information and defining minimum standards on criminal content.

210 For example through the Safer Internet Programme, which aims to protect children against harmful Internet content.
paedophilic content and material offending against human dignity\textsuperscript{211}. Blocking efforts are increasingly making use of centralised blacklisting at the level of the access provider\textsuperscript{212}. These efforts have been subject to criticism, mainly due to the scope of the filtering and the lack of transparency.

\begin{itemize}
  \item On 18 June 2009, \textbf{Germany} enacted the "\textit{Gesetz zur Erschwerung des Zugangs zu kinderpornographischen Inhalten in Kommunikationsnetzen}". The legislation aims to counter child pornography by method of a DNS block list\textsuperscript{213}. The law excludes the possibility of prosecuting users solely on the basis of visiting a blacklisted site. The legislation received significant opposition, with 130,000 citizens signing the largest official e-petition in German history\textsuperscript{214}. One of the main concerns is that the system could allow for filtering of other content in the future without due process\textsuperscript{215}.
  
  \item In April 2009, media in \textbf{Belgium} reported that judicial and law enforcement authorities were working on a blacklist. The list is said to contain a "few thousand" websites\textsuperscript{216}. Users trying to access blacklisted content would be rerouted to a page containing a stop-sign\textsuperscript{217}. On request of the Belgian public prosecutor, the system was tested on a controversial Dutch website containing a list of neighbourhoods in which convicted paedophiles reside. The scope of the filter will encompass websites containing content that is harmful for public order, offends public decency, or can damage computer systems\textsuperscript{218}. In addition, policy makers have also been playing with the idea to block gambling websites\textsuperscript{219}.
  
  \item In the \textbf{Netherlands}, a blacklist containing around 150 websites (compiled by the National Police Forces) is being enforced on a voluntary basis by a limited number of access providers. The list does not contain websites that are hosted in EU countries, and the list is checked by a taskforce every two months. A study report commissioned by the Ministry of Justice has concluded that the use of the list cannot be made obligatory, as Dutch law provides no basis for the blocking of Internet content\textsuperscript{220}. In addition, the report strongly criticises the effectiveness of the measures.
\end{itemize}

\textsuperscript{211} This can be seen as a logical consequence of the limited competence of Europe in this field and the cultural differences between the Member States. See COM (1996) 487, p.11: \textit{Each country may reach its own conclusion in defining the borderline between what is permissible and not permissible.}

\textsuperscript{212} It is interesting to note that in the Commission Communication of 1996, it is stated that a regime in which access to websites on a centralised blacklist is blocked at the level of the access provider constitutes \textit{"restrictive regime is inconceivable for Europe as it would severely interfere with the freedom of the individual and its political traditions"}. Thirteen years later, some European Member States have, and others are planning to implement such blacklists. See COM (1996) 487, p.14.

\textsuperscript{213} DNS blocking involves redirecting all attempts to access a blacklisted site to a standard web page explaining that the site that was requested contains illegal content. See www.ispa.be/files/0902_position_x20on_x20blocking.pdf, p. 1

\textsuperscript{214} http://opennet.net/blog/2009/06/germany-passes-legislation-block-child-pornography

\textsuperscript{215} According to non-profit organisation IP Watch, the regional court in Hamburg has already ruled that such an infrastructure could be used against other illegal content. Various politicians have mentioned online gambling, copyright violations and protection from online "killer-games" as examples of content that might be subject to blocking in the future. See www.ip-watch.org/weblog/2009/06/19/germany-builds-infrastructure-to-block-the-internet

\textsuperscript{216} Like the German system, Belgium makes use of DNS blocking to prevent access to blacklisted content.

\textsuperscript{217} http://84.199.40.99/

\textsuperscript{218} Art. 39bis Belgian Code of Criminal Procedure

\textsuperscript{219} A new draft law regulating online gaming requires gambling operators to acquire a license for the organisation of offline games of chance in order to be able to organise online games. In addition, the server of the operator must be located in Belgium in order to obtain a license. The Commission has criticised the proposal. See www.ulys.net/en/legal-updates-1228/the-european-commission-s-detailed-opinion-on-the-draft-belgian-gaming.html

\textsuperscript{220} The report (in Dutch) can be consulted at www.wodc.nl/images/1616_volledige_tekst_tcm44-117157.pdf
In France, the proposed "Loi d'orientation et de programmation pour la performance de la sécurité intérieure", would oblige French access providers to participate in blocking websites that have been blacklisted by the Minister of Internal Affairs. Gambling websites were among the content targeted by French authorities. Failure to comply can result in fines up to 75,000 EUR and prison sentences. The filtering procedure has been criticised as easy to circumvent and lacking judicial oversight.

Pursuant to a law adopted in 2006, the National Bureau of Investigation of Finland has also started to compile a blacklist. The aim of the blacklist, which contains around 1,700 websites, is to prevent access to websites containing child pornography. While access providers voluntarily block the list, the ministry of Transport and Communication has implied that if they would not voluntary block access to sites on the list, the government would make the blocking mandatory. The blacklist leaked on the Internet, and was subject to criticism as not all sites on the list turned out to be paedophilic in nature.

In the United Kingdom, access providers are expected to block access to sites that have been identified as containing child pornography by the Internet Watch Foundation. Although filtering is not government mandated, threats of regulatory action ensured that access providers implemented content blocking mechanisms. While the scope of current blocking efforts is limited to paedophilic content, the Home Office has previously indicated that it has considered requiring access providers to block access to articles "glorifying terrorism", an act that is punishable under the 2006 UK Terrorism Act.

Denmark's largest access provider voluntarily started filtering paedophilic content in 2005. In May 2006, the coverage of the filter had extended to 98% of Danish Internet users. Since then, concerns have risen that blocking efforts would surpass the scope of child pornography. A statement by Danish minister Helge Sander, saying that regulating gambling by blocking foreign websites "did not conflict" with efforts to protect the freedom of speech, lead to a reaction of Civil Rights proponents including the Danish Bar and Law Society. On 4 February 2008 a Danish court ordered Danish access provider Tele2 to shutdown access to the filesharing site The Pirate Bay for all its Danish users.

---

221 See the intervention of JM Planche, member of the former CCRSCE (comité consultatif des Réseaux et Services de Communications Electroniques): www.jmp.net/images/doc/2009-04-27 loppsi v1.3.pdf
223 The law (in Finnish) can be consulted at www.finlex.fi/fi/laki/ajantasa/2006/20061068.
224 See the report of Electronic Frontier Finland at www.effi.org/blog/kai-2008-02-18.html.
225 E.g., the list contained numerous sites that only offered legal pornography. The list of censored websites can be consulted at http://wikileaks.org/wiki/797_domains_on_Finnish_Internet_censorship_list_including_censorship_critic_2008.
226 See www.iwf.org.uk/
227 For example, former Home Office Minister Vernon Croaker had set a deadline of the end of 2007 for all access providers to implement content blocking mechanisms. See I. Brown, Internet censorship: be careful what you ask for, see http://ssrn.com/abstract=1026597.
228 See http://publicafaires.linx.net/news/?p=497
229 See www.cphpost.dk/news/politics/90-politics/45822-plan-to-block-foreign-Internet-gambling-sites-hypocritical.html
230 It is interesting to note that the court ruling concluded that Tele2 had assisted in copyright infringement because they give their customers access to The Pirate Bay, thereby copying copyrighted material in their routers. However, article 5.1 of Directive 2001/28/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society explicitly exempts "temporary acts of reproduction [...] which are transient or incidental in nature [and] an integral and essential part of a technological process and whose sole purpose is to enable a transmission in a network between third parties by an intermediary."
9.1.2. Evaluation

Risks for the internal market – The examples above show that the regulation of content on the Internet has gained momentum in the Member States. While the scope of the European efforts in this respect has mainly been limited to content of which the undesirability of the content is uncontested, some Member States seem to want to extend the blocking effort to other content, such as gambling websites and violent video games. Although the actual number of issues has been limited so far, the rising importance of content filtering might create obstacles for the internal market.

For example, in 2006, the Data Retention Directive\(^{231}\) was enacted in order to remedy the differences between national provisions concerning the retention of data online service providers had to comply with\(^{232}\). Obligations laid down by the Member States to adopt a variety of filter systems, each filtering different content, entails similar risks.

Although most of the blocking methods that are currently being used are easy to circumvent, they will prevent a large part of the Internet audience from accessing blocked content. However, filtering techniques can be expected to develop further, and might at some point be harder to counter. In addition, the implementation of these advanced filtering techniques at the level of the access provider can be expected to bring with them significant costs\(^{233}\). Consequently, access providers based in a Member State that mandates the implementation of such techniques could find themselves at a competitive disadvantage. Developments in the field of advanced filter systems should be followed closely to avoid any market distortions in this respect.

Moreover, filtering efforts can become a threat to the free movement of services. First, as noted above, differences in the national provisions concerning the filtering measures that need to be implemented by access providers may create internal market obstacles. For example, it has been shown that certain filter systems can severely reduce the speed of Internet access\(^{234}\). As such, an obligation imposed by a Member State to implement a certain filter system could pose difficulties in a cross-border context. Second, there is a risk that Member States will try to enforce local regulations, such as license requirements, by blocking service providers that are not in compliance, even if these service providers legitimately offer their services in other Member States. An example of such a situation can be found in the plans of both Belgium and France to block gambling operators that do not comply with local license requirements\(^{235}\). Divergent filtering strategies in the Member States could lead to similar problems for other services in the future.

9.1.3. Recommendations

As the jurisprudence with regard to free movement of services has been well developed, the focal point of any regulatory action on the short term should be the exchange of information between industry and


\(^{232}\) Recital 6 of Directive 2006/24/EC.

\(^{233}\) For example, a solution capable of analysing 80 Gigabit per second of data was being marketed for 550,000 euro in May 2008. See http://arstechnica.com/old/content/2008/05/throttle-5m-p2p-users-in-real-time-with-800000-dpi-monster.ars.

\(^{234}\) A 2008 study by the Australian Communications and Media Authority showed that almost all filter systems resulted in slower Internet access. Two of the investigated tools slowed access with up to 75 percent. See www.acma.gov.au/webwr_assets/main/lib310554/sp-level_internet_content_filtering_trial-report.pdf, p. 4

\(^{235}\) In response to the Belgian plans, the European Commission sent a detailed opinion on June 29th 2009, asking clarification about certain aspects of the draft gambling law that is currently being discussed. For France, similar steps were taken on 9 June 2009.
the various policy levels, allowing effective recourse in case of instances of illegitimate blocking. The fact that every Member State maintains its own list of blocked websites, hinders a full picture on which websites have been blocked. In order to address this issue, Member States should be stimulated or obliged to inform each other in case a service provider established on their territory is being blocked, allowing them to take appropriate action (such as criminal proceedings against the blocked service provider, or proceedings against the blocking Member State)\textsuperscript{236}. Also, mechanisms to exchange information beyond specific cases (either by governments or industry-organisations) should be implemented, in order to allow for the development of a more harmonised blocking policy\textsuperscript{237}.

If the filtering of content by the Member States would prove to become an obstacle for the Internal market or other rights and values of the European Community, it could be considered to centralise the authority over the filtering of content, either to the European level, or to an industry organisation representing European access providers. In both cases, appropriate judicial review should be provided for. Such a centralised regime could initially be limited to certain categories of content on which agreement can be reached by the Member States. In a later stadium, the desirability and feasibility of extending the scope of the regime could be gradually expanded.

In the medium term, it could also be envisaged to create a "Data Blocking Directive", for reasons that are similar to the reasons why the Data Retention Directive was adopted (the legal and technical differences between national provisions concerning the retention of data presented obstacles to the Internal Market). Such Data Blocking Directive could then specify which data can be blocked, and how the blocking should be performed in practice.

10. Recommendations

10.1. Anticipating net neutrality interferences?

Several net neutrality interferences have been reported in the United States, Europe and other parts of the world\textsuperscript{238}. Although the number of net neutrality cases has been fairly limited up until now, the number of known interferences is increasing\textsuperscript{239}. Furthermore, it can be assumed that many interferences exist, but have not yet publicly surfaced\textsuperscript{239}. In addition, while the number of problematic interferences has been rather limited in Europe, the blacklisting of content has clearly found its way to the agenda of the Member States.

An analysis of the current EU legal regime reveals the fragmented nature of the current rules, and the fact that there exist few specific rules to effectively deal with neutrality interferences. Although more general rules of competition law, as well as the SMP rules, can be used to deal with some situations

\textsuperscript{236} As noted on page 4 of COM (1996) 487, Community intervention may be justified if the presence of illegal and harmful content on the Internet has direct repercussions on the workings of the internal market.

\textsuperscript{237} While it is understood that cultural differences limit the possibility of establishing a uniform blacklist in all the Member States, it should be possible to reach consensus on a category of content (for example of paedophilic nature) for which the blocking is coordinated on a European level. See COM (1996) 487, p.11.

\textsuperscript{238} See, for example, the HanaTV case in the Republic of Korea. This service provider introduced a video-on-demand service in 2006, which was subsequently blocked by broadband provider LG Powercomm and cable television operator Cuxix (among others). This blocking was partially resolved by the intervention of the Korean Communications Commission in December 2007. See www.soumu.go.jp/main_sosiki/joho_tsusin/eng/pdf/070900_1.pdf, p. 13-14.

\textsuperscript{239} See, for example, the survey on packet shaping undertaken by several Japanese telecom companies in 2007 (available at www.jaipa.or.jp/other/bandwidth/guidelines_e.pdf, p. 2). Among the 280 companies (mainly access providers) that answered the survey, 25% admitted to implement packet shaping and 11% was investigating packet shaping. Most of the traffic shaping was targeted at restricting traffic of specific applications and protocols.
where dominant access providers engage in neutrality interferences, the current rules seem to fall short when applied to non-dominant access providers. Similarly, data protection legislation could be used against net neutrality interferences, but only in specific circumstances, and depending on the technology used by the access provider. National regulatory authorities may not have the power and procedural tools tailored to detecting or dealing with potentially unwanted behaviour.

In other words, when neutrality interferences will intensify, then it may be difficult in the short term for national regulators to effectively deal with (all of) them.

The key question is therefore whether it is useful to introduce rules to anticipate this situation. We are of the opinion that limited regulatory intervention is indeed required, as several elements point in this direction and the social and economic importance of Internet access has recently been underscored:

- In Finland, a new law coming into effect in July 2010 gives Finish citizens a legal right to broadband Internet access

- In France, the Constitutional Council ruled that Internet access is a component of freedom of expression, so that administrative bodies are prevented from cutting off consumers' Internet access in case of repeated copyright infringement

- In November 2009, the European Parliament underlined the importance of human rights (particularly privacy) in relation to internet access

- The examples mentioned in this chapter show that access providers have incentives to commit certain net neutrality infractions, which opens up the possibility of interference with these rights.

- The long term effects of limitations on net neutrality are unclear, so that this matter is too important to leave unmonitored. Competitive pressure alone may not suffice to prevent all unwanted behaviour (e.g. due to switching costs).

We therefore recommend the European Commission to take a clear public policy position on the issue of net neutrality in the very short term, to encourage access providers to adhere to the neutrality principles described above. This policy position could be part of a broader "charter of Internet rights" for Europe, which should build upon the existing legal instruments and judicial decisions that stress the importance of the Internet in modern society. The policy position could then be complemented by self-regulatory initiatives that implement the neutrality principles on a technical level. For example, in respect of bandwidth management, a clear set of criteria should be established, in order to avoid that access providers use bandwidth management techniques for other purposes than warranting a smooth delivery of content or services.

A "comply or explain" approach could then be envisaged, allowing access providers a limited time frame (e.g. one year) to comply with these rules, and, as the case may be, to state their reasons for not complying.

---

240 The announcement of Finland’s Ministry of Transport and Communications (in Finnish) can be consulted at http://www.lvm.fi/webfi/uutinen/view/919166; See also www.cnn.com/2009/TECH/10/15/finland.internet.rights/index.html

241 The judgement of the Constitutional Council (in French) can be consulted at www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank/download/cc-2009580dc.pdf; See also

242 The proposed new telecoms rules now explicitly state that any measures taken by Member States regarding access to or use of services and applications through telecoms networks must respect the fundamental rights and freedoms of citizens, as they are guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms and in general principles of EU law. Such measures must also be appropriate, proportionate and necessary within a democratic society. In particular, they must respect the presumption of innocence and the right to privacy.

243 See Section 4.

244 See Section 4.
complying with certain of these rules. Such an approach would not only create a framework for access providers to adhere to, but would also provide national regulatory authorities with extra information on the amount, type and effect of net neutrality interferences taking place. In any event, authorities should closely monitor evolutions in this respect, and should be given appropriate legal power, manpower and budget to perform this monitoring.

If such efforts for self-regulation do not yield the envisioned effects in the short term, we would opt for a light touch regulation, preferably within the existing telecommunications regulation, as described in the policy recommendations in the following paragraphs.

Finally, if net neutrality infractions would continue after the implementation of light touch regulation, the neutrality principles described above should be enacted into strict laws.

10.2. Obligation to inform

Above, we explained the principle that access providers should allow their users to send and receive the legitimate content of their choice, to use services and run applications of their choice, and to connect hardware and use software of their choice that do not harm the network.

The increasing number of cases in which access providers have been shown to engage in practices which are contrary to this principle, warrants a cautionary approach. Therefore, according to the second principle, if restrictions do apply, access providers should inform their users about these restrictions before selling an Internet connection.

The current provision proposed by the Commission seems suited to inform users about any applicable restrictions:

"Member States shall ensure that where contracts are concluded between subscribers and undertakings providing electronic communications services and/or networks, subscribers are clearly informed in advance of the conclusion of a contract and regularly thereafter of any limitations imposed by the provider on their ability to access or distribute lawful content or run any lawful applications and services of their choice."

Such an obligation has a "light touch" and stimulates competition between access providers. In addition, such an approach has already been proposed by the Commission. Ideally, the information provided by access providers should be provided on the basis of a standardised template, and published online to allow consumers easy access to the information.

10.3. Minimum service levels

The current legal framework does not allow to intervene when an access provider degrades the quality of service to unacceptably low levels. To remedy this situation ex ante, minimum service levels need to be defined and imposed upon access providers.

---

245 See 4, Network neutrality as a policy principle?
Such minimum service levels need to distinguish between various transmission technologies (wired, wireless, cellular network, …), and need to be updated in order to take into account evolutions in Internet usage.

10.4. Extended powers for national regulatory authorities

The application of the SMP regime to issues of net neutrality is fraught with difficulty, since the retail broadband market is not identified by the Commission as one of the relevant markets on which the SMP regime can be applied, and because the various actions available to national regulatory authorities have not been designed to deal with net neutrality issues.

The powers of national regulatory authorities should be extended (or clarified) in order to allow intervention in cases where blocking is deemed discriminatory or harmful for competition or innovation. This intervention should be possible irrespective of the presence of significant market power, so that regulators can intervene on a case-by-case basis.

Above, we proposed the principle that regulators should have sufficient monitoring capabilities to observe the behaviour of access providers. It could also be envisaged to provide regulatory authorities with additional tools to gather information relating to net neutrality infractions from access providers and other stakeholders on an ad hoc basis, e.g. by creating a procedure for information requests to access providers.

10.5. Blocking illegal content

In the short term, mechanisms ensuring the exchange of information between the various stakeholders (law enforcement, industry organisations, blocked content providers) should be implemented in order to allow democratic control over filtering efforts, effective recourse and the development of a harmonised European approach towards the blocking of illegal content.

If the filtering of content by the Member States would prove to become an obstacle for the Internal Market or other rights and values of the European Community, it should be considered to create a central authority, to which responsibility over filtering efforts is given.

In the medium term, it could also be considered to introduce a "Data Blocking Directive", analogous to the Data Retention Directive.
EU study on the

Legal analysis of a
Single Market for the Information Society

New rules for a new age?

10. Spam
11. Cybercrime

November 2009
Chapter 10 Spam

1. Introduction
2. Overview
   2.1. Problems caused by spam
   2.2. Reasons for spamming
   2.3. Definition of spam
   2.4. Legal treatment of spam under current EU framework
   2.5. Legal issues under the current legal framework
   2.6. Enforcement
   2.7. Retention of spam
3. Conclusions
4. Recommendations
   4.1. Short term
   4.2. Mid-term
   4.3. Long term

Chapter 11 Cybercrime

1. Introduction
2. Applicable legal instruments
   2.1. CyberCrime Convention
   2.2. Framework Decision on Attacks against Information Systems
   2.3. Data Retention Directive
   2.4. Data protection legislation
   2.5. Other legal instruments
3. International cooperation
   3.1. ENISA
   3.2. The G8 High-Tech Crime Sub-Group 24/7
   3.3. Organization for Security and Co-operation in Europe
4. Are all types of cybercrime harmonised?
   4.1. Phishing
   4.2. Identity theft
   4.3. DoS attacks
   4.4. Spyware and other malware
5. Conclusions
6. Recommendations
   6.1. Supporting the Cybercrime Convention
   6.2. Supporting a harmonised implementation of the Framework Decision
   6.3. Strengthening cooperation between authorities
   6.4. Encouraging authorities to take action
   6.5. Additional responsibility for access providers
   6.6. Public-private sector cooperation

This study was commissioned by the European Commission's Information Society and Media Directorate-General, in response to the invitation to tender OJ 2007/S 202 244659 of 19/10/2007. The study does not, however, express the Commission's official views. The views expressed and all recommendations made are those of the authors.
Chapter 10

Spam

1. Introduction

On November 11th 2008, the internet access of the U.S. based web hosting service provider McColo was blocked by two major upstream providers, because the firm’s servers were allegedly being used for illegal activities. The Washington Post reported that the McColo acted as a host for syndicates related to the sale of counterfeit pharmaceuticals and designer goods, fake security products and child pornography via e-mail. Following the shutdown, various security firms reported a steep decline of 75 percent in the volume of unsolicited e-mail sent worldwide.

Although the McColo example shows that targeted legal actions can be a useful tool to diminish the worldwide volume of spam, fighting unsolicited e-mail can not be done by legal means alone. There is a wide consensus that the solution to spam is to be found in a combination of technology and law, so that support from the private sector is crucial in finding an effective solution.

While the most well-known kind of spam is unsolicited e-mail, the term is also applied to other forms of unsolicited communications, such as messages targeting instant messaging systems, blogs, wiki's, Usenet, and internet forums. In this chapter, all these kinds of unsolicited electronic messages will be investigated.

2. Overview

2.1. Problems caused by spam

Volume – According to a recent report from security service provider MessageLabs, spam accounts for more than 90% of total e-mail traffic. In some European Member States, such as Germany, France and the Netherlands, the amount of spam in May 2009 exceeded 95% of total e-mail traffic. In addition, one in 317 e-mails was identified to contain malware, and one in 404 e-mails comprised a phishing attack.

Infringes upon users rights – In the ePrivacy Directive, the sending of unsolicited communications for direct marketing purposes is considered an intrusion of the privacy of the recipient. Moreover, since the information collected by spammers to distribute their unsolicited e-mails is gathered without the consent of the recipient, the collection constitutes a breach of a user’s privacy. Spam is also often misleading and deceptive, for example because it presents itself as originating from a legitimate source, such as a

1 See www.washingtonpost.com
2 See www.spamcop.net/spamgraph.shtml?spamyear for a graphical illustration of the impact of the McColo shutdown on the amount of unsolicited e-mail.
4 The word "spam" will be used to refer collectively to all of these manifestations of unsolicited communications.
6 See Chapter 11 - Cybercrime
7 Preamble 40 ePrivacy Directive
pharmaceutics company or a financial institution. In addition, spam often contains adult content, which can be harmful to some individuals, minors in particular.

**Harmful content** – Besides infringing users rights and causing annoyances, spam has also become more harmful over the course of time. Spam messages are being used for purposes such as infecting computers with viruses, manipulating stock markets and selling illegal pharmaceutical products. These risks affect consumer confidence, thus undermining the success of e-commerce and the information society as a whole. In addition, the trend towards digital convergence is broadening the platforms on which spam can spread. While spam used to be limited to personal computers, the internet capabilities of PDAs, cell phones and smartphones make these devices plausible targets. But even devices that are not internet-enabled can become a target of spam, for example by way of unsolicited text messages.

**Harmful distribution methods** – It is estimated that more than 80% of all spam sent in June 2009 originated from botnets. A botnet is a network consisting of computers that have been infected by malicious code allowing them to be remotely controlled. Spammers build (or rent) botnets, in order to distribute the workload and cost of sending spam among the infected computers in the botnet. Computers are turned into members of the botnet ("bots") by the remote installation of malware, which can be spread through means such as malicious websites, instant messengers and e-mail. As such, spam can be used to build a network of bots that can, in turn, permit spammers to send even more unsolicited e-mails. In addition, botnets can also be used for other harmful purposes, such as the carrying out of DDOS attacks.

**Costs** – The costs of the massive amount of spam that is being sent every day can be divided between direct and indirect costs. Direct costs include the cost of broadband capacity, processing power and storage capacity for customers, access providers and backbone operators. These costs also include the cost of services (such as MessageLabs) or anti-virus software, which have become required to safely use the Internet. The cost for loss of human time and the cost incurred by third parties whose e-mails inadvertently get lost in spam filters also constitute direct costs.

Indirect costs, on the other hand, include financial or identity theft, virus infections, fraud, deceptive marketing, loss of consumer confidence, threats to security of corporate networks, etc.

The total welfare loss caused by spam is difficult to estimate. The indirect costs are hard to calculate accurately, and disagreement also exists over direct cost estimates. For example, it is controversial how to cost the time of private individuals. One recent report estimates that spam will cost a total of 91.6 billion EUR worldwide in 2009.

---

8 See Commission communication, on fighting spam, spyware and malicious software, COM (2006) 688 final, p. 3
9 See Commission communication, on unsolicited commercial communications or "spam", p. 4
10 See www.messagelabs.com/mlireport/MLIReport_2009.06_June_FINAL.pdf
12 See Chapter 11 - Cybercrime
14 Commission communication, on unsolicited commercial communications or "spam", p. 8
16 See www.ferris.com/research-library/industry-statistics/
2.2. Reasons for spamming

Spam is so popular as a medium for mass-communication, because costs for senders remain nearly constant. No large budget is required to start sending spam, and once the initial investments in equipment have been made, the volume of spam that is being sent has little impact on the cost. Consequently, spammers have an incentive to send as many unsolicited e-mails as possible, as it increases their chances to infect or deceive victims, sell goods or spread their message.

As such, e-mail spam exemplifies a perfect example of the so-called "tragedy of the commons": spammers use resources (both physical and human) without bearing the entire cost of those resources. In fact, spammers commonly do not bear the cost at all, but externalise it, passing over the costs on internet service providers, users and society as a whole.

The underlying reason for sending spam is typically commercial. Since a huge number of e-mails can be sent at a low cost, only a limited number of recipients need to act upon the messages in order to keep sending them viable. A study performed by the Messaging Anti-Abuse Working Group\(^\text{17}\) showed that among the respondents which had clicked on or responded to spam messages, twelve percent did so because they were interested in the product or service being offered\(^\text{18}\). A recent study showed that spammers can expect to receive one response for every 12.5 million e-mails they send\(^\text{19}\).

Another way to derive profit from spam is by using the messages as a delivery tool for content pertaining to activities such as fraud and extortion. Alternatively, spam can also be used to flood recipients with political statements.

2.3. Definition of spam

Since "spam" covers a wide range of non-requested communications, it is hard to define the term accurately. In general, the word spam is commonly used to describe unsolicited e-mails that are sent in bulk\(^\text{20}\). Certain definitions also stress the commercial nature of spam\(^\text{21}\).

However, these three concepts ("bulk", "commercial" and "unsolicited") are on themselves problematic, as they do not provide enough flexibility to deal with the variety of the content that is distributed using the unsolicited communications.

- **Bulk** – Literature typically states that one e-mail cannot be spam, although to a particular user it does not matter if and how many others receive the same message\(^\text{22}\). The ePrivacy Directive does not require that an e-mail is sent in bulk: the Directive refers to "permission" as the decisive criterion, not the quantity in which messages are being sent\(^\text{23}\).

  It should be recognised that limiting "spam" to messages that are sent in bulk, makes little sense. Using techniques such as random text generation, spammers are able to distribute a unique

---

\(^{17}\) See www.maawg.org/home


\(^{19}\) See http://news.bbc.co.uk/2/hi/technology/7719281.stm

\(^{20}\) Commission communication, on unsolicited commercial communications or "spam", p. 5

\(^{21}\) For example, the US CAN-SPAM act of 2003 establishes requirements for those who send commercial e-mail.


message to each user. These random messages are more efficient in circumventing preventive measures, and can be generated with software that is freely available on the Internet.

In addition, by only targeting bulk messages, certain types of unsolicited mail would stay below the radar. For example, “spear-phishing” is a form of spam targeting a small group of carefully selected users in order to gain access to information such as credit card numbers, company secrets or government information. In order to deceive the recipient, spear-phishing messages are personalised, and the sender often tries to impersonate a trusted source in order to make detection more difficult.\(^{24}\)

Regulators sometimes use a specific number of messages that is being sent as a touchstone for regulatory intervention.\(^{25}\) Typically, caps range somewhere between the level of 50 to 100 e-mails. The US CAN-SPAM act of 2003 foresees aggravating circumstances for conduct involving the sending of multiple commercial messages.\(^{26}\) However, such caps are easy to circumvent by using multiple e-mail addresses to send the messages, or by sending the messages in several smaller batches.

- **Unsolicited** – Not every unsolicited e-mail qualifies as spam. A status update from an online service or a friend forwarding an e-mail containing a joke, are two examples of unsolicited messages, showing that the unsolicited character of an e-mail is very subjective.

The term “unsolicited” poses particular problems in the context of “tell-a-friend”-services. These popular services, which can be found on many websites, allow an internet user to enter the e-mail addresses of one or more friends, who then receive a standard message inviting them to visit a particular website, participate in a contest, etc. The ePrivacy Directive prohibits the implementation of such services, as they constitute unsolicited communications. This restriction is perceived as too far-reaching, and as a result compliance by the merchant is low. This is exemplified by the fact that the Dutch telecommunications regulator OPTA has deemed it necessary to define four criteria that need to be respected in order for a tell-a-friend service to be legitimate.\(^{27}\)

- **Commercial** – The answer to the question whether a message is commercial in nature leaves much room for interpretation and is interpreted differently across jurisdictions. It is impossible to use the concept as a sole criterion to separate spam from other messages. Messages from legitimate sources, such as political communications or messages from not-for-profit organisations are not commercial in nature but can constitute an unsolicited communication. Also, harmful messages containing spyware, viruses or hate speech often pursue goals that are not directly “commercial” in nature.

"Bulk", "unsolicited" and "commercial" are therefore not typically used as a criterion on themselves, but rather in combination. One combination that is often used in literature is that of unsolicited commercial e-mail (UCE). However, this combination does not cover harmful messages containing harmful content sent for non-commercial purposes. Another combination found in literature is that of unsolicited bulk e-mail (UBE). According to the Spamhaus, an organisation which tracks e-mail spammers and spam-

\(^{24}\) OECD, o.c., p. 22

\(^{25}\) For example by imposing a maximum cap on the number of e-mails that may be sent at the same time

\(^{26}\) See US CAN-SPAM act of 2003, Sec. 1037. (b) I. The term ‘multiple’ is defined as “more than 100 electronic mail messages during a 24-hour period, more than 1,000 electronic mail messages during a 30-day period, or more than 10,000 electronic mail messages during a 1-year period.”

related activity, a message constitutes spam only if it is both unsolicited and bulk. While this distinction is broader as it focuses more on the delivery method and not on the content of the message, it cannot be used to deal with certain types of spam, such as messages used for spear-phishing.

2.4. Legal treatment of spam under current EU framework

This section contains an overview of the treatment of spam under the current EU legal framework. It is divided into two sections, a distinction is made between the actual prohibition to send unsolicited messages (Section 2.4.1) and the prohibition to gather e-mail addresses (Section 2.4.2).

2.4.1. Prohibition on sending

Various European legal instruments contain provisions which prohibit the sending of spam. Currently, the ePrivacy Directive has become the central instrument in European anti-spam regulation. However, in order to get the whole picture of European anti-spam regulation, the rules laid down in this directive need to be read together with the rules regarding spam in the Distance Selling Directive, the eCommerce Directive, the ePrivacy Directive, and the Unfair Commercial Practices Directive.

Distance Selling Directive – The Distance Selling Directive aims to protect the consumer's right to privacy by barring or limiting the use of certain particularly intrusive means of communication. In this respect, article 10.1 of the Directive makes the use of automatic calling and fax machines for the means of distance communication subject to the prior consent of the consumer. For other means of distance communication, such as e-mail, no opt-in is required. Article 10.2 prescribes that they may only be used if there is no clear objection from the consumer.

eCommerce Directive – The eCommerce Directive harmonised certain requirements with regard to unsolicited commercial communication by electronic mail. Article 7.1 requires Member States in which unsolicited commercial communications are allowed to ensure that these communications are clearly and unambiguously identifiable. Article 7.2 builds on article 10, 2 of the Distance Selling Directive, and lays down a requirement on service providers to regularly consult the opt-out registers in which natural persons can register themselves.

The eCommerce Directive allowed Member States a free choice between an opt-in or an opt-out regime. However, the increasing number of problems caused by spam urged the legislator towards spam resulting in the adoption of the European ePrivacy Directive and the adoption of the US CAN SPAM Act 2003.


The ePrivacy Directive prohibits the sending of commercial communications by fax, e-mail or using automated calling systems without the prior consent of the recipient. Article 13.1 states:

---

28 www.spamhaus.org/definition.html
29 See Chapter 11 - Cybercrime
31 Preamble 17 of the Distance Selling Directive
32 iViR, Regulating spam - Directive 2002/58 and beyond, 2004, o.c., section 1.1
The use of automated calling systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent.

In accordance with article 13.4, this regime applies only to subscribers who are natural persons. However, Member States can choose to extend the opt-in regime to legal persons.

Article 13.2 contains the only exception to article 13.1. If electronic contact details are obtained from customers in the context of the sale of a product or a service, this information may be used by the seller for direct marketing of similar products or services, on the condition that customers are given the opportunity to object to the use of their contact details, both when they are collected and on receipt of each message by the sender. This exception is only applicable to e-mail or SMS messages, but does not extend to messages sent by fax or through automatic calling machines.

Prohibited practices – Besides the general opt-in obligation imposed by article 13.1, article 13.4 of the ePrivacy Directive aims to prohibits two practices often encountered in relation to spam. First, it is prohibited to send e-mail for direct marketing purposes in which the identity of the sender on whose behalf the communication is made, is concealed. Secondly, e-mail for direct marketing purposes cannot be sent without containing a valid address to which the recipient may send a request to cease the communications.

Relevance of the eCommerce Directive – Although the ePrivacy Directive has become the central instrument in European anti-spam regulation, certain provisions of the eCommerce Directive retain their relevance. In accordance with article 7.1 eCommerce Directive, in cases where commercial communications are still permitted (for example, when a Member State has not extended the application of article 13 of the ePrivacy Directive to legal persons), these communications must be clearly and unambiguously identifiable upon receipt. This provision can be complied with by including the word "advertisement" in the header of the e-mail message, so that a message can be identified without even opening it. Also, the requirement imposed by article 7.2 to consult the opt-out registers retains its relevance in non-harmonized situations, for example with regard to legal persons.

Unfair Commercial Practices Directive – The Unfair Commercial Practices Directive protects consumers against a number of misleading and aggressive commercial practices. Annex I to the Directive contains a list of practices that are unfair under all circumstances. One such practice relates to a specific type of spam: the “persistent and unwanted solicitations by telephone, fax, e-mail or other remote media except in circumstances and to the extent justified under national law to enforce a contractual obligation” is deemed aggressive, and thus unfair, under all circumstances. Member States must therefore foresee effective, proportionate and dissuasive penalties against this type of spam-related practice.

2.4.2. Gathering e-mail addresses

In order to reach a large target audience, spammers require as much e-mail addresses as possible. One way to obtain contact information is through a practice closely related to spam, called "e-mail harvesting".


34 Article 13 Unfair Commercial Practices Directive
E-mail harvesting has been defined by the Commission as the automatic collection of personal data on public Internet-related places — e.g., the web, chatrooms, etc.\(^{35}\)

Working Party 29 has analysed the practice of e-mail harvesting, and has concluded that it is unlawful for three reasons\(^{36}\):

- Collecting an e-mail address on the Internet in order to use it to send spam is a breach of article 6.1.a of the Data Protection Directive, which imposes the obligation to *fairly* process personal data.
- E-mail harvesting is also a breach of article 6.1.b of the Data Protection Directive, which requires that personal data is only collected for specified, explicit and legitimate purposes and is not further processed in a way incompatible with those purposes. Obviously e-mail addresses that have been published on a website, were not intended to be re-used for sending unsolicited e-mails.
- Article 7.f of the Data Protection Directive sets out a balance of interests test, requiring that the data processing is *necessary for the purposes of the legitimate interests pursued by the controller [...] except where such interests of the controller are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1(1).* Given the cost imbalance and the nuisance to the recipient, Working Party 29 is of the opinion that mailings using harvested e-mail addresses cannot be regarded as passing this balance test.

### 2.5. Legal issues under the current legal framework

#### 2.5.1. Are all types of spam covered?

The scope of the harmonised opt-in regime is limited in three ways. These limitations are the result of difficult negotiations among Member States. They also result from the minimum harmonization approach that was taken, allowing Member States to apply stronger measures.

*Limitations as to the type of communication* — The scope of the anti-spam measures of the ePrivacy Directive is explicitly limited to three types of unsolicited communications: automated calling machines, faxes and electronic mail\(^{37}\), whereby "electronic mail" is defined as *"any text, voice, sound or image message sent over a public communications network which can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient"*\(^{38}\). In addition, recital 40 to the Directive explicitly mentions SMS as a subcategory of e-mail. For all other "unsolicited communications for purposes of direct marketing", Member States are free to choose for an opt-in or an opt-out regime\(^{39}\). An earlier version of article 13.1 also included *"other personally addressed electronic communications"*, in order to cover mobile Internet products such as SMS. However, this addition was removed\(^{40}\).

The ePrivacy Directive’s anti-spam regime cannot be applied to all these platforms.

- Whether unsolicited messages sent over *instant messaging* networks qualify as spam, depends on the technical capabilities of the network. Some instant messaging networks only allow to send

---


\(^{36}\) Article 13.1 of the ePrivacy Directive

\(^{37}\) Article 2.h of the ePrivacy Directive

\(^{38}\) Article 13.3 of the ePrivacy Directive

\(^{39}\) iViR, *Regulating spam - Directive 2002/58 and beyond*, 2004, o.c., section 2.4
messages to recipients that are online at the time of sending. The anti-spam regime will not apply here, since the definition of "electronic mail" requires the possibility to store messages in the network until their collection by the recipient.

- Unsolicited messages posted on Usenet will never qualify as spam, since the messages will be stored even after the recipient has collected them. This is contrary to the definition of "electronic mail", which requires that the message is stored until it is collected by the recipient. This definition does not correspond to the functioning of Usenet, which stores messages for a period of time determined by the Usenet-server, irrespective of the collection by one or more recipients.

- Search engine spam tries to exploit the indexation mechanisms of a search engine in order to improve the rank of a specific web page in the search engines' results. This type of spam does not correspond to the definition of "electronic mail", since the messages are stored on the network irrespective of the collection by one or more recipients.

- Nowadays, a large number of blogs, wiki's and social community sites use "captcha's", which require that the user copies an alphanumerical code displayed in a box in order to comment on or contribute to an article. This measure has become necessary in order to combat unsolicited messages – often containing advertisements – that are being posted by automated bots. Since the messages posted by these bots reside on the network until they are removed by a user with the required permissions or an anti-spam tool, this type of spam can not be classified as electronic mail.

- Bluetooth technology can be used to send spam to mobile phones (or other Bluetooth enabled devices such as mobile computers or e-book readers). Almost all modern mobile phones and laptops have Bluetooth functionality, and the technology can be used to deliver geographically relevant spam, for example when walking past a billboard or entering a store. The ePrivacy Directive does not apply to Bluetooth spam, since a Bluetooth connection can not be seen as constituting a network.

- Unsolicited messages have also been known to appear in the file sharing community. For example, in 2000, a company called Flatplanet.net managed to hijack searches on the Gnutella filesharing network, and caused these queries to return advertisements for their software package (which allowed to send spam over the Gnutella network). This type of spam is covered by none of the three types of unsolicited communications within the scope of the Directive.

- Voice over IP (VoIP) networks can also be used as an outlet for spam. Spammers typically use a software program that allows them to automatically call VoIP users. As soon as the spammer manages to establish a connection to the (voice-mail of the) user, a pre-recorder message is played. Since the software enabling the automated calls probably qualifies as an “automated calling machine”, VoIP spam is covered by the Directive.

- Website pop-ups are one of the most recurring forms of unsolicited communication. Typically, pop-ups are opened in a new browser window by a website in order to display advertisements. More malicious forms of pop-ups run in the background and execute code in order to infect a computer or open multiple windows displaying advertisements. Pop-ups cannot be classified under one of the three types of unsolicited communications covered by the Directive.

---

41 Captcha’s are deliberately designed to be difficult to decipher by software. Ideally, captcha’s are easy to decipher for human beings, but very difficult to decipher for software.


43 This type of spam is sometimes referred to as SPIT (for "Spam over Internet Telephony")

44 Article 13.3 of the ePrivacy Directive

45 Consequently, these types are sometimes referred to as "pop-unders".
This overview shows that several manifestations of spam do not fall within the scope of the ePrivacy Directive. Although not necessarily all of them are as annoying and harmful as “traditional” e-mail spam, their occurrence does cause real problems in practice. This is exemplified by the success of anti-spam software and services that are tailored to target some of these manifestations of spam. Therefore, we propose to implement another, more technology-neutral definition of spam. The reference to “other remote media” in the Unfair Commercial Practices Directive, which establishes an opt-out regime, can serve as an example of such neutrality.

Limitations as to the purpose of the communication – The ePrivacy Directive limits the scope of the anti-spam measures to communications “for the purposes of direct marketing”, but does not elaborate on what constitutes a direct marketing communication. Direct marketing implies that a promotional message is delivered to a limited group of potential customers, as opposed to a potentially unlimited audience that can be reached through a mass medium, e.g. broadcasting or a newspaper.

The question whether communications originating from organisations with a non-commercial nature can constitute direct marketing has been the subject of debate. In recital 30 of the Data Protection Directive, the concept of direct marketing is explained as encompassing marketing “carried out commercially or by a charitable organisation or by any other association or foundation, of a political nature”. However, during the drafting process of the ePrivacy Directive, a recital dealing with communications by political parties and charities was deleted. The recital stated that activities aimed at recruiting new members, fund-raising or lobbying for votes, are included in the concept of direct marketing as established by Directive 95/46/EC. Messages by political organizations or others for purposes other than direct marketing, for example the expression of views, thoughts and ideas, are not covered by the provisions on unsolicited communications of this Directive. The recital was deleted by the European Parliament, because the distinction between direct marketing and the expression of views, thoughts and ideas was deemed to be artificial. However, according to the Commission, this deletion did not affect the substance of the Directive.

This has been confirmed by Working Party 29, which stated that article 13 of Directive 2002/58/EC covers any type of sales promotion, including direct marketing by charities and political organisations (such as fund raising). Consequently, the ePrivacy Directive does not limit its scope to direct marketing communications originating from a sender with a commercial purpose. However, common forms of spam containing spyware or messages with the purpose of swindling the recipient are likely outside the scope of the Directive when they do not contain commercial content.

Limitations as to the subscriber – Article 13.5 of the ePrivacy Directive limits the scope of the harmonisation to unsolicited communications directed at subscribers who are natural persons. Member States are free to take measures to protect the interests of legal persons, for example through establishing an opt-out register. If such a register is established, the provisions of the eCommerce Directive will apply. Since the sender will often have difficulty mapping which contacts are legal and which are natural persons, the limitation as to the subscriber is often burdensome in practice.

46 An example of such a service is Mollom.com, which targets spam on blogs and social networks. Available at http://mollom.com.
47 See Section 4.2.2
48 See Section 2.4.1
49 IViR, o.c., section 2.5
51 Article 29 Working Party, o.c., p. 7
52 See Section 2.4.1.
2.5.2. National rules to be followed

Although the national rules have been harmonised to a large extent, differences still exist between the Member States. In situations where national rules differ, the question arises whether the sender must comply with his own set of national rules, or with the rules of the country of the recipient. In addition, service providers from outside the EU that wish to start a mailing campaign which targets more than one Member State are confronted with different rules in each Member State.

2.5.3. Competent court

As with many problems in the online context, there is uncertainty with regard to which law applies to breaches of the obligations imposed by the legal framework for spam, and which court is competent to deal with them. Besides the classic international private law forum, the place of residence of the defendant, European jurisprudence states that in the case of tort law the court of the "place where the damaging fact has occurred" is also competent to decide on the matter. The place where the damaging fact has occurred can be the place where the action was initiated (the place where the spam is sent from) or the place where the result of the action occurs. The former criterion is problematic, since spammers can easily locate themselves in jurisdictions without legal requirements with regard to spam. The latter criterion is also hard to deal with spam, as spam can be sent from and to anywhere in the world.

2.5.4. Implementation differences between Member States

The eCommerce and ePrivacy Directives have only harmonised the most important rules with regard to spam, leaving much discretionary power to the Member States, mainly with regard to the application of the rules to legal persons acting as a recipient, and to other sending mechanisms than the three explicitly mentioned by the Directive.

For example, originally the Dutch Telecommunications regulation did not require consent in order to address commercial communications to legal persons. As per 1 July 2009, the explicit consent of all legal persons is required, obliging senders to check whether they have the explicit consent of each legal person in their contacts database. This change illustrates that the old as well as the new arrangement is possible under the regime of the ePrivacy Directive.

These implementation differences create significant difficulties because spam is, by its very nature, cross-border. Accordingly, when a service provider established in one Member State sends a message to a recipient of another Member State, the service provider may inadvertently breach the spam laws of the recipient Member State, even when the message does not constitute spam in the originating Member State.

2.5.5. Opt-in

In order to opt into receiving communications for marketing purposes, the addressee needs to give its consent. The concept of consent is used in the eCommerce Directive as well as in the ePrivacy Directive, but in practice it is often unclear what actions are required to record a sufficient consent.

54 ECJ C 217/66, Handelskwekerij GJ Bier BV/ Mines de potasse d'Alsace SA, 1976 ECR 1735
55 See recital 30 and 31 eCommerce Directive
56 Article 31.1 ePrivacy Directive
The Data Protection Directive defines the data subject's consent as "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed". A large number of websites require the user to tick a box to indicate consent, a practice explicitly confirmed by recital 17 of the ePrivacy Directive. An equally prevalent technique is to include a clause somewhere in a website's general conditions in which it is stated that the user consents to receive information for direct marketing purposes. It is unclear whether such a practice would constitute a freely given and informed consent, but there is a significant risk that the opinions of the courts of the various Member States would reach different conclusions on this subject.

2.5.6. "Tell-a-friend" and viral marketing

It is unclear whether the inclusion of a "tell-a-friend" system and the use of other viral marketing techniques are prohibited under the ePrivacy Directive. Member States seem to take a different position on this subject. For example, the Dutch telecommunications regulator OPTA explicitly allows the implementation of a tell-a-friend system on four conditions:

- the communication occurs on the initiative of the user, and the website may not offer any consideration to the sender or the recipient;
- the identity of the person who initiated the e-mail message must be clear to the recipient, so as to ensure that he can inform the sender if he does not appreciate such e-mail messages;
- the sender must be able to inspect the entire message that is sent on his behalf, so as to ensure that he can accept responsibility for the personal content of that message;
- the website in question may not store or use the e-mail addresses and other personal details for purposes other than sending that one message on behalf of the sender and must secure the system against potential abuse, such as the automated transmission of spam.

Other authorities do not always agree with this pragmatic position of the OPTA. The Spanish data protection authority, for example, has prohibited the use of tell-a-friend tools, as they are used to circumvent anti-spam laws.

2.5.7. "Soft opt-in"

The "soft opt-in" regime in article 13.2 of the ePrivacy Directive allows the use of contact information that was previously obtained in the context of a sale of a product or service for direct marketing of similar products or services from the same seller. This exception is only applicable to e-mail or SMS messages, but does not extend to messages sent by fax or through automatic calling machines.

It is unclear whether the notion of "sale" is to be interpreted strictly, or also covers services that are provided for free or mere contract negotiations. In an earlier draft, the text contained the word "purchase" instead of "sale". However, the text was amended to exclude the possibility to approach consumers that had merely expressed an interest in a product or service, indicating that contact information can only be used in case an actual sale took place. Also, the Directive does not specify whether the restriction to products from the same seller implies a legal analysis – barring use of the contact information beyond

---

57 Note that this practice is not regarded as problematic in some Member States, such as the United Kingdom
58 www.cbpweb.nl/documenten/pb_20081203_tell_a_friend.shtml
60 iViR, Regulating spam - Directive 2002/58 and beyond, 2004, o.c., section 2.6.2
the legal entity that obtained it – or an economic one. The notion of "similar" products and services is problematic, as it is unclear how narrow this concept should be interpreted, creating legal uncertainty for stores that sell a large number of items, hindering them from using contact information obtained from previous sales.

2.5.8. Sufficient sanctions?

Legislators need to foresee sanctions that outweigh the potential economic profit that can be derived from sending spam, by cutting into the profit or foreseeing criminal sanctions for the worst violations. The Commission has noted that not all Member States provide for criminal or administrative sanctions, and that penalties vary greatly among Member States. Currently, cyber-criminals risk jail sentences varying from one to three years. The Commission has acknowledged that these sanctions might not be a sufficient deterrent, and supports harmonised jail sentences of five years.61

Criminal and administrative sanctions can be a useful tool, since judicial redress is generally not considered as being sufficient. The laws of the Member States provide for various private rights of action which can be used to deal with spammers. For example, spam that contains a reference to a trademark without the required permissions opens up the possibility of action by the rightsholder under intellectual property laws.62 An access provider may also try to sue a client responsible for sending spam for breach of contract, provided that the contract with the client prohibits such behaviour.63

Besides the difficulties in tracking spammers, the main reason for the lack of success of this private right of action can be attributed to the limited pecuniary interest in pursuing litigation.64 A first factor is the high cost of litigation. A second factor is the difficulty in proving the actual damages caused by spam. While damages may be easier to prove in case of fraudulent spam, the damage caused by commercially motivated spam will be more difficult to demonstrate. This problem could be tackled by legislation which reflects the damage caused by spam, and which facilitates restitution of costs to damaged parties.65 Such legislation already exists in the United States.

The US CAN SPAM Act 2003 provides for a limited private right of action against spammers. The Act authorizes access providers that are adversely affected by a violation of the rules prohibiting commercially motivated spam to bring a civil action in any district court of the United States with jurisdiction over the defendant.66 The Act also provides for statutory damages. For messages which contain header information that is materially false or materially misleading, these damages which amount to 100 $ per unsolicited message sent.67 For messages which do not contain misleading header information, damages are fixed at 25 $ per message.68 Unless in the case of messages containing

---

61 See www.ft.com/cms/s/0/10a407b6-5913-11de-80b3-00144feabdc0.html
62 See America Online, Inc. v. IMS, 24 F.Supp.2d 548 (E.D., Va., 1998), in which AOL successfully sued a marketing company which had sent spam which seemed to original from AOL to over 60 million AOL subscribers.
63 For example, in 2006, Microsoft filed a complaint against a British spammer for breaching the terms of use of its Hotmail service, which prohibit the sending of spam. The case was eventually settled out of court. Available at www.theregister.co.uk/2006/09/13/ms_sues_british_spammer
65 See www.oecd-antispam.org/article.php3?id_article=239
66 U.S.C. § 7706(g)(1)
misleading header information, the total amount of damages is capped at 1.000.000 $\textsuperscript{69}$. Damages can be raised or lowered, in case of aggravating or mitigating circumstances\textsuperscript{70}.

2.5.9. Redress by individuals?

Although Member States allow individuals or legal entities to claim civil damages, incentives to do so are usually very limited. The reasons are the same as those set out in the preceding paragraphs: the costs of legal action usually outweigh the potential benefits, since procedures are time and resource intensive. In addition, particularly in cases of non-fraudulent spam, it is hard to prove any actual damage, since only the direct costs to the recipient are somehow measurable. Notwithstanding these barriers, successful civil complaints have been brought against spammers. For example, in 2007, an English company was ordered to pay 750 £ in damages by a small claims court for sending a single unsolicited message. However, the lack of certainty with regard to the amount of damages to be awarded in proceedings concerning spam is likely to deter most individuals from pursuing legal action.

The lack of clarity with regard to the rules that need to be applied by the sender in a cross-border context can be seen as another barrier hindering effective civil action\textsuperscript{71}. As a result of political compromise, the Rome II Regulation excludes defamation, privacy and other personality rights from its scope, and there are no other specific rules governing the competence of national courts and the applicable law with regard to the subject of spam.

2.5.10. Distribution of legal provisions between various legal instruments

A lot of uncertainty exists with regard to the relationship between the eCommerce Directive and the other legal instruments discussed above. The fact that the legal provisions relating to spam are distributed between four distinct legal instruments, whereby the provisions in the ePrivacy Directive have almost completely eroded the rules laid down in the other instruments, does not help the establishment of a clear anti-spam legislation.

Communications – This issue is amplified by the differences in wording used in the various Directives, and the fact that the Directives were written with a different field of application in mind. For example, the eCommerce Directive defines and uses the term "commercial communications", while the ePrivacy Directive defines the term "communications" and uses the term "unsolicited communications".

Subscribers and users – In order to send electronic mail for direct marketing purposes, article 13 ePrivacy Directive uses the term "subscriber" instead of "user". This results in problems where there is no simple two-party relationship between sender and recipient. For example, in case an employer subscribes to a newsletter that will be received by its employees, the employees will not be granted the protection of the Directive, since they are not the subscriber to the newsletter.

2.5.11. Impact on privacy and data protection

A strict interpretation of the European privacy and data protection legislation would imply that access providers, mail service providers and employers should be granted permission in order to install anti-spam filters, as these filters necessarily rely (at least in part) on analysis of the content of messages.

\textsuperscript{69} U.S.C. § 7706(g)(3)(B)

\textsuperscript{70} For example, if the court the court determines that the defendant committed the violation wilfully and knowingly, the amount of damages may be tripled. If the violation occurred despite commercially reasonable efforts to maintain compliance, damages may be lowered.

\textsuperscript{71} See Section 2.5.2
As such, it could be argued that these filters breach data protection regulations and the confidentiality of communications. However, these objections do not seem to be a real issue. For example, while Working Party 29 has stressed that although e-mail communications will almost certainly be covered by Article 8 ECHR, and that communication partners that use e-mails may reasonably expect that their communications will not be inspected by third public or private parties, it does not consider the installation of an anti-spam filter as a breach of data protection legislation\textsuperscript{72}.

Working Party 29 argues that the installation of filtering software is allowed by article 4 of the ePrivacy Directive, which requires e-mail providers to take appropriate technical and organisational measures to safeguard the security of their services. In addition, Working Party 29 is of the opinion that no consent is required in the context of the Data Protection Directive, since the installation of spam filters can be seen as necessary for the e-mail provider in order to perform properly its service contract with the data subject. This situation is covered by article 7.b of the Data Protection Directive, which allows the processing of personal data when necessary for the performance of a contract to which the data subject is party.

Even so, these arguments do not take away all doubt, and the careful wording of the Working Party is an indication of the fact that clarification on this subject is required\textsuperscript{73}.

2.6. Enforcement

2.6.1. Cooperation

The cross-border nature of spam requires a coordinated approach by the relevant enforcement agencies. However, the principles of sovereignty interfere with the ability of countries to target spammers outside their boundaries. Measures against spam are hindered because of the fact that national enforcement agencies cannot impose their national legislation on spammers operating from another jurisdiction. In addition, evidence against a spammer located in another country can be difficult to obtain, so that spammers can choose to operate from jurisdictions that have not concluded any judicial cooperation treaties.

CNSA – At the EU level, the Commission aimed to deal with some of these problems by establishing the Contact Network of Spam Enforcement Authorities (CNSA). CNSA was set up following the Commission Communication of January 2004, and aims to facilitate sharing information and best practices between the national authorities of EU Member States with regard to the enforcement of anti-spam legislation\textsuperscript{74}. In addition, a voluntary agreement was drawn up in February 2005 to establish a common procedure to facilitate cross-border handling of spam complaints\textsuperscript{75}. However, not all Member States have adopted formal procedures to handle such complaints, making it difficult to cooperate efficiently. The Commission has already invited Member States to investigate ways of removing the existing barriers to information

\textsuperscript{72} See Opinion 118 of the Working Party "on privacy issues related to the provision of e-mail screening services", available at http://ec.europa.eu/justice_home/fsi/privacy/docs/wpdocs/2006/wp118_en.pdf

\textsuperscript{73} It should be taken into account that the opinion of the Working Party is not binding. Even so, it has a significant practical impact on national data protection authorities, who largely follow the opinions of the Working Party.

\textsuperscript{74} See Rapid IP/05/146, European countries launch joint drive to combat "spam", 7 February 2005, available at http://europa.eu/rapid/pressReleasesAction.do?reference=IP/05/146

\textsuperscript{75} OECD, o.c., p. 40
exchange and co-operation and the possibility of requesting action from their counterparts in other Member States.\textsuperscript{76}

**CPC** – In 2004 the Regulation on Consumer Protection Cooperation was adopted in order to stop dishonest practices of traders targeting consumers living in other EU countries.\textsuperscript{77} The Regulation sets up an EU-wide network of national enforcement authorities and lays down the framework and general conditions under which Member States are to cooperate in the field of consumer protection. The regulation contains provisions with regard to the exchange of information, the coordination of surveillance and enforcement activities as well as provisions relating to mutual assistance. However, Annex I to the Regulation, which enumerates the Directives within the scope of the Regulation, makes no mention of the ePrivacy Directive, thus excluding the most important legal instrument with regard to spam out of its field of application.\textsuperscript{78} However, since the Unfair Commercial Practices Directive prohibits persistent and unwanted solicitations through remote media, the network seems to have the necessary competence to deal with spam.

**International level** – In addition to these European initiatives, the Commission is promoting cooperation against spam in an international context. For example, the Commission held a vice chair position in the OECD Task Force on Spam and is involved in the International Telecommunication Union. Another international initiative concerning SPAM is the London Action Plan, which aims to promote international spam enforcement cooperation and address spam related problems, such as online fraud and deception, phishing, and dissemination of viruses.\textsuperscript{79} The CNSA involves enforcement authorities that are grouped in the London Action Plan, including third countries such as the United States and Japan as well as industry stakeholders.\textsuperscript{80}

### 2.6.2. Unsatisfactory prosecution measures by Member States

**Lack of Member State enforcement** – In the past years, a limited number of Member States has succeeded in prosecuting spammers:

- In the Netherlands, the telecom authority OPTA has the authority to impose administrative fines on companies or individuals violating local spam regulations. For example, in 2005, the telecom authority OPTA issued a total of 60,000 € in administrative fines against three Dutch companies responsible for sending commercial spam. A record fine of 510,000 € was issued in 2008 against two Dutch spammers for sending luring recipients in calling a pay number. In 2009, a fine of 250,000 € was imposed on a Dutch citizen deemed responsible for sending unsolicited e-mails. In this last case, OPTA decided to impose the high fine taking into account the number of e-mails sent (at least 21 million), the long duration of the infraction, the large number of complaints received by OPTA, the fact that warnings of OPTA were ignored, and the need to deter other potential spammers.\textsuperscript{81}

- In the United Kingdom, regulators and courts have dealt with a limited number of spam-cases. In 2004, the regulatory body responsible for premium telephony services ICTSIS fined a New York

---

\textsuperscript{76} Commission communication, on unsolicited commercial communications or "spam", p. 18


\textsuperscript{78} The Distance Selling Directive, eCommerce Directive and Unfair Commercial Practices Directives are within the scope of the Regulation.

\textsuperscript{79} See www.londonactionplan.com/?q=node/1


\textsuperscript{81} The decision (only available in Dutch) is available at www.opta.nl/nl/download/publicatie/?id=2989
company which had sent spam that encouraged users to connect to a premium rate dial-up service\textsuperscript{82}.

- In France, the National Commission for Information Technology and Liberties ("CNIL") launched an inquiry against a French company after receiving complaints from users that were unable to unsubscribe from the companies mailing list. The company initially responded that it would address the situation, which was said to be the result of a technical problem. However, continuing user complaints led to the issuance of a fine of 30,000 €\textsuperscript{83}.

Although the above examples show that some Member States have already undertaken action with regard to spam, there seem to be insufficient incentives to invest resources in the prevention and prosecution of spammers. The reasons for this lack of incentives should probably be found in the technical and legal difficulties encountered when fighting spam, and in particular in the difficulties resulting from the fact that most spam is sent from outside the Member State. However, the lack of recourses to support enforcement measures undermines the effectiveness of the anti-spam legislation. The lack of enforcement is illustrated by several security breaches and controversial Internet marketing strategies in Member States such as Germany, the UK and Malta. The Commission has already called on the regulatory authorities and stakeholders in Europe to step up their actions to fight illegal online activities such as spam, spyware and malicious software\textsuperscript{84}.

In a recent Commission-funded study on spam, spyware and malicious software\textsuperscript{85} it was highlighted that in recent years Member States have become more active in the fight against spam and other threats that undermine confidence in the Information Society. This study also notes that certain Member States have a high activity level in the fight against these threats, while others have a lower level. Irrespective of the level of activity of the relevant Member States, this study considers that "in general not enough deterring measures" \textsuperscript{86} have been implemented. Although this study covers issues that go beyond spam, such as spyware, it nevertheless reflects the lack of enforcement measures on Member States.

**Target of enforcement activities** – In the past years, a limited number of Member States have effectively prosecuted spammers. As shown by the examples above, legal action is mostly targeted at commercially motivated spam. The prosecution of other threats, such as spam sent with criminal intent, has been limited\textsuperscript{87}. The fact that the European legal framework is focused on spam with commercial intent, can be expected to strengthen this trend\textsuperscript{88}. Although there are other legal instruments available to deal with these types of unsolicited communications, an extension of the scope of existing spam legislation would provide authorities with additional tools to pursue legal action against the most malevolent forms of spam.

**Differences between Member States** – There are significant differences between the efforts invested by Member States in the enforcement of anti-spam regulation. Sometimes, this is linked to the difference
between the authorities that deal with spam: in some Member States the enforcement of the anti-spam rules is performed by telecoms regulators (e.g. the Netherlands) or data protection agencies (e.g. France, Ireland and Greece), in other Member States it is performed by consumer agencies (e.g. Denmark) or law enforcement bodies (e.g. Belgium). Other times, this can be attributed to a lack of public awareness about the possibility to report infractions to the relevant authorities, so that efforts to raise public awareness could prove useful. Other reasons for the limited enforcement cited by the Contact Network of Spam Enforcement Authorities include the cross-border nature of the problem, lack of detailed regulatory requirements or self-regulatory guidelines and insufficiently deterrent penalties.

Even so, in some Member States authorities do have the authority to impose substantial fines. For example, in April 2008, the Dutch telecommunications authority OPTA imposed a fine of over €500,000 on a company for sending unsolicited e-mails.

**Overlapping competence of authorities** – A crucial factor in the fight against spam is the speed of intervention by enforcement authorities. Since the sending of unsolicited messages requires no advanced equipment, spammers can relocate their operations within a matter of days. However, due to the fact that spam relates to a variety of legal subject fields — such as consumer rights, privacy and network security — there are often multiple agencies that have a mandate to deal with an aspect of spam.

In Italy, for example, the data protection authority is responsible for the enforcement of anti-spam regulation, but e-mails containing deceptive messages fall under the responsibility of the competition authority. In some other Member States, the data protection authority does not have the competence to impose sanctions or to enforce the provisions on unsolicited communications against legal persons. In order to allow Member States to effectively deal with spam, each country should not have more than one authority responsible for the distribution and content of unsolicited communications. In addition, these authorities should be able to impose sanctions on individuals and companies who infringe the European anti-spam regulations. A central spam authority would have the additional benefit of further enhancing cooperation between the Member States.

### 2.7. Retention of spam

The Data Retention Directive requires internet access providers and telecom operators to store traffic data regarding all email messages sent over their network (e.g., the email addresses involved, the names and addresses of the users, the IP addresses used, the date and time when the message was sent, the DSL line from which the email was sent, etc.) during a period between 6 and 24 months. It depends on the Member States whether or not the Internet access providers and telecom operators are reimbursed for the costs associated with this data retention.

---


92 OECD, o.c., p. 37

93 Commission communication, on unsolicited commercial communications or "spam", p. 14

94 Directive 2006/24/EC of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC

95 or, more formally, providers of publicly available electronic communication services
Although the majority of emails sent nowadays qualify as spam, the Data Retention Direction does not differentiate between spam and other emails, and requires all emails sent over the network to be stored. Taking into account that the purpose of the storage of the emails is “for the investigation, detection and prosecution of serious crime” (as defined by each Member State)\(^{96}\), it can be regretted that no provisions were included specifically relating to spam emails. Exempting internet access providers and telecom operators from having to store spam-emails – or at least reducing the retention period – would significantly reduce the costs associated with storing the data, while the impact on the investigation / detection / prosecution of serious crimes is likely negligible.

3. Conclusions

1. Spam is a horizontal issue, touching upon different aspects of telecommunication services, consumer protection, security, and privacy, at national and cross-border levels\(^ {97}\). Due to legal and technical difficulties, there is no simple solution or "silver bullet" to stop spam\(^ {98}\).

2. There are some legal problems with the current European approach with regard to spam: the lack of a unified legal framework with regard to spam and the absence of a clear definition of the notion, uncertainty about the meaning of certain basic concepts in the regulation (such as the terms "subscriber", "sale" and "consent"), confusion with regard to the applicable law and the competent court, gaps in the legislation with regard to new technologies and new forms of spam (the current legislation does not cover everything what is in day-to-day practice conceived as spam) and implementation differences in the Member States. In addition, the legal framework makes things overly complex. Examples of this complexity can be found in the fact that the scope of the ePrivacy Directive is limited to natural persons, or in the limitation of the "soft opt-in" exception to unsolicited communications through e-mail.

3. Even so, it must be concluded that the current legal framework sufficiently addresses the most prominent form of spam. Therefore, although various improvements can be made to the European anti-spam legislation, the most important problem seems to be the lack of sufficient enforcement mechanisms in some of the Member States.

4. Recommendations

In this section, we provide a list of recommendations to solve various issues identified in this chapter. A distinction is made between recommendations that can be implemented on the short term (2010-2015), the mid-term (2015-2020) and the long term (2020 and beyond). These time frames align with the relative political and legal difficulty to implement these recommendations, as well as the urgency involved. Hence, the threshold for implementing recommendations for the short term is relatively low, or the urgency involved is rather high. Conversely, recommendations for the mid-term require important legal modifications, or may receive more political resistance. Recommendations for the long term are of a more visionary nature.

\(^{96}\) Article 1.1. Serious crimes typically
\(^{97}\) OECD, o.c., p. 24
\(^{98}\) OECD, o.c., p. 6; Commission communication, o.c., p. p. 3
4.1. **Short term**

4.1.1. *Do not focus on legislative intervention in the short term*

In practice, the majority of spam relates to traditional email spam, for which there is already sufficient (although somewhat complex) legislation. In our opinion, the enforcement instead of the extension of these rules should be the priority.

Our main recommendation for the short term is therefore to not focus on legislative actions to solve the spam problem. Although there are several legal problems associated with the current spam framework, solving these problems should not be a priority, and can be postponed to a later stage, when the current email spam problem is largely tackled.

In our opinion, any further strengthening of the legal framework risks to target the wrong parties, because such strengthening will likely increase the compliance cost for the average *bona fide* company, while only marginally affecting companies and natural persons that have built their business model on the sending of spam emails. Targeting the right parties with the right measures should therefore be the priority in the short term.

If legislative action would nevertheless be undertaken in the short term, we recommend to focus on clarifying the current rules in order to reduce the compliance burden for bona fide companies.

4.1.2. *Cooperation*

Existing procedures for cooperation between Member States, such as the CNSA cooperation procedure, should be enhanced in order to fight spam more effectively. Such efforts could be supported by designating one central spam authority in each Member State. In addition, collective actions by the Member States should be encouraged, and should be targeted at "professional" spammers, "phishers" and messages that contain malware. Measures should be taken to increase the commitment of the Member States, and additional resources should be freed for enforcement activities.

In addition, the creation and enhancement of cooperation procedures beyond Member State level should be encouraged. Such procedures could be developed within the framework of the OECD, and should allow sharing of information and the provision of investigative assistance.

4.1.3. *Administrative sanctions*

Since the traditional criminal and civil courts are often inefficient in dealing with infringements of anti-spam regulation, national enforcement authorities should be able to impose administrative sanctions on spammers, particularly in clear-cut cases. Administrative sanctioning mechanisms should not replace, but supplement the national legal systems. Although some Member States already foresee in the possibility of administrative sanctions, this is not always the case. In addition, it should be considered to allow internet service providers or consumer organisations to start legal proceedings against spammers, as individual users will rarely have sufficient incentives to start such proceedings.

---

99 See Section 2.6.1
100 OECD, o.c., p 70
101 Commission communication, on fighting spam, spyware and malicious software, COM (2006) 688 final, p. 8
4.1.4. **Encourage the adoption of technical measures**

It is easy to hide one's true identity when sending e-mail, due to the fact that e-mail was originally designed with a focus on functionality instead of on security\(^{102}\). Therefore, the adoption of new technical standards with a focus on increased security should be encouraged. For example, technologies such as Sender Policy Framework (SPF) and Sender-ID allow to detect whether the sender of an e-mail is authorized to use a given domain name. Other technologies such as DomainKeys Identified Mail (DKIM) and Message Enhancements for Transmission Authorization (META) add a cryptographic signature to each e-mail, which can then be used to authenticate the sender.

Another approach would be to require some form of payment for each e-mail that is sent. For example, the IronPort Bond Sender Program is used to certify e-mail senders as legitimate and requires them to post a financial bond from which a debt will be taken if the sender violates the code of conduct\(^{103}\). A similar system – which involves no money at all – is advocated by Microsoft: computational spam-fighting\(^{104}\). If this system were to be implemented, each unsolicited e-mail would have to be paid for in computational time. Using a cryptographic key, the receiver would be able to verify if the e-mail has actually been "paid for". While someone sending only a couple of messages would hardly notice, spammers sending a huge amount of messages would have to invest heavily into computational resources.

Besides factors such as cost and effectiveness, technical measures should take into account the amount of user control and respect for data protection and privacy\(^{105}\).

4.1.5. **Accelerate consumer education & awareness**

Consumers should be made aware of the threats posed by spam. Consumers should be informed on how to deal with unsolicited e-mails (e.g., refraining from opening the e-mail or trying to unsubscribe), why they should not respond to spam (products sold are often fake and sometimes downright dangerous), what software to use to limit spam and where to get it, where complaints can be filed, and so on. These educational efforts should be made by access providers, e-mail service providers as well as governments.

Awareness should not only be raised among the addressees of unsolicited communications, but also among potential senders. This can be done by educating businesses on how to communicate with their clients through electronic means in a manner that is compliant with the applicable legislation, and by encouraging direct marketing associations to follow-up evolutions in anti-spam legislation in order to enable them to inform their members\(^{106}\).

4.1.6. **Encourage industry driven initiatives and codes of conduct**

There is a widespread consensus that industry-driven initiatives and codes of conduct can play an important role in anti-spam regulation. The OECD has stated that Internet Service Providers and e-mail service providers have an important role to play, and that governments and regulators should support the development of ISP codes of practice that complement, and are consistent with, existing legislation\(^{107}\).

\(^{102}\) OECD, o.c., p. 29
\(^{103}\) See www.ironport.com/pdf/ironport_2002-06-25.pdf
\(^{105}\) Commission communication, on unsolicited commercial communications or “spam”, p. 24
\(^{106}\) OECD, o.c., p. 14
\(^{107}\) OECD, o.c., p. 10
The Commission has also expressed its support for Europe-wide codes of conduct for direct marketing\textsuperscript{108}.  

**Examples** – The "Technology and Policy Proposal" of the Anti-Spam Technical Alliance (ASTA) is an example of such a code of conduct. The document, released in June 2004, recommends a series of best practices to be implemented by internet service providers and mailbox providers, organisations that provide Internet connectivity, legitimate bulk e-mail senders and consumers aimed at preventing ISPs and their customers from being sources of spam\textsuperscript{109}. SPOTSPAM is another example of an industry-driven initiative in relation to spam. SPOTSPAM is a project that was proposed by ECO, the German member of EuroISPA, a pan European association of European Internet Services Providers\textsuperscript{110}. The project was co-funded under the European Commission’s Safer Internet Programme. The aim of SPOTSPAM is to facilitate legal action against spammers at the international level by allowing spam complaints to be submitted to the SPOTSPAM database via national Spamboxes. The information stored in the database can then be used by the appropriate authorities to take action against spammers\textsuperscript{111}. Another interesting example, as it pertains to non-e-mail related forms of spam such as SMS and MMS, is the "Mobile Spam Code of Practice"\textsuperscript{112} from the GSM Association. Although it is not legally binding, this document reflects a commitment by signatory operators to fight mobile spam. Under this document, operators must cooperate with each other to address spam issues as well as to take other measures aimed at protecting customers, such as reviewing customer contracts and/or terms & conditions to ensure "that up-to-date and relevant anti-spam conditions are included"\textsuperscript{113}.

**User interaction** – A large number of Internet Service Providers have already implemented defensive measures to filter spam. This is allowed under the current data protection rules\textsuperscript{114}. Nevertheless, adequate information should be provided to consumers with regard to the use of filter mechanisms, and consumers should have the option to opt-out of their use. At the very minimum, consumers should be able to consult a list of the messages that have been blocked by the system and select the ones that should be delivered. This approach has the advantage that spam filters can be designed to become "smarter" through the user input, so that it might be considered to adopt a technical standard with regard to such systems.

**Other stakeholders** – Not only organisations that provide Internet connectivity can play a role in combating spam. As spam becomes more frequently used for phishing operations, online service providers that are potential targets of such operations – such as financial institutions – should be encouraged to adopt a policy and to inform users with regard to which kind of information will and will not be transmitted and requested by e-mail and how fraudulent messages can be identified and reported\textsuperscript{115}.

\textsuperscript{108} Commission communication, on unsolicited commercial communications or “spam”, p. 22

\textsuperscript{109} See www.microsoft.com/presspass/press/2004/jun04/06-22ASTAPR.mspx

\textsuperscript{110} See www.euroispa.org

\textsuperscript{111} See www.spotspam.com

\textsuperscript{112} Available at http://gsmworld.com/documents/code_of_practice.pdf

\textsuperscript{113} Section 5 of the Code of Practice

\textsuperscript{114} See section 2.5.11

\textsuperscript{115} OECD, o.c., p. 45

\textsuperscript{116} For an example of such a policy, available at http://pages.ebay.com/help/tutorial/accountprotection/js_tutorial.html
4.1.7. Measuring spam

The detection and measurement of spam should be encouraged in order to provide the responsible authorities with accurate and up to date information on the source, target, content and volume of spam in a given region or country.

Besides technical measures at the access provider level, enforcement authorities would benefit from information directly supplied by individual users. However, users seem to have little incentive to report infractions. In order to encourage reporting of infractions, Member States could make available dedicated mailboxes to which users can forward unsolicited communications for statistical and analytical purposes, a method that has already been tested in Belgium and France. Reporting of unsolicited messages does not only provide authorities with statistics that allow a better understanding of spam in general, it also allows to set and adapt enforcement priorities\(^\text{117}\). The Commission has supported the use of dedicated mailboxes through the funding of the SPOTSPAM initiative\(^\text{118}\).

4.2. Mid-term

4.2.1. "Defragment" the current rules

The legal provisions relating to spam are currently distributed between four distinct legal instruments, whereby the provisions in the ePrivacy Directive have almost completely eroded the rules laid down in the other instruments. Taking into account our recommendation that the offline and online rules should be unified, we would recommend to centralise all spam rules in one Directive.

4.2.2. Changing the legal definition of spam

In order to address the issues and gaps that have been identified above, article 13 of the ePrivacy Directive should be adapted in order to include new forms of spam and solve issues with the current legal framework. The new article should meet the following requirements:

- Technology neutrality – In order to ensure sufficient flexibility, a more technology-neutral approach to spam should be adopted, so that new communication technologies are covered in case they become a target of spammers. More specifically, all communication technologies that allow a sender to distribute its message at a marginal cost of nearly zero while burdening the recipient and the network should be covered by the legislation\(^\text{119}\). In any event, the current limitation to automatic calling machines, fax and electronic mail is outdated.

Inspiration for a more technology neutral approach can, for example, be found in the definition used by the European Code of Practice for the use of Personal Data in Direct Marketing of the Federation of European Direct Marketing (FEDMA), which has been approved by the Article 29 Working Party\(^\text{120}\). FEDMA defines direct marketing as "the communication by whatever means (including but not limited to mail, fax, telephone, on-line services etc...) of any advertising or marketing material, which is carried out by the Direct Marketer itself or on its behalf and which is directed to particular individuals". This definition covers SMS, Bluetooth, and other means of communication.

\(^{117}\) Commission communication, on unsolicited commercial communications or "spam", p. 16 – 17
\(^{118}\) See Section 4.1.6
\(^{119}\) OECD, o.c., p. 26
\(^{120}\) See [www.fedma.org](http://www.fedma.org)
The proposed amendments to the ePrivacy Directive in the context of the telecom package review takes into account the lack of technology neutrality. In its current form, the scope of the opt-in requirement will be extended to automated calling and communication systems without human intervention. As a result, unsolicited communications for direct marketing purposes will be prohibited as long as they are sent using an automated communication system. The change implies that unsolicited communications sent by other means than fax or e-mail will only be prohibited by the ePrivacy Directive if they are sent using an automated system. In view of the large number of messages that needs to be sent in order to make a profit, this limitation does not seem to pose problems in the context of commercially motivated spam. Certain other forms of spam (e.g. targeted spam sent in limited numbers with a view of compromising a specific user's computer) will still fall out of the scope of the amended article 13. This is not problematic, as the provisions discussed in Chapter 11 (cybercrime) may be more apt to deal with these forms of spam.

- **Unsolicited** – The current requirement that the communication must be unsolicited in order to fall within the scope of the ePrivacy Directive, should be retained. Likewise, the opt-in regime and the obligation to include a valid address to which the recipient may send a request that the unsolicited communication ceases should be retained.

- **Legal persons** – The unequal treatment of natural and legal persons should be corrected. This distinction makes the legislation overly complex, and makes it necessary to make a distinction between contact information from natural and legal persons, which is often impossible to make in practice.

- **Subscribers** – The reference to the term "subscriber" should be adapted, in order to avoid interpretation problems in cases where there is no two-party relationship between sender and recipient. For example, the word "addressee" could be used to extend the scope of the protection. This concern is taken into account in the proposed amendments to the ePrivacy Directive in the context of the telecom package. Under the amended article 13, communications for commercial purposes will only be allowed in respect of subscribers or users who have given their prior consent.

- **Commercial purpose?** – The scope of the current legal framework is limited to communications with a commercial purpose. We are of the opinion that this limitation should be removed, since the risk exists that a large portion of very harmful unsolicited messages (e.g., spam containing spyware), may be regarded as non-commercial in nature.

- **Bulk?** – It was noted above that one of the requirements often used to define the concept of spam is that the messages should be sent in "bulk". However, it does not require advanced technology to distribute messages that are personalised to a certain extent. In addition, the question arises what limit (50 e-mail? 100 e-mails? 1000 e-mails?) should be used to define this concept. Therefore, we suggest to refrain from using this requirement, as is the case in the current legislation.

- **Exceptions** – The current exception with regard to similar products and services seems reasonable and should be retained. However, the concepts "sale" and "similar products" should be clarified, and the scope of the exception could be broadened to all communications technologies.

For example, the following article could be adopted:

"Are prohibited:

(1) any unsolicited communications for non-personal purposes sent through electronic means. Communications are not considered unsolicited if:
- the addressee has given its prior informed consent;
- they are necessary for the performance of a contract to which the addressee is party;
- they are necessary for compliance with a legal obligation;
- the contact details of the addressee were obtained by the sender in the context of a commercial relationship with the recipient and the communication concerns similar products or services;

(2) any communication sent through electronic means and intended for publication on an electronic medium, of which the nature or contents does not correspond with the aim or the content of this electronic medium. *\(^{122}\)

4.2.3. Total harmonisation of spam regulations

Although the national rules have been harmonised to a large extent, the existing differences between the Member States are burdensome for service providers inside and outside the Member States. For example, if the sender and the addressee reside in different Member States, it is unclear which national law should be applied. Therefore, we recommend a total harmonisation of the legal framework with regard to spam, so that the question of which national law should apply is not relevant to determine whether the anti-spam rules have been breached.

4.3. Long term

4.3.1. Spam treaty?

As long as the national laws of the European Member States are not geared to one another and to the laws of third countries, the cross-border nature of spam will make taking legal action against spammers difficult and burdensome. The need for a more thorough harmonisation of the national legislation in the Member States was already emphasized above \(^{123}\). Besides this internal harmonisation, Member States should also seek to bring European anti-spam legislation into line with the legislation in third countries.

The role of the international level in dealing with spam was stressed by the Declaration of the 2003 World Summit on the Information Society in Geneva and the associated Action Plan \(^{124}\). This was confirmed by the Commission, which undertook to investigate the best way to follow-up the results of the 2003 World Summit in the EU, taking into account the Tunis Summit held in 2005 \(^{125}\). As it is clear that the lack of harmonisation poses significant legal barriers to a successful policy against spam, we recommend that the Commission further investigates which measures can be taken at the international level. Ideally, such an investigation could result in a treaty aimed at harmonising certain aspects of the legal framework with regard to spam, such as applicable law, competent court, exceptions and covered technologies and cooperation in the persecution and conviction of spammers.

\(^{122}\) For the avoidance of doubt: item (2) refers to spam on blogs, website forums, etc.
\(^{123}\) See Section 4.2.3
\(^{125}\) Commission communication, on unsolicited commercial communications or “spam”, p. 19
4.3.2. **Unify offline and online spam rules**

Currently, in most Member States, offline unsolicited communications are subject to an opt-out system. Consequently, advertisers can send generic or personalised paper advertisements to recipients without their consent, unless the recipient would protest against this advertisement (for example, by placing a "no advertisements" sticker on his door, or by individually asking an advertiser to no longer send paper advertisements).

However, the online and offline environment are steadily converging towards one another. This can already be observed for the way contact details are gathered and advertisement campaigns are being generated.

For example, it is a common practice in an offline shop to ask a customer for his online contact details. Similarly, many online web forms ask for a customer's online and offline contact details. Advertisement agencies are also increasingly targeting online and offline environments in the same campaign. In some cases, the online and the offline versions of the campaign will be similar. In other cases, the online version is "supporting" the offline version by offering additional information about the product or service, dedicated games, competitions, etc.

Taking into account this convergence of the offline and the online world, we are of the opinion that the same principles should apply to unsolicited communications in both the online and the offline environment. Accordingly, there should also be a basic opt-in system for all offline unsolicited communications, all commercial communications should be clearly marked as such, and the natural or legal person on whose behalf the commercial communication is made must be clearly identifiable.

While the extent of the unsolicited communications problem is not as significant in the offline environment as in the online environment, it should be recognised that the problems faced in the offline environment are basically very similar. As is the case in the online environment, offline advertisers have to accumulate large amounts of contact details to execute personalised campaigns. Similar to the waste of bandwidth and server capacity in the online world, there is a significant level of wasted efforts of offline papers that are directly discarded without ever being read. And similar to the online world, unsolicited communications tend to waste a recipient's time, by requiring him to distinguish advertisements from regular mail (with a possibility of errors), and throwing advertisements in the bin.

Nevertheless, we acknowledge that several implementation details will differ between the online and offline environment, as both environments obviously still have their own characteristics, despite the convergence.

For example, exercising an opt-out in the online environment could be as easy as placing a "no advertisements" sticker on a door or mailbox. Conversely, telling all online advertisers that you no longer want to receive their advertisements, would require sending an separate e-mail to all advertisers.

4.3.3. **Making service providers responsible**

In the medium to long term, it could be considered to make access and telecommunications service providers responsible for providing spam-free internet access. We refer to section 6.9 of Chapter 3 for a detailed explanation of this proposal.
Chapter 11
Cybercrime

1. Introduction

Online criminal activities have become a viable economic activity for fraudsters. The shift towards an information society has caused the emergence of an underground economy, in which criminals can earn hard cash by hosting fraudulent websites, spamming, conducting denial-of-service attacks, creating and renting out botnets, stealing financial and identity information, distributing child pornography and even carrying out terrorist activities. The Internet provides a flexible platform that can be used to quickly and easily spread malicious software and to carry out attacks on individuals, companies and governments from anywhere in the world.

While computer viruses were originally written out of curiosity, the potential profits are attracting wrongdoers which only require a computer and an internet connection to carry out their activity. The size of the threat is exemplified by the botnet Conficker, which was first detected in November 2008. In January 2009, the botnet was estimated to include more than 8 million infected machines, making it the largest botnet known to date. The much smaller Storm botnet, which contained around 75000 computers, was estimated to bring in 2.4 million euros in revenue per year. The Organization for Security and Cooperation in Europe (OSCE) estimates that cybercrime costs the global economy $100 billion a year.

Although various national and international legal instruments have been created to deal with these new forms of criminal activity, the rapid changes in technology, the lack of trained personnel and the international nature of the problem are causing difficulties for law enforcement agencies that have to address cybercrime. Furthermore, only a small part of national criminal laws is currently harmonised between EU Member States.

2. Applicable legal instruments

2.1. CyberCrime Convention

2.1.1. Introduction

The most recognized legal instrument with respect to criminal activity in cyberspace, is the Council of Europe's Convention on Cybercrime. The Convention on Cybercrime, which is the only binding international instrument on this issue, serves as a guideline for any country developing comprehensive national legislation against Cybercrime. The Convention aims to act as a framework for international cooperation between states, by supporting a fast and effective regime of international co-operation.

---

126 See www.f-secure.com/weblog/archives/00001584.html
128 See www.diplomaticourier.org/kmitan/articleback.php?newsid=327
The Convention is a historic milestone in the fight against cybercrime and cyberthreats. It entered into force on July 1, 2004, and was signed (but not yet ratified) by all the European Member States. The Convention is also used as a model law or as a guideline by many countries outside Europe, such as the United States of America, Canada and Japan. In addition, it is recommended by several regional organisations, promoting a global harmonisation of legislation on cybercrime.

On 7 November 2008, an Additional Protocol to the Convention on Cybercrime was adopted by the Committee of Ministers, criminalising certain racist and xenophobic acts committed in cyberspace. The protocol criminalises the dissemination of racist and xenophobic material through computer systems, the issuance of racist and xenophobic motivated threats through such systems, online denial or approval of genocide or crimes against humanity, as well as aiding or abetting the commission of any of these offences.

2.1.2. Scope

The Convention has a substantive, as well as a procedural component. The primary purpose of the Convention is to harmonise domestic substantive criminal law offences and investigation procedures. The global nature of cybercrime requires a common international framework that allows punishment of these crimes, irrespective of where they are committed. In order to reach this goal, the Convention requires signatories to adapt their criminal laws in order to criminalise certain conduct that is committed through, against, or related to computer systems.

The Convention covers criminal activities such as illegal access to computer systems, intentional interception of information without right, intentionally committed data or system interference and distribution and use of devices and certain information to commit any of these offences. It also deals with computer-related offences such as computer-related forgery and fraud, child pornography and infringement of copyrights and related right.

In order to guarantee an effective enforcement of these rules, the Convention also imposes an obligation on signatories to implement measures that allow authorities to investigate cybercrime. These include the ability to search and intercept material on computer networks, the power to collect, search, seize and preserve data as well as the power to intercept communications. In addition, the Convention imposes an obligation to provide international cooperation to other parties in the fight against cybercrime. This obligation covers extradition of offenders, a mutual assistance duty, as well as the designation of a point of contact in order to ensure the provision of immediate assistance.

2.1.3. Implementation

Despite its entry into force in 2004, not all signatories have ratified the Convention on Cybercrime. A significant number of European Member States are among the signatories that have yet to ratify the
Convention\textsuperscript{134}. The situation with regard to the Additional Protocol to the Convention is similar\textsuperscript{135}. Although it should be noted that not all signatories to the Convention have signed the Protocol, only a limited number of the (signing) Member States have ratified the Protocol\textsuperscript{136}.

The Council of Europe itself has cited the low number of ratifications of the Convention as its biggest weakness\textsuperscript{137}. The lack of clout of international authorities with respect to cybercrime became especially clear in 2007, when the computer systems of the Estonian parliament, banks, ministries, newspapers and various other organisations became the target of a DoS attack\textsuperscript{138}. In this context, European Commissioner for Justice and Home Affairs Franco Frattini called for European Member States to step up cooperation in the fight against cybercrime\textsuperscript{139}. Also in 2007, the European Council called for the development of a policy framework in the field\textsuperscript{140}. In view of the need for a harmonised and international approach of the issue of cybercrime, there is a broad consensus that the full implementation of the relevant international legal instruments is seen as the only satisfactory and efficient way to proceed\textsuperscript{141}.

2.2. Framework Decision on Attacks against Information Systems

2.2.1. Introduction

In October 1999, at the Tampere European Council, the Member States agreed on the need to approximate provisions concerning offences and sentencing in the area of Cybercrime\textsuperscript{142}. In February 2005, as a response to a growing threat of attacks against information systems and increased concerns of terrorist attacks aimed at Member States’ critical infrastructure, the Council of the European Union adopted the Framework Decision on Attacks against Information Systems\textsuperscript{143}. The Framework Decision intends to supplement and build upon the other EU and international instruments. The Convention on Cybercrime in particular has served as a basis for the drafting of the decision\textsuperscript{144}.

\textsuperscript{134} The European Member States that have yet to ratify the Convention on Cybercrime are Austria, Belgium, the Czech Republic, Greece, Ireland, Luxembourg, Malta, Poland, Portugal, Spain, Sweden and the United Kingdom

\textsuperscript{135} An overview of the signatories and the ratification status of the Protocol is available at http://conventions.coe.int/Treaty/Commun/ListeTableauCourt.asp?MA=49&CM=16&CL=ENG

\textsuperscript{136} Cyprus, Denmark, France, Latvia, Lithuania, Romania and Slovenia. The United Kingdom, Spain, Italy, Hungary, the Czech Republic and Bulgaria are not among its signatories of the Protocol.


\textsuperscript{138} See section 4.3

\textsuperscript{139} See www.infoworld.com/d/security-central/ec-urges-coordinated-effort-against-cybercrime-267

\textsuperscript{140} See www.consilium.europa.eu/docs.cfm?doc=pressData&df=ec&d=94932.pdf


The objective of the Framework Decision is to improve cooperation between authorities in the Member States, through approximating their criminal laws relating to attacks against information systems. To attain this goal, the Framework Decision contains substantive as well as procedural components, which are described in further detail below.

### 2.2.2. Scope

The Framework Decision imposes on Member States the obligation to provide for effective, proportionate and dissuasive criminal penalties for three main offences, each one involving "information systems". Similar to the Convention on Cybercrime, the definition of information system in the Framework Decision puts the emphasis on the automatic processing of data which is a wide enough concept to allow for a certain extent of technology neutrality. The main offences under the Framework Decision are illegal access to information systems, illegal system interference and illegal data interference.

In all cases, the criminal act must be intentional. Member States have to assure that instigating, aiding, abetting and attempting to commit any of the three main offences is also punishable as a criminal offence. The fact that an offence is committed in the context of a criminal organisation is considered an aggravating circumstance, resulting in a penalty between two and five years of imprisonment.

With respect to the procedural component, the Framework Decision sets forth that each Member State will have jurisdiction with regard to the offences committed on its territory or by one of its nationals. Where an offence falls under the jurisdiction of several Member States, they must cooperate in order to decide which State will prosecute the offenders. In addition, Member States must provide for operational points of contact available twenty-four hours a day and seven days a week.

### 2.2.3. Implementation

Similar to the Convention on Cybercrime, issues have been identified with regard to the implementation process of the Framework Decision on Attacks against Information Systems. Member States had to inform the Commission of any provisions transposing the obligations set forth in the Framework Decision by 12 March 2007. By that date, only one Member State had transmitted a text, which was incomplete.

More than one year later, Greece, Ireland and the United Kingdom had informed the Commission that the implementation had been delayed, and still no response was received from Malta, Poland, Slovakia and Spain.

---

145 Recital 1 of the Framework Decision on Attacks against Information Systems
146 Article 1 (a) of the Framework Decision defines the concept of information system as "any device or group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of computer data, as well as computer data stored, processed, retrieved or transmitted by them for the purposes of their operation, use, protection and maintenance"
147 Article 5 of the Framework Decision on Attacks against Information Systems
148 Article 7 of the Framework Decision on Attacks against Information Systems
149 Article 10.1 of the Framework Decision on Attacks against Information Systems. For legal persons, which are also punishable under the decision, the location of the head office is decisive for the establishment of jurisdiction.
150 Article 11.1 of the Framework Decision on Attacks against Information Systems
152 Ibid., p. 2 - 3
In addition, the Commission has noted that the Framework Decision has been implemented in very different ways in the Member States. For example, Member States were given the option to limit criminalising illegal access to information systems to "cases which are not minor". A number of Member States have used this option:

- In the Czech Republic, illegal access is criminalised only in cases where the data is subsequently misused or damaged;
- In Finland, the requirement for criminal responsibility is that the data must be 'endangered'; and
- In Latvia, illegal access is only criminalised only "if substantial injury is caused thereby".

The Commission considers the above interpretations to be out of character with article 2.1 of the Framework Decision, as they focus on criminal intent and specific risks or damages, rather than the gravity of the offence. In addition, the substantial divergence in what constitutes "illegal access to an information system" goes against the aim of the Framework Decision to harmonise the constituent elements of cybercrime offences. In some Member States, similar problems exist with respect to the description of illegal system and illegal data interference.

### 2.3. Data Retention Directive

The aim of the Data Retention Directive is to harmonise the obligations of "electronic communications service providers" (i.e., telecom and network operators) to retain certain data for the purpose of criminal investigations. The Directive targets mobile, internet and fixed telephony, internet access as well as email. All affected parties needs to retain traffic data regarding these communications, including the name of the parties involved, the user ID and address of the source and the target of the communication, the date and time the communication took place, the equipment used and (with respect to mobile telephony) the geographic location involved. Conversely, the actual content of the communication must not be retained. The Directive does not provide full harmonisation. The data retention term, for example, can vary from 6 to 24 months. Similarly, Member States remain free to decide whether they reimburse telecom and network operators for the costs relating to the retention obligations.

Since the obligation under the Data Retention Directive to retain internet traffic data only applies since March 15, 2009, it is not our intention to evaluate the Directive in this study. However, it should be noted that the Directive has encountered a lot of opposition. Besides the widespread aversion to a general data retention obligation – often based on human rights grounds – and the fact that the Directive does not harmonise all key data retention aspects, the Directive is criticised for leaving too much room for interpretation, effectively undermining the Directive’s harmonisation efforts.

For example, the question whether online e-mail services (such as the ones provided by Microsoft Hotmail, Google Mail and Yahoo Mail) fall within the scope of the Directive has already been subject to debate. Although there are textual arguments in the Directive as to why the traffic data for e-mails sent through these services should be retained, online service providers such as Microsoft, Google and Yahoo are not targeted by the Directive.

---

153 Ibid., p. 3
154 Article 2.1 of the Framework Decision on Attacks against Information Systems
155 Recital 11 of the Framework Decision on Attacks against Information Systems
157 Directive 2006/24/Ec Of The European Parliament And Of The Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC
Also, it should be noted that the European Court of Justice has recently rejected an action for annulment against the EU Data Protection Directive on the grounds that the Directive falls within the scope of the third pillar of the European Union, while the Directive was adopted with a qualified majority vote.\textsuperscript{158}

In any case, we are of the opinion that the Data Retention Directive is not sufficiently harmonised, which may give rise to Internal Market obstacles. For example, its most important element – the duration of the retention – can vary from 6 months to 24 months. Member State implementations indeed seem to vary at this point, so that cross-border access providers will in practice need to adhere to the requirements of the most stringent Member State.

2.4. Data protection legislation

Data Protection Directive – As discussed in detail in Chapter 4 (privacy and data protection), the EU Data Protection Directive contains the general rules regarding the processing of personal data. As the scope of this Directive is very wide and many types of cybercrime rely on some type of "processing" of personal data (for which the informed consent of the data subject is often required), the Data Protection Directive is also a relevant legal instrument to tackle cybercrime.

ePrivacy Directive – The ePrivacy Directive also sets forth several provisions that are relevant in the field of cybercrime:

- Article 4 imposes an obligation on providers of a publicly available electronic communications services to take "appropriate technical and organisational measures to safeguard security of its services, if necessary in conjunction with the provider of the public communications network with respect to network security". However, compliance with article 4 seems to be limited in practice, possibly due to the uncertainty with regard to the meaning of the article. For example, a restrictive interpretation would imply a duty to protect the access provider's own data. A broader interpretation, however, would include the duty to protect against unsolicited or damaging information.\textsuperscript{159} We are of the opinion that the scope of this article should be clarified, as it could be envisaged to make access providers responsible for the security of the Internet infrastructure, as explained in Chapter 3 (overview).

- Article 5.3 of the ePrivacy Directive generally prohibits the use of electronic communications networks to store information, or gain access to information stored in the terminal devices of users, without the prior consent of the user. While this provision mainly targets cookies, it can also be used against surreptitious spyware. Furthermore, in the current parliament proposal to amend the ePrivacy Directive, this article would be further optimised to target spyware.

- In the current parliament proposal to amend the ePrivacy Directive, article 13.4 would explicitly target phishing activities ("in any event… the practice of encouraging recipients to visit websites that contravene Article 6 of Directive 2000/31/EC, shall be prohibited"). Moreover, a new article 13.6 would allow individuals and legal persons to take legal action against infringements of national provisions adopted following article 13 of the ePrivacy Directive.\textsuperscript{162}

\textsuperscript{158} ECJ C-301/06, Ireland v Parliament and Council, O.J. C 82 of 04.04.2009, p. 2
\textsuperscript{159} IViR, o.c., section 3.1
\textsuperscript{162} "6. Without prejudice to any administrative remedy for which provision may be made, inter alia, under Article 15a(2), Member States shall ensure that any natural or legal person adversely affected by infringements of national provisions adopted pursuant to this Article and therefore having a legitimate interest in the cessation or prohibition of such..."
2.5. **Other legal instruments**

- **Framework Decision 2001/413/JHA on combating fraud and counterfeiting of non-cash means of payment** aims to recognize fraud involving any form of non-cash means of payment as a criminal offence in all EU Member States. The Framework Decision establishes a series of criteria to determine the jurisdiction of the national judicial authorities in respect of these offences and puts in place cooperation mechanisms between the private and public bodies responsible for electronic payments and the relevant enforcement authorities.

- **Framework Decision 2004/68/JHA on sexual exploitation of children** lists a number of activities such as distribution, dissemination, transmission and making available of child pornography, which are to be considered illegal and have to be sanctioned by the Member States. The Framework Decision sets out criteria for determining jurisdiction, and contains provisions with regard to extradition of offenders.

3. **International cooperation**

3.1. **ENISA**

In 2004, the European Network and Information Security Agency (ENISA) was established. The main objective of ENISA is to develop expertise to stimulate cooperation between the public and private sectors with regard to network and information security, and provide assistance to the Commission and Member States. The Agency's activities include giving advice and recommendations, analysing data and supporting awareness raising efforts. ENISA provides assistance to the Commission and the Member States in their dialogue with the industry to address security-related problems. It also follows the development of standards, promotes risk assessment activities by the Member States and interoperable risk management routines and produces studies on these issues.

3.2. **The G8 High-Tech Crime Sub-Group 24/7**

The G8’s Subgroup on High-Tech Crime is one of the five Subgroups that was created to implement the Forty Recommendations of the so-called "Lyon Group", a group of experts brought together in 1995 to look for better ways to fight international crime. In 1998, the subgroup developed and established a

---


167 See [www.enisa.europa.eu](http://www.enisa.europa.eu)

constantly available network of experts to assist in high-tech crime investigation, meant to ensure that
criminals never receive safe haven, and that law enforcers have the technical and legal means to fight
cybercrime\textsuperscript{169}. Other activities of the subgroup include involvement in negotiations related to high-tech
crime, the drafting of best practice documents, threat and impact assessments for new technologies and
organising training conferences on cybercrime\textsuperscript{170}.

3.3. **Organization for Security and Co-operation in Europe**

The Organization for Security and Co-operation in Europe (OSCE) is an \textit{ad hoc} organisation under the
United Nations Charter consisting of fifty-six states in Europe, Central Asia, and America\textsuperscript{171}. The OSCE
Action Against Terrorism Unit (ATU) has a mandate to combat the use of the Internet for terrorist
purposes\textsuperscript{172}. In this context, the ATU organizes workshops which provided a means to exchange best
practices and encourage international legal cooperation.

The organisation promotes cooperation between governments on an international level as well as
between the public and private sector. For example, in 2006, the OSCE Ministerial Council called for
states to expand international cooperation, take appropriate measures to protect critical infrastructures,
increase monitoring of terrorist websites, and adopt the Council of Europe Convention on Cybercrime\textsuperscript{173}. The Ministerial Council's decision, which served as an update to an existing decision on combating the
use of the Internet for terrorist purposes\textsuperscript{174} also encouraged member states to participate in the G8 24/7
Network of Contacts for High-Tech Crime\textsuperscript{175}.

4. **Are all types of cybercrime harmonised?**

Although the drafters of the Convention on Cybercrime aimed to make the Convention future-proof by
including flexible definitions that would be able to deal with new (methods of committing) crimes, not all
possible forms of cybercrime are covered by the Convention\textsuperscript{176}. Below, it will be verified whether
contemporary criminal activities committed in or through cyberspace are sufficiently covered by the

4.1. **Phishing**

\textbf{Concept} – "Phishing" is a form of cybercrime that is carried out to make a victim disclose personal or
secret information\textsuperscript{177}. By sending out e-mails that look like an e-mail from a legitimate source (such as a

\begin{flushleft}
\textsuperscript{170} See www.usdoj.gov/criminal/cybercrime/g82004/g8_background.html
\textsuperscript{171} See the cyber security organization catalog, available at www.cistp.gatech.edu/catalog/oneOrg.php?id=61
\textsuperscript{175} See Section 3.2
\textsuperscript{176} M. CHAWKI and M. S. A. WAHAB, "Identity Theft in Cyberspace: Issues and Solutions", \textit{Lex Electronica}, vol. 11 n° 1, p. 29
\textsuperscript{177} C. CALLANAN and M. GERCKE, \textit{Cooperation between law enforcement and internet service providers against cybercrime: towards common guidelines}. Council of Europe Project against Cybercrime, final version, 25 June 2008
\end{flushleft}
financial institution or e-mail provider), the sender tries to trick the addressee into providing sensitive information (such as a user name and password for a site, a credit card number or social security information).

Phishing messages are designed to be difficult for the victim to identify the fraudulent nature of the message, often by using familiar brands to address the user. For example, a phishing e-mail designed to seemingly originate from an online payment provider could request addressees to enter their username and password "for maintenance purposes".

The user input is transferred to the phisher, who can use it to transfer money using the victim's online payment account. A more recent manifestation of this form of cybercrime is "spear-phishing". Although the methods that are used are the same, this type of phishing focuses on a select group of users with the goal of obtaining very specific information.

**Legal treatment** – The Convention and the Framework Decision on Attacks against Information Systems do not contain an explicit prohibition of phishing, but rather a number of provisions that criminalise actions closely related to it:

- Article 7 of the Convention criminalises "computer-related forgery" and can be applied with regard to the use of falsified e-mails.
- Article 2 of the Convention, criminalises "access to the whole or any part of a computer system without right", and article 2 of the Framework Decision on Attacks against Information Systems criminalises "illegal access to information systems". Both provisions can be applied to phishers who hack a system to display a phishing website.
- Article 8 of the Convention criminalizes computer-related fraud and can be applied to any fraudulent use of the data obtained from the victim which causes loss of property.

Since the size of the phishers' target group bears no relevance for the application of these provisions, "spear-phishing" is also covered by these provisions. Consequently, phishing seems to be sufficiently covered by the Convention.

In addition, phishing activities are covered by the Data Protection Directive, due to its wide interpretation of the concepts of "personal data" and "processing". Moreover, phishing will also be explicitly targeted by the proposed new article 13.4 of the ePrivacy Directive.

4.2. **Identity theft**

**Concept** – Identity theft describes criminal acts aimed at fraudulently obtaining and using another person's identifying information. Although identity theft does not necessarily imply the use of technical means or the Internet, if is often combined with sophisticated and even automated attacks at a manageable cost.

---

178 According to phishing site www.phishtank.com, Paypal (14575), Google (374x) and Bank of America (267x) constituted the top three of most imitated brands in May 2009

179 See Chapter 10 on spam

180 In particular, article 8 criminalizes the causing of loss of property to another person by any input [...] of computer data [...] with fraudulent with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person. The act has to be committed intentionally.

181 M. GERCKE, *Internet-related identity theft, Council of Europe Project on Cybercrime, discussion paper, November 2007*, p. 4
Examples of data that could be used to impersonate someone include social security numbers, passport numbers, dates of birth, addresses, phone numbers and financial account information. The data can be obtained through classic espionage, phishing, or other means.

For example, in 2008, criminals managed to load malware onto 300 servers of an American supermarket chain, allowing them to intercept card data stored on the magnetic stripe of payment cards as customer’s used them at the check-out counter\(^{182}\). The breach saw 4.2 million credit card numbers taken, and more than 1,800 of those numbers have been reported as having been used\(^{183}\).

The information obtained can also be used to open or take over credit card accounts, apply for loans, rent apartments, contract with utility companies, issue checks using another person’s name and account number, institute bankruptcy proceedings and obtain employment using a victim’s name and details\(^{184}\).

**Legal treatment** – As is the case with phishing, the Convention does not define identity theft as a separate cyber-offence, but criminalises actions closely related to the offence.

- Article 2 of the Convention and article 2 of the Framework Decision on Attacks against Information Systems can be applied to hackers accessing computer systems in order to steal information.
- Article 4 of the Convention and article 4 of the Framework Decision on Attacks against Information Systems, both with regard to "data interference", can be used to deal with the installation of malicious software on the computer of potential victims, as was the case in the example above.
- Article 5 of the Convention, "computer interference", and article 3 of the Framework Decision on Attacks against Information Systems, "illegal system interference", targets situation where criminals would hinder the functioning of a computer system by altering or damaging the computer’s data.
- Article 6 of the convention criminalises the production, procurement, sale and possession of devices, software, computer passwords and similar data with the intent to use them for the purposes mentioned in the article 2 to 5 of the convention.

Although these articles seem to cover most of the activities related to identity theft through electronic means, possibly not all techniques are covered. Article 3 of the Convention, which prohibits the interception by technical means of non-public transmissions of computer data to, from or within a computer system, covers situations in which identity thieves intercept data during a transfer. However, the question whether illegal access to information stored on a hard disk is covered, is subject to debate. The debate revolves around the fact that when a perpetrator gains access to a computer system and uses it to make a copy of the information to another disk, this process is not "intercepted" but "initiated" by the perpetrator\(^{185}\). If such transfers would indeed fall outside the scope of the Convention, criminals would not be punished for direct disk to disk transfers. However, other articles of the Convention, such as article 2, could still apply.

Although the Convention protects the integrity of computer systems, it does not protect the integrity of the identity itself. Such a protection would be useful, since it is often easier to prove the theft of identity than it is to prove the crimes that are committed using the identity (which are often masked because they were committed using the identity of the victim). For these reasons, the European Commission has

---


\(^{184}\) M. CHAWKI and M. S. A. WAHAB, o.c., p. 3

\(^{185}\) M. Gercke, o.c., p. 25
already noted the possible need for legislation in cases where cyber crime is committed in conjunction with identity theft\textsuperscript{186}. Such a separate provision on identity theft was recently adopted by Norway.\textsuperscript{187}

Finally, similar to phishing, identity theft is also covered by the Data Protection Directive.

4.3. DoS attacks

**Concept** – A denial-of-service attack ("DoS attacks") can be defined as an attack which slows or stops the operation of a cyberspace resource or service by overwhelming it with insincere requests\textsuperscript{188}. DoS attacks are usually conducted using botnets, networks of computers that have been infected by malicious code allowing them to be remotely controlled. By directing the computers in the botnet to simultaneously visit the same Web site, the site can be overloaded and made inaccessible. These attacks have been used successfully against companies (e.g., web shop Amazon) and governments. The disruptive potential was shown in the April 27 DoS attacks against Estonia, which targeted the Estonian presidency and the parliament, almost all of the country's ministries, political parties, news organisations, banks and firms specializing in communications technologies\textsuperscript{189}.

**Legal treatment** – DoS attacks are covered by article 5 of the Convention on Cybercrime, which prohibits the intentional serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data. Article 3 of the Framework Decision on Attacks against Information Systems ("illegal system interference") contains a similar provision. A successful DoS attack would block users from accessing the site or would cause serious deterioration of response times.

Although DoS attacks are covered by the applicable legal framework, neither the Convention nor the Framework Decision contain specific provisions criminalising the creation and use of botnets, which are commonly used to conduct DoS attacks\textsuperscript{190}. Currently, the Framework Decision on Attacks against Information Systems provides for maximum sanctions between one and three years of imprisonment in case of illegal system interference\textsuperscript{191}. In view of the substantial potential economic impact of these attacks, it should be considered to foresee in specific and tougher sanctions for the creation and/or use of botnets\textsuperscript{192}. In order to undermine the revenue of the creators of botnets, the practice of renting a botnet should be made subject to similar criminal sanctioning.

---


\textsuperscript{187} See http://www.cybercrimelaw.net. The provision punishes "he who without authority possesses of a means of identity of another, or acts with the identity of another or with an identity that easily may be confused with the identity of another person, with the intent of a) procuring an economic benefit for oneself or for another person, or b) causing a loss of property or inconvenience to another person"

\textsuperscript{188} N.C. ROWE and E.J. CUSTY, *Deception in Cyber Attacks*, in *Cyber Warfare and Cyber Terrorism*, 2008, p. 94

\textsuperscript{189} See www.guardian.co.uk/world/2007/may/17/topstories3.russia

\textsuperscript{190} This type of DoS attack is also referred to as DDoS ("Distributed Denial of Service Attack"), as the computers conducting the attack are distributed over the botnet.

\textsuperscript{191} Article 6.1 of the Framework Decision. Article 7 of the Framework Decision provides for a maximum penalty of five years of imprisonment, when the infraction has been committed within the framework of a criminal organisation.

4.4. **Spyware and other malware**

**Concept** – "Malware" is short for malicious software and is typically used as a catch-all term to refer to any software designed to cause damage to a single computer, server, or computer network, whether it is a virus, spyware, etc.\(^{193}\) "Spyware" is a form of malware that is designed to gathering information about a person or organisation without their consent. Another use of viruses and similar forms of malware is to allow for the remote control of infected computers, which can be used to carry out DoS attacks, to send spam or for other types of criminal activity. Malware can amongst others be contracted by surfing to a malicious website or opening an e-mail containing the software.

**Legal treatment** – Malware is also covered by the Cybercrime Convention. Relevant articles are article 4 (data interference) which can be applied in situations where malware affects the data on a system, and article 5 (system interference) when malware affects the functioning of the system itself. Article 3 (illegal interception) can also be used to deal with spyware, as the article covers the interception of transmissions to, from or within computer systems. In parallel, article 3 (illegal system interference) and article 4 (illegal data interference) of the Framework Decision on Attacks against Information Systems can be applied. In addition, malware distributed through e-mail will fall within the scope of European anti-spam legislation\(^ {194}\).

Similar to phishing and identity theft, the distribution of spyware is also generally covered by the Data Protection Directive, because many spyware programs rely on the processing of information relating to natural persons. Furthermore, spyware and malware can also be covered by article 5.3 of the ePrivacy Directive (prohibition to store information in terminal equipment), for those cases where the prior consent of the user was not obtained for installing the spyware or malware.

### 5. Conclusions

1. The existing European and international legal instruments **suffice to deal with most forms of cybercrime**. Only with regard to **identity theft** and **DoS attacks**, additional legislation should be considered.

2. Compared to the European anti-spam legislation, the legislation with regard to cybercrime is already **relatively harmonised** at the international level. The problems that do exist with regard to the current legislation are situated at the Member State level, rather than the European level.

3. The **lack of harmonisation on the Member State level** is an impediment for effective action against cybercrime. For example, twelve Member States (namely Austria, Belgium, the Czech Republic, Greece, Ireland, Luxembourg, Malta, Poland, Portugal, Spain, Sweden and the United Kingdom) have not yet ratified the Cybercrime Convention, causing gaps in the legislation of the Member States. The Framework Decision on Attacks against Information Systems suffers from a similar lack of harmonisation\(^ {195}\).

The lack of harmonisation affects cooperation between national law enforcement authorities, which benefits from a harmonisation of crime definitions\(^ {196}\). Consequently, steps should be taken to **encourage Member States to ratify** the Cybercrime Convention in a consistent way in order to ensure further harmonisation of the legal framework with regard to cybercrime.

---


\(^{194}\) See Chapter 10 on spam

\(^{195}\) For example, in 2005 a UK judge acquitted an individual that has conducted a DoS attack, because the 1990 UK Computer Misuse Act does not prohibit such attacks. K. Grant DJ, *R v. a minor*, Wimbledon Youth Court, 2 Nov 2005

\(^{196}\) COM (2007) 267 final, o.c., p. 8
4. Besides these harmonisation issues, the European legislation with regard to cybercrime is **sufficiently advanced and future-proof**, and ready to deal with most situations. However, although the legal "groundwork" is present, effective enforcement seems to be lacking. The Commission has recognized that efficient structures for cross-border cooperation are lacking, being underutilised or not yet sufficiently developed, and that traditional mutual assistance mechanisms are too slow to deal with urgent cyber crime cases. Consequently, the European framework for judicial cooperation should be expanded. In addition, cooperation with the private sector should be increased, as these forms of cooperation can be a valuable contribution to the fight against cybercrime.

6. **Recommendations**

6.1. **Supporting the Cybercrime Convention**

The Cybercrime Convention can deal with almost all forms of cybercrime, so that the need for additional legislative intervention is limited. However, identity theft is not sufficiently covered, and should be penalized with separate criminal sanctions. In addition, it should be considered to provide for specific sanctions for the creation and use of botnets, as these networks have become an important tool for cybercriminals.

However, the European Commission must take steps to encourage the twelve Member States that have not yet ratified the Convention to do so as quickly as possible, as the lack of harmonisation poses serious threats to the ability to deal with cybercrime in an efficient manner. In addition, to avoid allowing criminals a large number of safe havens, the Commission should also encourage third countries to accede to the Convention and its additional protocol.

6.2. **Supporting a harmonised implementation of the Framework Decision**

Although the Framework Decision on Attacks Against Information Systems is of significant importance for the harmonisation of cybercrime regulation in Europe, the international nature of the issue warrants an approach that exceeds Europe in geographic scope, thus placing emphasis on the ratification of the Cybercrime Convention. Nevertheless, the differences in implementation of the Framework Decision in the Member States constitute a barrier to an effective European legal framework with regard to cybercrime.

Member States that have not already done so should implement the Framework Decision in their national legislation. In addition, Member States must be encouraged to take into account the remarks of the Commission with regard to a harmonised implementation of the Framework Decision. The Commission should follow up on this harmonisation effort as it has done in its June report to the Council.

6.3. **Strengthening cooperation between authorities**

The efficiency of the existing substantive legal framework is hampered by a lack of effectiveness in enforcement. Efficient structures for cross-border cooperation between the competent authorities need to be created and further developed. These structures should foresee in a clear distribution of responsibilities.

---

197 *Ibid.*, p. 6
responsibilities and provide a framework for the exchange of information, cross-border enforcement. Strengthening and reconsidering the role of ENISA (the European Network and Information Security Agency) could be a solution in this regard.

6.4. **Encouraging authorities to take action**

Despite the fact that costs caused by cybercrime are substantive, the slow ratification of the Cybercrime Convention by the Member States shows that cybercrime is not seen as a priority. Measures should be taken to increase the commitment of the Member States to deal with these new forms of criminal activity.

6.5. **Public-private sector cooperation**

Public-private sector cooperation initiatives should be encouraged in order to allow common action against cybercrime. In particular, a framework should be developed to support the exchange of information and expertise between public bodies and the industry. The development of technological measures to fight cybercrime, such as filters and accreditation mechanisms should be stimulated, in order to stimulate consumer confidence in the information society. Cooperation could also be aimed at increased awareness among stakeholders and consumers about the threat of and possible solutions to cybercrime.

6.6. **Additional responsibility for access providers**

Parallel to our recommendation with regard to spam, it could be considered to make access and telecommunications service providers more responsible for a safer Internet in the medium long term. We refer to section 6.9 of Chapter 3 for a detailed explanation of this proposal.
EU study on the

Legal analysis of a
Single Market for the Information Society

New rules for a new age?

12. Dispute resolution
13. Self regulation

November 2009
Table of contents

Chapter 12 Dispute resolution in the online context ................................................................. 3

1. Introduction ........................................................................................................................... 3
2. Dispute resolution challenges in the online environment .................................................... 4
3. Application of traditional legal instruments of international private law .......................... 4
   3.1. Do the traditional instruments still apply? .......................................................................... 4
   3.2. The problem of localisation .............................................................................................. 5
4. Alternatives to the traditional approach ............................................................................. 7
   4.1. Alternative Dispute Resolution ......................................................................................... 7
   4.2. Online Dispute Resolution .............................................................................................. 11
   4.3. Small claims procedure .................................................................................................. 17
   4.4. Credit card charge backs ............................................................................................... 18
5. Conclusions ....................................................................................................................... 19
6. Recommendations ............................................................................................................. 20
   6.1. Short term .................................................................................................................... 20
   6.2. Mid-term ..................................................................................................................... 21

Chapter 13 Self regulation ...................................................................................................... 26

1. Introduction ......................................................................................................................... 26
2. Self-regulation in the information society ......................................................................... 26
3. Approaches to self-regulation ............................................................................................ 27
4. Types of self-regulation ...................................................................................................... 28
   4.1. Codes of conduct .......................................................................................................... 28
   4.2. Trustmarks .................................................................................................................... 28
   4.3. Technical standards ...................................................................................................... 30
   4.4. Labelling systems, user rating systems and reputation techniques .............................. 30
5. Importance of self-regulation ............................................................................................. 31
6. Advantages and limitations of self-regulation .................................................................... 33
   6.1. Advantages of self-regulation ....................................................................................... 33
   6.2. Primary disadvantages and limitations of self-regulation .............................................. 34
   6.3. Secondary disadvantages and limitations of self-regulation ....................................... 35
7. Some examples of self-regulation ....................................................................................... 36
   7.1. Internet content ............................................................................................................ 36
   7.2. Technical standards ...................................................................................................... 37
8. Second-level self-regulation on online platforms ............................................................... 38
   8.1. Social communities ....................................................................................................... 38
   8.2. Wikipedia .................................................................................................................... 39
   8.3. Virtual worlds .............................................................................................................. 40
   8.4. Conclusion .................................................................................................................... 42
9. General evaluation of self-regulatory initiatives ................................................................. 43
   9.1. Success criteria ............................................................................................................ 43
   9.2. Requirements for all self-regulation initiatives ............................................................. 43
10. Conclusions ....................................................................................................................... 44
11. Recommendations .......................................................................................................... 44
    11.1. Supporting self-regulatory initiatives ......................................................................... 45
    11.2. Incorporation in technology ....................................................................................... 45
    11.3. Increased use of standards .......................................................................................... 45
12. Recommended uses for self-regulation ............................................................................. 47
This study was commissioned by the European Commission's Information Society and Media Directorate-General, in response to the invitation to tender OJ 2007/S 202 244659 of 19/10/2007. The study does not, however, express the Commission's official views. The views expressed and all recommendations made are those of the authors.
Chapter 12
Dispute resolution in the online context

I. Introduction

On 22 May 2000, the Tribunal de Grande Instance of Paris issued an injunction against American internet service provider Yahoo!, which required Yahoo! Inc. (US entity) to take all possible measures to prevent the access in France of web pages that auction Nazi objects. Furthermore, Yahoo France was ordered to warn all French surfers about the risks involved in viewing the web pages concerned.

The Court found that the auctioning of Nazi objects constituted a "manifestly illegal disturbance" and a contravention of the French Penal Code. Yahoo, on the other hand, argued that the French court was not competent, as the web pages were targeted at an American audience, Yahoo offered its services from the United States, and the measures imposed by the Court undermined its freedom of opinion and expression, guaranteed by the First Amendment of the United States. Yahoo furthermore argued that it was technically challenging to properly distinguish French surfers and other surfers.

Despite the technical objections — confirmed by a panel of experts appointed by the Court — and the various objections against the Court's competence, the injunction was confirmed in November 2000. If Yahoo would not comply with the order, it would be fined 100,000 francs (about 9,150 EUR) for each day of delay.

The decision of the French Court triggered significant reactions: thousands of websites criticized the judgement, and hundreds of newspapers followed suit. According to these reactions, France was destroying "free speech" on the Internet by forcing its rule on anyone who used the Internet anywhere. The case has therefore become the landmark case on the difficulty to apply national laws to a global medium such as the Internet.

Although the decision caused a stir in 2000 (at a time when many legal commentators argued that national states were not competent to regulate the transnational internet), these extra-territorial judicial decisions have become increasingly accepted. Only recently, in a judgement of 2 March 2009, a Belgian penal court sentenced search engine Yahoo! to pay a fine of 55,000 Euro because the company refused to hand over information that would enable the Belgian authorities to identify several fraudsters using Yahoo e-mail accounts. Yahoo's argument that the Court was not competent due to its US establishment was once again rejected, despite its reasonable objection that Belgium and the United States had agreed an international treaty that specified how a prosecutor should seek information from a U.S. company. The Belgian decision quickly sank in oblivion, as these types of decisions seem to have become commonplace.

*   *

The cases above illustrate that dispute resolution procedures on the Internet are intrinsically complex, due to a combination of factors, such as the difficulty to apply traditional rules of jurisdiction to an

---


international medium. Even in more straightforward cases, such as consumer disputes over goods or services bought on the Internet, the dispute resolution procedures lack in effectiveness, despite the emergence of new dispute resolution models and a variety of initiatives that have been undertaken over the years. Not much substantive progress has been made in resolving the fundamental problems, which demonstrates that the problem of online dispute resolution does not lend itself to traditional solutions. This chapter therefore aspires to provide guidance in this debate and looks for alternatives.

2. Dispute resolution challenges in the online environment

Greater number of potential conflicts – The growth of the Internet has intensified international contacts and transactions. Web shops are mushrooming, as starting an online business is relatively easy. Online shopping has now become mainstream. Furthermore, citizens spend a significant amount of time online, often multitasking between participation in international communities or seeking involvement in collaborative creative projects with other citizens from various countries. Many activities on the Internet are also widely distributed among actors. Consequently, a greater number of cross-border disputes can arise, involving small businesses, consumers and other non-professional parties.

Involvement of multiple jurisdictions – Transactions on the Internet often involve persons from foreign jurisdictions, and typically have immediate cross-border effects or even a global reach (such as publishing a web page). This mix of jurisdictions involved creates legal difficulties, not only with respect to the substantive legal rules that apply to the parties’ relationships, but also with respect to the court that is competent to handle disputes and the possibility to enforce judicial decisions in other jurisdictions.

Low value of disputes – Many online transactions have a low value. In case of a dispute, the monetary value of the dispute will often be less than the cost of convening the disputants in the same room, or perhaps even less than the cost of a teleconference.

Anonymity and lack of face-to-face contacts – Transactions take place all over the world, typically between parties that have never met face-to-face. Furthermore, a party can never be presumed to be who he or she claims to be.

Automated decision making – Contrary to face-to-face relations, where humans are involved to take conscious decisions, many decisions and transactions on the Internet are taken and generated, without direct human involvement.

3. Application of traditional legal instruments of international private law

3.1. Do the traditional instruments still apply?

Determining the jurisdiction and applicable law in traditional (offline) court proceedings is handled by private international law, which is a complex field of law. This complexity is exponentially augmented in

5 C. RULE, Online dispute resolution for business, 2002, p. 4
the online environment, because the traditional laws regarding the applicable law are focused on elements of the physical world.

The traditional laws of private international law were created by "digital immigrants", and are organised on the assumption that activities can be geographically delimited (whereby each state can regulate what occurs within its territory)\(^7\). The online context, however, has few real connections with the physical world: beyond the telecom infrastructure, the Internet is often said to have no connections with the real world\(^8\). Hence, online activity is not by default located in a single territory — for example, a website can be accessed everywhere. The technical characteristics of the Internet and its ubiquitous nature therefore result in occasional inconclusiveness of the traditional legal instruments\(^9\), which leads to confusing discussions and situations where an activity is subject to multiple and contradictory regulation, or to no regulation at all\(^10\).

Particularly in the early days of the public adoption of the Internet (mid-1990s), many scholars were eager to discard traditional state-based laws\(^11\). They asserted that the traditional, geographical-based rules of law would not be transferable to the transnational internet, that states could not possibly apply their laws to all the online activities, and that this new "cyberspace" was completely beyond their legitimate and actual supervision\(^12\). They therefore concluded that cyberspace should be treated as a distinct and independent place for regulatory purposes\(^13\).

The problem is, however, that the fundamental building blocks and actors of cyberspace have a real-world existence, and are necessarily located in some physical country\(^14\). Consequently, the predictions of these early authors have not proved to be true. On the contrary, states have regulated the Internet, although with varying success. The debate has thus moved from the question of whether States can regulate the Internet, to the question of how it can be done. This has particularly resulted in a tendency towards applying "country-of-origin" and "country-of-destination" rules\(^15\).

### 3.2. The problem of localisation

The most important legal instrument to determine which court is competent to handle a dispute, is the Brussels I Regulation\(^16\). Related to this is the question which country's laws apply to a certain transaction, for which the most important legal instruments are the Rome I Regulation\(^17\) (for contractual obligations) and the Rome II Regulation\(^18\) (for non-contractual obligations).

---

\(^7\) U. KOHL, *Jurisdiction and the Internet - regulatory competence of online activity*, Cambridge University Press, 2007, p. 4

\(^8\) K.V. KONOORAYAR, "Regulating Cyberspace: The Emerging Problems and Challenges", *Cochin University Law Review*, 2003

\(^9\) A. PATRIKIOS, o.c., p. 67

\(^10\) C. REED, o.c., p. 308

\(^11\) For example, in their epic article "Law and Borders - The Rise of Law in Cyberspace", Johnson and Post argued that "[g]lobal computer-based communications cut across territorial borders . . . undermining the feasibility – and legitimacy – of laws based on geographic boundaries".

\(^12\) U. KOHL, o.c., p. ix

\(^13\) U. KOHL, o.c., p. 11

\(^14\) REED, p. 218

\(^15\) U. KOHL, o.c., p. 25


\(^17\) Regulation No 593/2008 of 17 June 2008 on the law applicable to contractual obligations

\(^18\) Regulation No 864/2007 of 11 July 2007 on the law applicable to non-contractual obligations (Rome II)
All three legal instruments strongly and mainly rely on the localisation of objective elements (such as the residence of a party, the place of business, the place where the contract is performed, where advertisements were received, where a tortuous act took place, etc.) in order to determine the applicable law or the competence of a national state.

Evaluation – To a certain extent, the Regulations simplify the issue of determining the jurisdiction and applicable law in the EU. However, the localisation element can be particularly troublesome in an online context, because resources are available from everywhere and the communications infrastructure is deliberately flexible, so that communication can pass an undefined number of servers. The result in many cases is that parties are faced with overlapping and contradictory claims as regards the localisation. The application of the localisation element to the online world can then either produce a reasonable result (when the transaction presents a clear link with the physical world), or a virtually useless result (when the product or service is delivered electronically). Hence, as is often stated, the Regulations do not sufficiently take into account the online context, and are insufficiently clear in their application to Internet disputes.

The following examples illustrate these concerns:

- **Place of delivery** – The place of delivery is one of the factors to determine the jurisdiction for a transaction. Although predictable for typical products in an offline context, the outcome of the "place of delivery" criterion for the electronic delivery of products or services depends on the technology used to deliver the product or service. When the service is provided through e-mail, the place of delivery can either be the location of the server of the mail provider, or the location of the user's personal computer. Conversely, when the service is delivered on an online platform or virtual world, the place of delivery is the location of the server of the service provider. However, using the location of a server (e.g., the web server of the service provider, or the e-mail server of the customer) is problematic, as it may even not be possible to determine the location in cloud computing infrastructures, where data may be distributed across different data centres.

- **Consumers** – With respect to consumers, the Brussels I and Rome I Regulation provide that a consumer can bring litigation against a business either in the consumer's domicile or in the defendant's domicile. Conversely, a business can sue a consumer in the consumer's domicile if the business *pursues commercial or professional activities in the Member State of the consumer's domicile* or, by any means, *directs such activities to that Member State or to several States including that Member State, and the contract falls within the scope of such activities*. It is unclear, however, what "pursue in" and "direct to" mean in ecommerce transactions. Neither concept is further explained in the Regulation itself, and each can encompass a wide range of activities (Is it, for example, sufficient that a website allows to be accessed from everywhere?). The European Council and the Commission later clarified that "it is not sufficient for an undertaking to target its activities at the Member State of the consumer's residence, or at a number of Member

---

19 C. REED, o.c., p. 230  
20 C. REED, o.c., p. 217  
21 e.g., an online order for the physical delivery of goods  
22 C. REED, o.c., p. 223  
23 HÖRNLE, o.c., p. 72  
25 Z. TANG, o.c., p. 44
States including that Member State; a contract must also be concluded within the framework of its activities" and that "the mere fact that an Internet site is accessible is not sufficient for Article 15 to be applicable, although a factor will be that this Internet site solicits the conclusion of distance contracts and that a contract has actually been concluded at a distance, by whatever means." However, the required level of advertising or active selling will be clarified by the ECJ.

Pending cases – Taking into account these ambiguities, it should not surprise that the ECJ has been asked to issue a ruling on the interpretation of these instruments. The following cases are currently pending:

- **Case C-278/09** 27: does a court have jurisdiction for infringement of personal rights allegedly committed by placing on-line of information and/or photographs on a website published in another Member State by a company domiciled in that second State, (i) on the sole condition that that Internet site can be accessed from the first Member State; or (ii) on the sole condition that there is between the harmful act and the territory of the first Member State a link which is sufficient, substantial or significant? Which criteria should be applied when the second condition would be used (number of hits, nationality of plaintiff, language used on the website, …)?

- **C-144/09** 28: Is the fact that a website of the party with whom a consumer has concluded a contract can be consulted on the Internet sufficient to justify a finding that an activity is being "directed", within the terms of Article 15(1)(c) of the Brussels I Regulation?

- **C-585/08** 29: Is it sufficient for the Brussels I regulation to assume that activities are "directed" to a certain Member State if a website can be consulted via the Internet?

### 4. Alternatives to the traditional approach

This section 4 describes various procedures and legal instruments that have emerged in recent years to resolve the dispute resolution conundrum on the Internet.

#### 4.1. Alternative Dispute Resolution

Although traditional court proceedings have since long proved their merits, they also have inherent shortcomings. These shortcomings include the cost of the procedure, the often lengthy trial and the complex question of which law applies and which court is competent to handle a case.30

These shortcomings become even more pronounced in an online environment, where the issues of the applicable law, the competent court and the low value of the disputed transactions can become prohibitive for parties to effectively pursue their rights. As a result, customers may become discouraged to initiate legal proceedings, even when the service provider would be located in the same country as the consumer. However, the threat of lengthy and costly litigation may also discourage online service

---

26 Z. TANG, o.c., p. 44
27 Reference for a preliminary ruling from the Tribunal de grande instance, Paris (France) lodged on 16 July 2009 - Olivier Martinez, Robert Martinez v Société MGN Limited
28 Hotel Alpenhof GesmbH v. Oliver Heller
29 Peter Pammer v. Reederei Karl Schlüter GmbH & Co. KG
30 Green Paper on alternative dispute resolution in civil and commercial law, COM(2002) 196 final, 19 April 2002, nr. 49
providers, particularly medium and small sized businesses — which take up the bulk of the online service providers\textsuperscript{31}.

Alternative dispute resolution (ADR) is widely regarded as holding great promise for the low-cost and efficient resolution of consumer disputes, especially cross-border disputes.

\textit{Note: unless mentioned otherwise, the following paragraphs deal with ADR as a mechanism to deal with disputes ensuing from business-to-business, business-to-consumer and consumer-to-consumer transactions.}

\subsection*{4.1.1. Introduction to alternative dispute resolution}

Alternative dispute resolution is a collective expression for all out-of-court dispute resolution mechanisms that interpose a neutral third party\textsuperscript{32}. The word "alternative" points to the fact that it was originally conceived as an alternative to the traditional, state-court system.

Systems for the out-of-court settlement of disputes differ greatly as regards their structure, operation and implementation\textsuperscript{33}. However, two basic forms of ADR can be recognised: mediation (where the neutral third party tries to broker a settlement between the parties) and arbitration (where the neutral third party makes a binding and enforceable decision as to how the dispute should be resolved). Both types require the parties to agree on the arbitration procedure, although such agreement is often reached before the actual dispute arises\textsuperscript{34}.

\begin{itemize}
\item **Mediation** – During mediation, a third neutral party (the mediator) helps the parties in reaching an amicable settlement, by applying information management skills that encourage the parties to more effectively communicate through rephrasing and better articulation of arguments. The distinctive feature of mediation is that the parties \textit{voluntarily} agree the terms of their settlement. Although mediation, as compared to arbitration or court decisions, can sometimes result in a significantly better outcome for both parties because the mediator will try to dig into the \textit{interests} of both parties in the dispute, only some disputes really lend themselves neatly to mediation. When the underlying interests of the parties cannot be aligned and the case does not lend itself to a compromise, mediation will be of little help\textsuperscript{35}.

Mediation is sometimes also said to be contrary to the notion of justice and fairness, because it tries to make each party's \textit{interests} meet in order to remove the dispute, instead of relying on each party's \textit{rights} (as a court would do)\textsuperscript{36}. For this reason, it is often said that mediation is not an \textit{alternative} to arbitration or court decision, but instead a complement to it that should be tried first\textsuperscript{37}. In fact, when no settlement is reached, mediation is often followed by (expedited) arbitration or expert determination. Mediation is therefore an important method to filter out certain disputes.
\end{itemize}

\textsuperscript{31} Z. TANG, o.c., p. 45
\textsuperscript{34} For example, in cases of domain name disputes
\textsuperscript{35} HÖRNLE, o.c., p. 55
Arbitration – Unlike mediation, arbitration is mandatory: once the parties have submitted to arbitration, they cannot withdraw from the process. Furthermore, mediation is coercive: the arbitration decision ("award") can be directly enforced, similar to a judgment, even cross-border due to the widespread ratification of the New York Convention on the Recognition and Enforcement of Foreign Arbitral Awards. An arbitration decision is also final: once it has been rendered, a court or other arbitrator can no longer handle the same issue (unless the decision would be successfully challenged). For these reasons, only arbitration is a real "alternative" to litigation.

As will be seen below (section 4.2), even more interesting new ways to deal with online disputes can be created when ADR is combined with typical online technologies, in what is typically referred to as "online dispute resolution" (ODR).

4.1.2. Importance of ADR

Growth – There has been an important growth of ADR in all economic areas. Even before the widespread public adoption of the Internet, it was predicted that the use of ADR would grow considerably in the years to come

Recommended by the European Commission – ADR was recognised by the European Commission as one of three approaches to help individual consumers gain access to justice. The Commission published several documents to improve ADR in consumer contracts, such as the Green Paper on alternative dispute resolution in civil and commercial matters, the Recommendation on the principles for out-of-court bodies involved in the consensual resolution of consumer disputes, the Recommendation on the principles applicable to the bodies responsible for out-of-court settlement of consumer disputes, and the proposal for a Directive on certain aspects of mediation in civil and commercial matters.

The European Commission has also supported ADR-related projects, such as the ECC-NET network. The aim of this network is to create consumer confidence by providing information to consumers on their rights, and by assisting them with cross-border disputes. Each Member State that participates in this network, is required to set up a central contact point, to provide consumers with information and support for making a claim towards a business located in another Member State. The network is co-financed by the European Commission and each of the participating countries.

Recommended by the eCommerce Directive – Article 17 of the eCommerce Directive provides in a general manner that Member States should ensure that their legislation does not hamper the use of out-of-court schemes available under national law, for dispute settlement.

Recommended or required by national courts – Some Member States require parties to try a mediation procedure before they are allowed to engage in the traditional litigation procedures. In Portugal and several German Länder, claimants must first resort to ADR before the actual judicial process.

---

38 K. BENYEKHLEF and F. GÉLINAS, p. 11
39 Communication from the Commission on "Enhancing Trust and Confidence in Business-to-Business Electronic Markets", COM(2004) 479 final, 14 July 2004, p. X. The other two approaches are the simplification and improvement of court procedures, and the improvement of communication between consumers and professionals
40 COM(2002) 196 final
41 Commission Recommendation of 4 April 2001
42 Commission Recommendation of 30 March 1998
43 COM(2004) 718 final
44 formerly EEJ-NET
45 OECD, Consumer dispute resolution and redress in the global marketplace, 2006, p. 28
proceedings may begin. In the United Kingdom, the court must encourage the disputants to use ADR to resolve the dispute, although it is not mandatory for the parties themselves to initiate ADR. In Ireland, Germany and Sweden, the court will attempt to achieve a settlement among the parties, even if such is not legally required.

**Used by governments** – A number of member countries have established ADR boards for B2C complaints. For example, in Austria, an arbitration panel was established to resolve disputes relating to energy services; in Denmark, Finland, Norway and Sweden, state-run ADR panels are competent to deal with most commercial consumer disputes; in Greece, there are public ADR panels operating in every prefecture. The Scottish Parliament has also held a historic debate on ADR, and disclosed plans for an ADR Centre in Scotland.

### 4.1.3. Advantages of ADR

**Faster resolution** – When properly channelled, ADR mechanisms enable parties to resolve their disagreements in weeks, instead of years through traditional state court proceedings.

**Greater expertise** – Although state courts have profound knowledge of their national laws, they often lack expertise in specialised or highly technical fields. In ADR procedures, the parties can often select the person they want to serve as their mediator or arbitrator, which can save the parties the time to “educate” the judge. This is particularly important in complex business transactions or technical areas.

**Confidentiality** – Discussions held in ADR proceedings are confidential, and parties can decide how much control over the process they want to retain. Conversely, state proceedings are often held publicly.

**Costs** – ADR proceedings are often said to be cheaper than traditional state court proceedings, and are heralded as a way to significantly reduce litigation costs. This is especially true for mediation, but also to a lesser extent for arbitration. For example, in cross-border disputes, documents often need to be translated into the national law of the state court – in most cases even when the language used is English – which can quickly become costly when large amounts of data are involved. Such translations are not typically needed in ADR proceedings.

### 4.1.4. Limitations of ADR

**Limited use for consumers** – The use of arbitration in consumer contracts is widely restricted in Europe, so that parties would still have to litigate and invoke traditional courts, despite an arbitration clause. For example, the Directive on unfair terms in consumer contracts requires Member States to invalidate any unfair term, “which has not been individually negotiated” and “causes a significant imbalance in the parties' rights and obligations to the detriment of consumer”. Mandatory arbitration agreements are not only explicitly listed as a prohibited unfair term in consumer contracts, they are also

---

46 See [www.casecheck.co.uk/tabid/1421/default.aspx?article=History+is+Made++Mediation 11](http://www.casecheck.co.uk/tabid/1421/default.aspx?article=History+is+Made++Mediation 11)

47 C. RULE, o.c., p. 2

48 M.S. MARTIN, “Keep it online: the Hague Convention and the need for online alternative dispute resolution in international business-to-consumer e-commerce”, *Boston University International Law Journal*, 2002:20, 125, p. 155; HÖRNLE, o.c., p. 70

49 Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, Article 3(1), and provision (q) of the Annex
contrary to the principles set forth in the Recommendation on Certain Aspects of Mediation\textsuperscript{50}. This restriction is retained in the new Proposal for a Directive on Consumer Rights\textsuperscript{51}. Although mandatory arbitration agreements are generally prohibited for consumers in the EU, other "soft" forms of arbitration may be permitted, provided they are individually negotiated, and do not affect consumers' right to resort to court\textsuperscript{52}. It may also be a solution to make arbitration agreements asymmetrically binding, \textit{i.e.} binding businesses only, while consumers remain free to initiate judicial proceedings\textsuperscript{53}.

\textbf{Getting the service provider to agree} – ADR schemes rely on the voluntary participation of parties. Although in specific cases (such as domain name disputes or trustmarks\textsuperscript{54}) a party may have committed in advance to ADR, this is most often not the case in general disputes.

\textbf{No standards} – There are no binding international principles that define procedural safeguards for the accessibility, independence, transparency, and cost of ADR procedures\textsuperscript{55}. Only some principles have been developed by both national states and the private sector\textsuperscript{56}. On the EU-level, the European Commission has issued the Directive on mediation\textsuperscript{57} as well as two recommendations to guide the implementation of ADR services for consumer disputes\textsuperscript{58,59}.

\textbf{Not yet up to its full potential} – A number of surveys suggest that ADR has not yet fulfilled its full potential as a low cost and efficient mechanism for the resolution of business to consumer disputes, either because the cost is still too high for consumers, or because the existence of the procedure is simply not known to disputing parties\textsuperscript{60}.

\section*{4.2. Online Dispute Resolution}

Although there is some disagreement\textsuperscript{61} about its precise scope (particularly in relation to traditional ADR), online dispute resolution (ODR) can be defined as a type of dispute resolution which is performed

\textsuperscript{50} Commission Recommendation of 30 March 1998, section IV, in which it is stated that "The consumer's recourse to the out-of-court procedure may not be the result of a commitment prior to the materialisation of the dispute, where such commitment has the effect of depriving the consumer of his right to bring an action before the courts for the settlement of the dispute."


\textsuperscript{52} Z. TANG, o.c., p. 49

\textsuperscript{53} Ibid.

\textsuperscript{54} T. SCHULTZ, \textit{Online dispute resolution: an overview and selected issues}, United Nations Economic Commission for Europe Forum on Online Dispute Resolution Geneva, 6-7 June 2002, section 3.2

\textsuperscript{55} See, in general, OECD, o.c., p. 18

\textsuperscript{56} For example, The International Chamber of Commerce has issued best practices for online dispute resolution (ODR) in business to consumer and consumer to consumer transactions.


\textsuperscript{58} Commission Recommendation of 30 March 1998

\textsuperscript{59} Commission Recommendation of 4 April 2001

\textsuperscript{60} See S. REILLY, The Need to Develop ADR in Ireland, European Consumer Centre Dublin, 2004, available at http://www.ecic.ie/resources/publications/ADR_development_in_Ireland.pdf. For example, in a 2004 survey of the UK National Consumer Council, it was found that the provision of ADR services to consumers is "ad hoc and presents a lottery for the consumer...[depending] either on the type of problem faced or where the problem arises, and sometimes depending on the ability of the consumer to afford the fees." A 2004 Eurobarometer survey found that 38% of respondents had never heard of bodies, such as arbitrators, ombudsmen, arbitration or conciliation bodies, that could offer an alternative to court action

\textsuperscript{61} See for example, J. KRAUSE, J. "Settling It On the Web: New technology, lower costs enable growth of online dispute resolution", ABA Journal News Now, October 2007: "any mediation, arbitration or dispute resolution that takes place outside of court and at least partially online takes place partially online"; conversely, C. FARAH, "Critical analysis of online dispute resolutions: the optimist, the realist and the bewildered", \textit{Computer and Telecommunications Law Review}, 2005, 11 (4), p.
substantially online, and uses the information processing powers of computers with the networked communication facilities of the Internet to facilitate the resolution of disputes between parties. Although ODR is relatively new, it has deep roots, being based on decades of work in the ADR field.

In ODR proceedings, the different stages of the dispute resolution process are performed through electronic communication means (such as online document management systems, multi-functional ODR platforms, settlement and negotiation software, online documents and forms, chatrooms and instant messaging, e-mail, videoconferencing, voice-over-IP software, etc.). These new techniques can augment the traditional means of resolving disputes.

ODR is said to have great potential to resolve disputes in e-consumer contracts, particularly in small disputes where the costs of the resolution must be kept proportionally low. For this reason, ODR is also often recommended by the European Commission. ODR is less appropriate to be used in fields where legal constraints are higher, such as family law and taxation law, because states are more sensitive to interventions in their sovereignty in these fields.

The majority of European countries have not yet developed ODR systems, and tend to maintain the traditional methods of Alternative Dispute Resolution (ADR) only. However, ODR procedures exist in a variety of contexts, from general disputes to specific disputes (e.g., in online auction sites), as part of a trustmark or seal programme, or on an independent basis. Currently, there are more than 100 ODR providers operating.

### 4.2.1. Types of ODR

"ODR" encompasses a variety of different methods. The most important are set forth below.

**Automated negotiation** – This type of ODR is carried out on an automated software platform, without the involvement of human operators. It usually involves a "blind bidding" negotiation process designed to
facilitate the settlement of the dispute. During this process, each party submits successive secret offers to the platform, which are not revealed to the other party until both parties’ submissions match certain standards (e.g., are within a certain monetary range of each other). This process encourages each party to define the preferred and bottom-line outcome of the dispute. It has proved to be particularly successful with insurance compensations and commercial activities. Automated negotiation is relatively successful, and is offered by many providers\textsuperscript{71}. Examples include Cybersettle and InterSettle.

**Assisted negotiation** – In assisted negotiation, a software platform assists the parties in their internal negotiations (no human arbitrator or mediator intervenes). The ODR service provider offers a variety of instruments to facilitate the negotiation, such as an overview of standard solutions, templates of written agreements, the storage of documents relevant to the dispute and secure sites.

**Online mediation** – Online mediation is the online form of traditional mediation, in which a third neutral person tries to bring the parties to settle by using one of the styles developed for traditional mediation, for instance facilitative or evaluative mediation. The only significant difference with traditional mediation is that the parties communicate online, often using advanced communication platforms that are tailored to specific types of disputes\textsuperscript{72}. For example, online forms can be offered that are focused on the particular type\textsuperscript{73}.

**Online arbitration** – Similar to traditional arbitration, online arbitration involves a third party who is chosen by the parties\textsuperscript{74}, and renders a decision on the case after having heard the relevant arguments and seen the appropriate evidence. The most well-known examples include the UDRP procedure and the .EU domain name dispute resolution process\textsuperscript{75}.

### 4.2.2. ODR success stories

Although ODR has not yet seen widespread adoption, there have been specific areas and ODR initiatives that are recognised as success stories.

**Austrian Internet Ombudsman** – The Austrian Internet Ombudsman was founded in 1999, and handles consumer disputes arising from e-commerce through mediation and arbitration. Austrian residents can initiate a complaint procedure against any business established in an EU Member State. The involvement of the Austrian Internet Ombudsman is free of charge for both parties\textsuperscript{76}. Although participation is not mandatory for web shops, some companies have agreed in advance to cooperate, as part of the Euro-label Trustmark Code of Conduct. In addition, the Ombudsman publishes the names of companies that are unwilling to participate on its website.

The Austrian Internet Ombudsman can be considered as a nice illustration of the capabilities of ODR. In 2006, it worked on 4,750 complaints, with a total of claims amounting to 609,000 EUR\textsuperscript{77}.

**UDRP** – Another successful example of ODR is the WIPO Arbitration and Mediation Centre, which is the dominant ODR provider registered with ICANN under its Uniform Domain Name Dispute Resolution

---

\textsuperscript{71} T. SCHULTZ, o.c., section 2.2

\textsuperscript{72} T. SCHULTZ, o.c., section 2.3

\textsuperscript{73} E.g., if the dispute concerns “non-delivery of goods”, the questions asked on the form are specifically targeted to this kind of dispute. See J. HÖRNLE, o.c., p. 79

\textsuperscript{74} Or nominated by the ODR service provider

\textsuperscript{75} T. SCHULTZ, o.c., section 2.4

\textsuperscript{76} Costs are borne by public funds from Austria and the European Commission

\textsuperscript{77} See J. HÖRNLE, o.c., p. 76 - 77
Policy (UDRP). Since 1999, it has resolved over 25,000 domain name disputes online, involving parties from 144 countries. The UDRP applies primarily to international domains (such as .com, .net, .org and .info), but is also used for a large number of country code top-level domains.

The ICANN UDRP administrative procedure is mandatory to domain name holders, although results are not binding. Panel decisions are enforced by domain name registrars, unless the respondent has filed an appeal to competent court of jurisdiction within a time period of ten days.

.EU – The alternative dispute resolution (ADR) for .EU domain name disputes is provided by an Arbitration Court established in Prague. The Czech Arbitration Court administers ADR Proceedings according to ADR rules, in line with the .EU public policy rules. The Czech Arbitration Court is the only arbitration board that is authorized to resolve domain name disputes regarding .EU domains, and handles complaints in all official EU languages.

Similar to UDRP, the .EU ADR procedure seems to be a very effective and fast way of resolving disputes. Hundreds of disputes have already been solved using ADR. Since the initiation of the first .EU ADR proceeding in 2006, close to 1,000 proceedings have been brought before the Court, and more than 900 decisions have been issued and published.

SquareTrade – SquareTrade was the official online negotiation and mediation service provider for auction platform eBay. Since 2000, it has handled over two million disputes, across 120 countries in five languages. It discontinued its dispute resolution services in early 2008.

During its operational period, SquareTrade was – from a practical point of view – the only formal dispute resolution option that was available to resolve disputes. For eBay seller-buyer disputes, litigation is generally very unattractive (even where no cross-border situation is involved), because the amount at stake is very low. However, the ODR-service of SquareTrade turned out to be very attractive, since it is integrated into the eBay platform on the basis of a cooperation agreement. The dispute resolution procedure was, literally, only one click away from a party's eBay account. Moreover, it was the only option for the resolution of negative feedback disputes.

SquareTrade provided automated negotiation and human-assisted disputed resolution. In the free of charge negotiation phase, the process was fully automated, with parties being guided by multiple choice suggestions on how their dispute might be solved. As a result, most disputes were resolved in the negotiation phase. Only if parties could not agree, a mediator could be invoked, although this resulted in a small charge. In total, 80% of the cases were resolved either through negotiation or mediation.

ECODIR – ECODIR (www.ecodir.org) consists of a consortium of European and North American Universities, as well as some private partners. It was launched in 2001 and ran as a pilot project until June 2003. During this time, ECODIR handled 62 cross-border cases, from over 14 countries.

ECODIR’s dispute resolution process is entirely voluntary, as there are no binding rules that force a party to respond to a claim submitted to ODR. All information relating to the claim, as well as the communication between the disputants and the mediator, take place on a secured private web space.

78 See www.wipo.int/amc/en/center/caseload.html
79 EC Regulation 874/2004
80 See J. GRIFFITH, p. 277-279
82 M. BONNICI, G. PIA, Self-regulation in cyberspace, 2007, p. 186
83 G.P. CALLIESS, o.c., p. 653
ECODIR's popularity has been very limited, primarily because – unlike SquareTrade – there is no direct link between the platform where the disputes arise (e.g., the web shop) and the dispute resolution platform. Furthermore, the remedies offered by ECODIR do not bind the parties. A party relies completely on the goodwill of the other party to actually stick to the agreement reached.

4.2.3. Advantages

All of the advantages of ADR, as set forth in section 4.1.3 above, also apply to ODR. In addition, the following advantages can also be identified.

Integration with the online platform – As ODR procedures rely heavily on IT tools, they can be more easily integrated with the online platform (as was the case, for example, with SquareTrade). It should be pointed out, however, that examples of direct integration have been fairly limited up to now.

Time savings – The use of the Internet creates greater flexibility for the parties to resolve their dispute. Similar to the permanent opening hours of a web shop, parties can submit their claims and reactions around the clock, not just during court hours or arbitration procedures. Traditional court proceedings, on the other hand, often invoke long delays, strict requirements for the submission of documents and various other procedural rules that are liable to create delays for the parties.

Convenience of the procedure – The use of asynchronous communications allows the parties to be prepared to carefully produce their response, without being intimidated by the physical appearance of the other parties.

Costs savings – ODR is less costly than traditional ADR or court proceedings, because there are no travel costs. Such savings are particularly important in low-value disputes, where the cost of a plane ticket is often higher than the value of the disputed transaction.

No geographical limitations – As ODR is not bound to a specific geographical location, parties can rely on expertise from neutral experts around the world. Furthermore, parties can find a solution for their problem even if they are far apart from each other.

4.2.4. Issues surrounding ODR

Need of party consent – Few parties participate voluntarily in a dispute resolution procedure. In most cases, they only participate because they are directly or indirectly forced to do so. This causes no issues for the UDRP procedure (where ownership of a domain name is at stake) or for online auctions such as eBay (where a seller or buyer's reputation is at stake), but can be particularly problematic for other voluntary schemes of dispute resolution, as is – for example – the case with the ECODIR project.

Recognition of decisions – It may be difficult to get ODR awards to be recognised and enforced by courts. For example, the New York Convention requires an authentic original (or duly certified copy) of an award, which must be in writing and signed by the majority of the arbitrators. Although these conditions can be met if electronic documents qualify as writing and electronic signatures are used, such solutions do not correspond to the current wording of the New York Convention, nor to its common interpretation.

---

84 M. BONNICI, o.c., p. 191
85 C. RULE, o.c., p. 6
86 T. SCHULTZ, o.c., section 3.1
Due process – One of the most important advantages of ODR is its speed, which can be reached by using simplified procedures and less formalism than is the case with traditional state court proceedings. However, these formalities in traditional judicial procedures have been introduced for valid reasons, the most important of which is ascertaining due process. Care must be taken to avoid that ODR procedures do not jeopardise due process in their flexibility\textsuperscript{87}.

Viable business model? – The viability of the ODR business model seems to be the major problem, as an ODR service only becomes economically sustainable when it handles large quantities of disputes of a similar nature. The problem is that a for-profit ODR provider must find an equilibrium between fees that are high enough to ensure a viable business model, and fees that are low enough to be proportionate to the amounts in dispute\textsuperscript{88}. This may impact an ODR service provider’s independence and impartiality\textsuperscript{89}.

Lack of face-to-face contact – Although the asymmetric nature of most ODR procedures constitutes a distinct advantage, the lack of face-to-face contact may also prove an important disadvantage, because body language and facial expressions are important components of communications. While videoconferencing and other online technologies may help to compensate this lack of face-to-face contact, they are no substitute for face-to-face meetings in the current state of the technology.

Loss of public oversight – Online disputes may reveal important information about emerging issues (such as defective products, consumer restrictions on digital services, ...) or societal trends (discriminatory practices, unethical business conduct). While authorities should police these issues, they become difficult to monitor in ODR, as ODR procedures are usually confidential.

Digital divide – The so-called “digital divide” between citizens who are proficient in online techniques and citizens who are not, may also constitute an important hurdle to the widespread use of ODR. The ODR procedure requires all parties in a dispute to be rather comfortable with sophisticated web technology\textsuperscript{90}, which may favour those who are more acquainted with the use of computers. It would be advisable neither to impose the use of technology nor to discourage it, taking into consideration all types of individuals and their needs\textsuperscript{91}.

4.2.5. Evaluation

An evaluation of the current state of ODR shows ambivalent characteristics.

On the one hand, ODR has proved to be very successful in specific areas, such as domain name disputes and auction websites. In these areas, ODR-service providers do not only make a very attractive offer for easy accessible, quick, effective, and low-cost dispute resolution, but have also succeeded in integrating their services in the online platform on which the dispute arises\textsuperscript{92}. They have therefore demonstrated to have reached a stage of maturity in these areas\textsuperscript{93}.

On the other hand, ODR shows little success outside its preferred specific areas. The general market of ODR services seems quite volatile, with limited success and recognition among potential customers.

\textsuperscript{87} Ibid.

\textsuperscript{88} M. BONNICI, o.c., p. 207

\textsuperscript{89} T. SCHULTZ, o.c., section 3.3

\textsuperscript{90} T. SCHULTZ, o.c., section 3.4

\textsuperscript{91} P. CORTES, o.c., p. 31

\textsuperscript{92} As was, for example, the case with the integration of the SquareTrade procedure in the eBay platform. See G.P. CALLIESS, o.c., p. 653

\textsuperscript{93} A. PATRIKIOS, o.c., p. 73
This limited success is linked to a variety of factors, the most important being the requirement that parties must consent to the ODR procedure. This is particularly problematic in B2C relationships, where the consumer is the weaker party and the web shop or online service provider does not generally have sufficient incentives to consent to the ODR procedure.

Another important hurdle for the success of general ODR services is the lack of direct integration with the online platform on which the dispute arises. This direct integration increases parties’ awareness of the possibility of ODR, and has been key in the successful SquareTrade procedure.

Nevertheless, we are of the opinion that the existing ODR services are representative of the potential of self-regulation in the resolution of online disputes.

4.3. Small claims procedure

Introduction – Small claims procedures have been described as a "middle ground" between formal civil litigation and alternative dispute resolution⁹⁴. Such a procedure already exists in several Member States⁹⁵, and has now also been adopted at the Community level⁹⁶, following a Green Paper⁹⁷ launched by the European Commission in December 2002.

The same Green Paper also led to the adoption of a European Order for Payment Procedure for uncontested pecuniary cross-border claims⁹⁸. The procedure sets forth minimum standards, compliance with which renders unnecessary any intermediate proceedings in the Member State of enforcement prior to recognition and enforcement. The procedure is primarily administrative, and less substantial than the full, adversarial small claims procedure, which will be dealt with in detail below⁹⁹. However, it is interesting to note that Germany and Austria have developed an IT application for the electronic processing of the European order for payment procedure¹⁰⁰. Such efforts could be extended to make the procedure available online everywhere in Europe.

The Regulation establishing a European small claims procedure aims to provide a Community wide uniform procedure for greatly reducing cross-border litigation costs, as an alternative to the domestic claims procedures. The new procedure is optional, as it is offered as an alternative to the possibilities existing under the national laws of the Member States. It will be applicable from 1 January 2009 in all EU Member States except Denmark, but is limited to cross-border cases.

Procedure – The procedure is (in principle) in writing, so that parties do not need to travel¹⁰¹. To file a claim, the claimant must fill in a standard claim form giving proper details of the claim, the sum demanded, etc. This form then needs to be submitted to the competent court by any means of communication acceptable to the Member State in which the action is taken. Once the court has received the form, it prepares a standard answer form which, together with the supporting documents, is served on the defendant. The defendant must then reply within thirty days. Any counterclaim submitted

---

⁹⁴ OECD, o.c., p. 28
⁹⁵ E.g., the Online Small Claims in Ireland and the Online Money Claim in England and Wales
⁹⁶ Regulation 861/2007 of 11 July 2007 establishing a European small claims procedure
⁹⁷ COM/2002/0746 final
¹⁰⁰ See www.epractice.eu/en/cases/europa
¹⁰¹ The Court can, however, ask the parties to physically appear, if the court deems this necessary for the merits of the case.
by the defendant is served on the claimant in the same way as the original claim was served on the
defendant. Judgment is given in thirty days, and the procedure provides for the direct enforcement of the
court decision, without the need for going through mutual recognition of judgements.

**Scope** – The Regulation deals with claims under 2,000 EUR in value (excluding interest, but including
legal costs), arising in cross-border disputes within the EU. The Regulation covers civil and commercial
matters, including not only consumer disputes, but a range of civil claims, such as personal injury
compensation, disability discrimination and unequal access to services\(^{102}\).

**Use of new technologies** – The Regulation allows the use of new technologies for transferring
information (e.g., evidence) to the court. However, it will be up to the Member States to decide which
means of communication are actually acceptable to them. It can be expected that in due time electronic
communications will be possible for every aspect of the judicial procedure to assist in the resolution of
online, as well as off-line disputes\(^ {103}\).

**Evaluation** – The objective of the Regulation is to create a cost-efficient procedure. This objective can
only be achieved by using electronic tools\(^ {104}\) and other ODR-like facilities. It is therefore regrettable that
the Regulation has missed the opportunity to exhort the extensive use of information technology.
Although it is still too early to evaluate the effectiveness of the Regulation, the Regulation nevertheless
has the potential to increase the effectiveness of redress mechanisms when appropriately assisted with
ICT tools.

### 4.4. Credit card charge backs

Credit card charge backs are remedies offered by payment card issuers to consumers. The actual
protection scheme varies considerably among Member States, and can include anything from the ability
to correct billing errors, to liability limits for unauthorised charges, or redress for non-conforming or non-
delivered goods and services\(^ {105}\). These protections can enhance consumer confidence in the use of
payment cards, and can also constitute consumer-friendly dispute resolution mechanisms.

Credit card charge backs can be a very efficient and practical means to deal with disputes small-value
transactions: they provide the consumer with significant leverage, and tend to equalise the unequal
bargaining power. The threshold towards application is very low, as a consumer does not need to search
for a lawyer, mediator or arbitrator, as he only needs to contact the payment card issuer\(^ {106}\).

The scope of credit card charge backs is, however, very limited. First, it obviously only applies to
purchases made by credit card. Secondly, it only applies to very simple disputes, *e.g.* when the
cardholder denies to have made the recorded purchase.

Even so, this mechanism of easy redress deserves approval. We therefore recommend integration of
similar features in other online payment instruments\(^ {107}\).

\(^{102}\) There are some exceptions, *e.g.* regarding customs, administrative matters, wills and succession, violation of privacy and
rights relating to personality, employment law and social security.

\(^{103}\) P. CORTES, *o.c.*, p. 31

\(^{104}\) Ibid.

\(^{105}\) J. HÖRNLE, *o.c.*, p. 38

\(^{106}\) Z. TANG, *o.c.*, p. 49

\(^{107}\) See section 6.1.1 below
5. Conclusions

The relative anonymity, lack of face-to-face contacts, as well as digital and cross-border nature of the Internet have increased the number of potential conflicts on the Internet.

While traditional state court proceedings have long established their role in the resolution of offline conflicts, there is substantial evidence that they are not able to meet the requirements of the online environment. Parties that want to resolve their dispute through traditional state court proceedings, will encounter difficulties in determining the applicable law and the competent court, and may also face important issues during the actual cross-border enforcement of the judicial decision. Moreover, state court proceedings are often slow, costly and formal, which does not align with the fast-moving nature of (often low-value) transactions on the Internet.

Alternative dispute resolution (ADR) is widely regarded as an alternative to state court proceedings, which can resolve online and offline disputes in an efficient, confidential and cost-effective manner. However, as is the case with state court proceedings, claimants can still be confronted with difficulties to enforce decisions resulting from ADR in case the other party does not comply voluntarily. Nevertheless, there has been an important growth of ADR in all economic areas, even before the widespread public adoption of the Internet. ADR has also been recommended and accelerated by the European Commission, national authorities as well as international institutions (such as the OECD). It is also recommended by the eCommerce Directive, which provides that Member States should ensure that their legislation does not hamper the use of out-of-court schemes.

While ADR proceedings were available before the public adoption of the Internet, the growth of the Internet has brought important new possibilities to ADR. The synergy between ADR and (online) information technology – online dispute resolution (ODR) – holds great promise as a method of resolving disputes that arise online, and for which traditional means of dispute resolution are unavailable or inefficient. Compared to "traditional" ADR, the inherent online characteristics of ODR provide further advantages, such as time savings, cost savings and a convenient procedure. In addition, ODR procedures integrated in online platforms can use reputation mechanisms (such as user rating systems\(^{108}\)), which can increase voluntary compliance with decisions. Numerous ODR service providers are available today, offering a variety of different methods to resolve disputes online, from automated negotiation to assisted negotiation, "blind bidding" and online arbitration.

Although ODR has proved to be very successful in specific areas (such as the UDRP and .EU domain name procedures and the SquareTrade settlement for auction provider eBay), it has seen fairly limited popularity outside these specific areas. Nevertheless, the existing ODR services are representative of the potential of self-regulation in the resolution of online disputes. The most important drawback of ODR is that it requires the parties to consent to the ODR procedure, which is particularly problematic in B2C relationship, where the consumer is the weaker party and the web shop or online service provider does not generally have sufficient incentives to consent to the ODR procedure. The most important other issues surrounding ODR include the recognition of ODR decision and concerns about due process.

The European Commission has recognised these concerns, and has recently adopted the European small claims procedure to resolve cross-border disputes. While some aspects of this new procedure (limitation to cross-border cases, low value of 2,000 EUR; data protection disputes are not covered; lack of adequate provisions supporting ADR and ODR) may hamper the adoption of this procedure, it holds great promise to resolve typical cross-border disputes of limited value, for which traditional court

\(^{108}\) See Chapter II, Section 4.4 for more information on user rating systems.
proceedings or ADR may be too costly or troublesome for parties to undertake. However, as the European small claims procedure has only taken effect in 2009, it is too early to tell whether this procedure will be adequate.

6. **Recommendations**

In this section 6, we provide a list of recommendations to resolve the various issues identified in this chapter. A distinction is made between recommendations that can be implemented on the short term (2010-2015) and recommendations that can be implemented on the mid-term (2015-2020). These time frames align with the relative political and legal difficulty to implement these recommendations, as well as the urgency involved. Hence, the threshold for implementing recommendations for the short term is relatively low, or the urgency involved is rather high. Conversely, recommendations for the mid-term require important legal modifications, or may receive more political resistance.

6.1. **Short term**

6.1.1. **Building in consumer protection in payment facilities**

Getting a service provider to participate has been pointed out as the Achilles heel of online dispute resolution procedures. We therefore recommend the European Commission to facilitate the creation of new payment methods that integrate dispute resolution and/or consumer protection in the core of their payment flow. In addition to the credit card charge backs discussed in section 4.4, we refer to the PayPal Buyer Protection Programme for tangible goods as an example of such (limited) integration of dispute resolution procedures. The PayPal Buyer Protection Programme service was created to counter the media and buyer dissatisfaction for faulty items that are sold through eBay\textsuperscript{109}. At the informal level, PayPal users are obliged to file a dispute and use a dedicated online platform to obtain a solution together with the seller (in some cases, PayPal mediates between the parties). PayPal also allows formal complaints and provides limited insurance.

6.1.2. **Encouraging the use of financial escrow services**

Financial escrow services are a type of self-enforcement\textsuperscript{110}, and can prove an effective means of redress, for both consumers and businesses. With an escrow account, the customer first submits payment to a third party (the escrow company), who verifies the payment and authorises the service provider to provide the service or ship the products ordered. The escrow company then tracks the shipment or delivery of the service, sets a number of days after reception, and pays the service provider unless the customer would file a complaint. The escrow company therefore acts as a secure third party.

As there have been several cases of fraudulent escrow companies, it could be envisaged to submit financial escrow services to a specific regulatory regime and/or encourage the use of trustmarks. In this regard, we refer to our recommendation in the electronic payments chapter of this study.

6.1.3. **Self-regulation of online service providers**

The most optimal type of dispute resolution for a certain online service (wiki, online game, virtual world, discussion forum, auction site, creative platform, etc.), depends on the type of service and the target

\textsuperscript{109} S. MYCOE, *The Great Big Ebay Con*, 2008, p. 44

\textsuperscript{110} T. SCHULTZ, o.c., section 3.2
audience. Consequently, we think self-regulation constitutes the most interesting option to create flexible online dispute resolution procedures.

For reasons of efficiency and better enforcement, these self-regulated dispute resolution procedures should be directly integrated in the platform itself. As pointed out in section 4.2.5 above, such direct integration has been one of the most important success factors of popular ODR procedures, such as the UDRP, .EU and SquareTrade procedures.

As argued in Chapter II.10 (self-regulation), we recommend to create formal technical standards for these self-regulated dispute resolution procedures. Such technical standards can, for example, specify how technical links can be established between a complaint, the user account of the disputing parties and (where relevant) the mediator or arbitrator.

6.1.4. Self-regulation of ODR service providers

In order to counter the various concerns with respect to ODR service providers (see section 4.2.4 above), it can be envisaged to create voluntary accreditation schemes of ODR service providers, similar to the accreditation scheme introduced by the eSignatures Directive. These schemes should encourage ODR to respect certain minimum values, such as:

- **Impartiality** – which is the basic guarantee to ensure that all parties have confidence in the fairness of the ODR procedure. The problem, however, is that ODR service providers are often unilaterally selected and paid by one party. This may cause ODR service providers to lean towards favouring businesses.

- **Transparency** – transparency means that relevant and clear information about the procedure should be available to both parties, preferably on a durable medium. This information must allow each party to understand how the procedure is developing, in order to decide how to react. Furthermore, any agreed solution should be recorded.

- **Fairness** – Fairness primarily aims to protect the consumer as the weaker party. It permits the parties to resort to judicial procedures or other dispute resolution systems before, during, or after the ODR procedure.

6.2. Mid-term

6.2.1. Resolving outstanding ADR/ODR legal questions

As noted in section 4.1.4, it is prohibited to impose mandatory arbitration procedures on consumers. In our opinion, the consumer protection Directives should state that imposing ADR / ODR is allowed towards consumers, under the conditions that the ADR/ODR service provider meets certain minimum quality criteria and that consumers retain the right to resort to court following the ADR/ODR. Such a possibility would be especially useful for dealing with small claims, provided that the ADR/ODR services are made cost-effective to consumers, e.g. through collective funding by online service providers. This

---

111 See M. BONNICI, o.c., p. 206; J. HÖRNLE, "Online Dispute Resolution - More than the Emperor's new clothes.", *Proceedings of the UNECE forum on ODR 2003*, 25
112 See also the Commission communication on out-of-court settlements
113 Z. TANG, o.c., p. 48
recommendation can also be linked to our previous recommendation that self-regulation for ODR service providers should be encouraged.

Another issue that should be resolved to foster the uptake of ADR/ODR, is the compatibility of the New York Convention with ODR awards (as noted in section 4.2.4).

6.2.2. Optimising the rules of private international law

As pointed out in section 3, the application of current legal instruments for private international law raises questions when applied to the online world. In the short to medium term, we think that there is a need either to clarify (e.g. through guidelines by the ECJ) how the rules apply in the online world or to insert specific provisions for the internet.

6.2.3. Introduction of e-courts

This chapter has made clear that it is difficult to find solid solutions to the transnational Internet within the parameters of national law. Even though the European small claims procedure holds great promise for resolving disputes in an efficient manner, it is limited in scope and essentially still relies on national courts. It is therefore frequently said that real solutions to the online dispute resolution conundrum lie outside the national-law framework.\(^{116}\)

In the medium term, we think it is useful to envisage creating EU-level online courts, dedicated to resolving (specific) disputes of civil law that arise in the online world. This court would be specialised in online matters – and its competence would at the same time be limited to online cases – but would in other aspects function like a traditional court, although everything would be handled online, without the necessary physical presence of the parties or their legal representatives. The whole process should be completely digital, and the hearing can be carried out in a more flexible way, e.g. through telephone, audio, video, or e-mail conference.

The idea may seem far-fetched and rather radical at this moment, but is not unrealistic: it has already been proposed in legal literature.\(^{117}\) Also, there are examples that are already operational and resemble an e-court, such as the .EU arbitration panel in Prague (Czech Republic) and the WIPO panels for UDRP procedures, which have proven to be able to efficiently handle cases from very different jurisdictions. In fact, similar to the .EU arbitration panel, we propose that the EU court would also publish its cases (respecting privacy rights of natural persons).

**Difference with state courts** – The proposed e-courts should not be confused with the ongoing efforts in various Member States to modernise traditional courts. Although information technology is not used extensively in the majority of the judicial procedures in the EU,\(^{118}\) several Member States are undertaking efforts to introduce electronic evidence, filings, hearings and testimonies, as well as other electronic documents, or other technologies in courtrooms. In the proposed e-courts, the use of online technologies would be mandatory (instead of optional).

**Advantages** – The e-court would have all the advantages associated with ODR proceedings, such as time savings (it requires no travelling), cost savings and convenience of the procedure (as the entire procedure would be performed online). Provided that a sufficient number of cases is submitted to the e-court, it will also be possible for the judges to specialise in matters, which avoids the current state of

\(^{116}\) U. KOHL, o.c., p. 24

\(^{117}\) See Z. TANG, o.c., p. 50

\(^{118}\) P. CORTES, o.c., p. 30
affairs, where traditional courts must often be "educated" by the parties on the technology or online facility that underlies their dispute.

Compared to other ODR procedures, the most important advantage of the e-court would be that parties cannot refuse cooperation (at the risk of being sanctioned by the e-court). However, a possible modulation of the e-court could be that it would only apply when other means of dispute resolution (such as normal ODR) do not apply, for example because a party (most probably the service provider) refuses to participate. Another important advantage is that e-courts would be more powerful, as their decisions do not need to be recognised by a court in order to be enforced.

**Competence** – In order to make the introduction of the e-court acceptable and realistic, we think it can be envisaged to apply several limitations to the competence of the e-court, at least during the initial phase.

A first restriction would be in the matters handled by the court. We would restrict the competence of the e-court to traditional e-commerce disputes, copyright and trademark infringements, data protection disputes and defamation cases:

- E-commerce disputes would include both services ordered and delivered online (download of software, music, videos or books, as well as access to other content online) and products ordered online.
- Disputes relating to intellectual property rights infringements would be limited to copyright, designs & models and trademark infringements, excluding any patent litigation. In our opinion, patent litigation issues are too complex to handle in a court for which an important goal is the speed and flexibility of its procedure.
- Cross-border data protection / defamation cases are becoming increasingly common, but are particularly difficult to deal with under the current legal instruments. For example, the "Rome II" Regulation on the law applicable to non-contractual obligations, explicitly excludes data protection issues. The same scope exemption applies to the new European small claims procedure.

In the initial phase, we would propose to limit the competence of the e-courts to disputes with a relatively low value (for example uphold a threshold of 4,000 EUR during the pilot phase). In light of the inexperience with the new court medium, cases with a value greater than this amount are probably best left to traditional courts during the start-up phase of the project.

It could also be considered to give e-courts the competence to deal with group proceedings (collective redress). It was already noted by the Commission that there is a need to develop specifically designed instruments for mass claims. The organisation of such proceedings could be greatly enhanced by the use of Web 2.0 tools, which are tailored to cooperation between users.

**Enforceability** – As pointed out above, one of the major obstacles towards each ADR/ODR system is the enforceability of decisions. In this regard, it could be considered to link the decisions of the e-court to the domain names. When online service providers would refuse to comply with the e-court's decision, their domain name could be temporarily suspended (or even permanently blocked), provided that all rights of defence have been respected and all appeal possibilities have been exhausted.

---

119 Should, by the time the e-court is introduced, sufficient self-regulation regimes be developed for ODR service providers, then it could be envisaged to not take into account refusals to cooperate with ODR service providers that are not subject to a decent self-regulatory regime.

While the blocking of a domain name may seem like a harsh decision in reaction to an individual transaction, it should be borne in mind that such blocking is a very efficient tool, which would only be used in case a service provider persistently refuse to comply with the court's decision, which would be similar to "contempt of court" in the offline environment. Also, the blocking of a domain name is practically feasible across the EU, as the number of DNS-operators and large internet access providers is manageable across the EU (preferably, standards should be developed to facilitate how the e-court's decision to block a domain is ultimately rippled down to the access provider's systems).

In a first stage, the blocking of domain names could be limited to .EU domain names, which would then be promoted towards customers as a guaranteed safe shopping haven. National domain names and generic domain names could then join the e-court enforceability mechanism when the system would prove successful.\textsuperscript{121}

**Difficulties** – Some practical difficulties can be expected in the technical aspects, for example how the real identity of parties can be checked, and how effective security can be ensured. However, as technology is rapidly maturing and the introduction of the e-courts is likely not for the immediate future, we think these practical hurdles can be overcome in time.

**Open issues** – There are no reasons why the e-court could not be used between two private individuals. However, the enforceability of decisions between private individuals could be lower than conflicts with service providers, as the leverage obtained from the domain-name blocking mechanism would not apply.

**Applicable law** – The question arises which laws should be applied by the new e-court. As pointed out in section 3 of this chapter, it is often very difficult to determine which law applies to a certain dispute, particularly when it concerns electronic services or tort law cases. These issues could be solved by clarifying the current rules of private international law (as set forth in section 6.2.2 above).

\textsuperscript{121} It should be acknowledged, however, that the blocking of their domain name blocking may not be a sufficient threat to all online service providers (in particular those service providers that do not operate a web site).

Nevertheless, it would also affect these service providers to a certain agree (e.g., because the functioning of their e-mail addresses would be affected).
Chapter 13
Self regulation

1. Introduction

A lack of trust in the safety of internet transactions is the third most important reason for consumers not to engage in online transactions: a recent survey indicates that 42% of respondents do not have confidence in these transactions.\(^{122}\)

In order to counter this trust issue, trustmarks and "web-seals" were introduced as from the late nineties. These trustmarks offer a kind of quality certification system, and are particularly used to foster a consumer’s trust in the merchant’s behaviour — particularly with respect to security, privacy, and general commercial practices. Web shops and online service providers that want to place the trustmark on their website, subscribe to the code of conduct of the trustmark organisation, and typically undergo an audit by the trustmark organisation to guarantee compliance. Trustmarks have therefore become the hallmark of typical self regulation schemes.

However, although they have been around for quite some time, trustmarks have never really taken off. According to recent studies, some EU Member States do not have any trustmark at all. Also, relatively very few web traders belong to trustmark organisations — for example, in the UK and Germany less than 10% of web shops have applied for a trustmark. There is also evidence which suggests that trustmarks have difficulties in achieving brand recognition by consumers and in becoming commercially viable and sustainable operations.\(^{124}\) As a result, there is a very low awareness of trustmarks, with only 10% of EU consumers claiming to have heard of them.\(^{125}\) Moreover, some trustmark organisations have proven to be not as trustworthy as they seem to be, as they did not react at all to obvious breaches of their code of conduct. Instead, the trustmark remained on the breaching merchant’s website at the time the violations occurred and remained there after the wrongful act was discovered.

It may therefore not surprise that trustmarks have not yet lived up their expectations.\(^{127}\) Still, there is evidence that trustmarks can positively contribute to customer confidence in online shopping.

2. Self-regulation in the information society

Self-regulation is not a new concept in the information society, as it has been part of the Internet since its very conception. For example, the inner working of the most fundamental building blocks of the Internet


\(^{123}\) See, for example, TRZASKOWSKI, E-commerce Trustmarks in Europe — an overview and comparison of Trustmarks in the European Union, Iceland and Norway, January 2006


\(^{126}\) P. BALBONI, Third-party liability of trustmark organisations in Europe, p. 11, available at http://arno.uvt.nl/show.cgi?fid=90317

\(^{127}\) European Parliament, Consumer Confidence in the Digital Environment Briefing Note, o.c., p. 10
are based on so-called "Request For Comments", i.e. *de facto* standards developed by the Internet Engineering Task Force, an open standards organisation. Self-regulation is also a well-known concept in the regulation of professions, sports, not-for-profit associations, financial services, insurance, advertising, medical care, environment protection and press\textsuperscript{128}.

### 3. Approaches to self-regulation

Legal literature typically distinguishes between *self-regulation* and *co-regulation*\textsuperscript{129}.

- **Self-regulation (sensu stricto)** refers to the "substitution approach", according to which self-regulation can be used as replacement regulation, until state regulation would be adopted. Once the state intervenes, the self-regulated efforts step aside in favour of the state regulation. Contrary to the "co-regulation" approach described below, self-regulation *sensu stricto* is developed independently of state regulation, and is not situated in a predefined legal framework developed by the state. It implies a minimal legal environment model, which is independent from a state public law framework\textsuperscript{130}.

- **A second approach is "co-regulation"**, where the authority to self-regulate comes from the state, following traditional concepts of delegation of power. The state then entrusts the achievement of its objectives to recognised parties in the field (such as economic operators, social partners, non-governmental organisations or associations), drawing on their practical expertise in order to achieve optimum regulatory results\textsuperscript{131}. All self-regulation should then be developed within the legal framework constructed by the state. Hence, there is a clear hierarchy between state regulation and self-regulation, as state regulation is more authoritative than self-regulation.

The co-regulatory framework is aspired to be dynamic and adaptable to markets, while at the same time being backed by government protection in areas of fundamental importance, such as privacy and consumer protection. The result is claimed to achieve wider "ownership" of the policies and better compliance\textsuperscript{132}, as stakeholders are involved during the preparation and enforcement of the rules. Co-regulation then offers a customised regulatory solution that can fit the policies of a state, while meeting the demands imposed by the technical reality of the Internet. This approach is mainly followed in the European Union.

For the sake of brevity, the term "self-regulation", as used in the remainder of this chapter, refers to both subtypes (unless noted otherwise)\textsuperscript{133} 134.

\textsuperscript{128} BALDWIN and CAVE, *Understanding regulation: theory, strategy and practice*, 1999, p. 125-137

\textsuperscript{129} See, for example, the definitions from the 2003 Inter-institutional Agreement Co-regulation between the Community institutions, the European Parliament, the Council and the Commission

\textsuperscript{130} M. BONNICI, G. PIA, *Self-regulation in cyberspace*, 2007, p. 25


\textsuperscript{132} Commission Communication "European Governance - a white paper", COM(2001) 428 final, 25 July 2001, p. 21

\textsuperscript{133} M. BONNICI, o.c., p. 15

\textsuperscript{134} Some authors (see, for example, J. BONNICI, o.c., p. 15) also recognise a third approach to self-regulation: "hybrid self-regulation". This means that self-regulation is used together with state regulation to create a hybrid regulatory arrangement on the Internet, which contains elements of both state regulation and self-regulation, but can in effect be called neither. In this approach, the state regulation does not give authority to, or exercise control over, self-regulation. Instead, hybrid arrangements are developed for activities that would be problematic for either state regulators or self-regulation to be dealt with. An example is the safe harbour arrangement for data transfers from Europe to the United States.
It should be noted that self-regulation is not necessarily more effective in achieving its regulatory objectives than state regulation, as there is no decisive argument why state involvement means better regulation. In fact, the opposite is often stated. It should also be noted that self-regulation is not a dichotomous situation of "only state regulation" or "only private regulation". Instead, multiple sources of regulation (which also include social norms and technical standards) can be active in parallel in the information society.

4. Types of self-regulation

There exists a wide variety of self-regulatory arrangements, which behave differently in ways that reflect history, government and stakeholder support and engagement, policy domain and area, resources, competition, etc. This section 4 provides an overview of the most common types of self-regulation, including some types for which the self-regulatory nature may not be immediately obvious.

4.1. Codes of conduct

Codes of conduct are the most well-known types of self-regulation.

A code of conduct is a set of rules that outlines the responsibilities of or proper practices for an individual or organisation. Member organisations subscribe to the code of conduct, and undertake to comply with the rules contained in it.

Codes of conduct are also at the core of a trustmark scheme, as it specifies all the obligations of participating shops, e.g. information requirements, mandatory participation in dispute resolution procedures and/or money-back guarantees.

The drafting of codes of conduct is recommended by several Directives, including the eCommerce Directive and the Data Protection Directive.

4.2. Trustmarks

4.2.1. Overview

Trustmarks or "web seals" arose out of the desire for data security and merchant credibility. They are generally considered as useful instruments for policymakers to foster the creation of consumer trust in e-commerce.

Typical trustmark systems are implemented via a vertical, top-down approach to accreditation, whereby an independent, high-level, third party is positioned as the final authority on trust.

---

135 HANS BREDOW INSTITUTE, Final Report Study on Co-Regulation Measures in the Media Sector, Study for the European Commission, Directorate Information Society and Media Unit A1 Audiovisual and Media Policies, June 2006, p. 17
136 See L. LESSIG, *Code and other laws of cyberspace*, 1999, p. 87
139 R. DE BRUIN et al, o.c., p. 22
140 articles 10.2 and 16
141 article 27
If an online service provider fails to meet the trustmark’s requirements, a complaint can be filed. The trustmark provider will then investigate the alleged breach. Depending on the severity of the breach, the investigation can lead to recommendations to remedy the breach, or revocation of the trustmark.

In Europe, the online trustmark phenomenon is still in its infancy\(^\text{142}\), despite the fact that they have existed since the late nineties. Important trustmarks in Europe include Confianza Online (Spain), "Luxembourg e-commerce certified" (Luxembourg), Thuiswinkel (the Netherlands) and Trusted shops (United Kingdom). In the United States, Verisign, TRUSTe and BBB (Better Business Bureau) are the most important examples.

4.2.2. **Shortcomings of trustmarks**

**Recognition by consumers** – A number of studies have been undertaken on the effectiveness of such trust-mark initiatives. These studies derived varying conclusions as to their effectiveness. Some research indicates that, although consumers are aware of trustmarks, the awareness of legitimate trustmarks is dubious, and the actual understanding of what the trustmark effectively represents is relatively poor\(^\text{143}\).

**Low popularity with online service providers** – The percentage of companies who use trust seals is very low\(^\text{144}\). For example, less than 10% of German and UK web shops have subscribed to a trustmark scheme.

**Enforcement of compliance** – Trustmarks have been criticized for not being responsive enough to sanction members that – even repeatedly – violate the trustmark’s code of conduct or policy. Most trustmark organisations do not seem to put in place all possible mechanisms for establishing and monitoring compliance with their specifications\(^\text{145}\).

**Stability of trustmarks** – Due to the difficult business model, trustmarks do not yet offer sufficient stability. Since their boom in 2000 and 2001, many trustmarks have gone out of business, although new trustmark initiatives are still regularly announced. Although there was an initial boom in the establishment of trustmarks immediately after the adoption of the eCommerce Directive, activity in this area slowed down\(^\text{146}\). Already, many trustmarks have gone out of business.

**Poor "EU sensitivity"** – Trustmarks predominantly work only on the domestic level\(^\text{147}\). Most of the trustmark schemes expose a lack of "European sensitivity", i.e. a lack of multilingual information a and lack of co-ordination between the existing EU initiatives regarding consumer confidence\(^\text{148}\).

**Independence and integrity of trustmark-provider** – Trustmark providers are paid by the website operator, which may undermine the independence and integrity of the trustmark provider. Trustmark

---

\(^{142}\) M. BONNICI, o.c.

\(^{143}\) T. MOORES, "Do Consumers Understand the Role of Privacy Seals in eCommerce?", *Communications of the ACM*, March 2005, Vol. 48 No 3


\(^{145}\) R. DE BRUIN et al, o.c., p. 78.

\(^{146}\) Report on E-commerce Directive, p. 16

\(^{147}\) G.P. CALLIESS, "Online Dispute Resolution: Consumer Redress in a Global Market Place", *German Law Journal*, Vol. 7, nr. 8, p. 656

\(^{148}\) R. DE BRUIN et al, o.c., p. 9
organisations can only be considered independent if their funding structure and the composition of their board of directors are neutral. However, this is often not the case.  

**Liability of trustmark-provider** – It is currently not clear to which extent trustmark providers can be held liable by consumers.  

**Continued compliance** – Another issue is that trustmarks reflect that the service provider complied with the trustmark's requirements at the moment of audit. It is debated whether the display of trustmarks illustrates continued compliance, or just compliance at the time the user organisation was audited.  

**Legitimising sub-optimal behaviour** – The very concept of trustmarks is sometimes criticised for legitimising sub-optimal behaviour, as they give consumers the impression that certain behaviour is better-than-average, while it may in fact be less-than-average (for example, with respect to privacy and data protection).  

### 4.3. Technical standards

Technical standards are an essential feature of the Internet. While not their primary intention, technical standards also have (self-)regulatory effects on internet activities, as compliance with technical standards is conforming to acceptable behaviour. Technical standards not only constitute a source of technical and legal rules, but also provide a way to implement rules of states and other entities, as they apply cross-border. Technical standards therefore complement the implementation of rules coming from state legislation.

Although this has been criticised in literature, in fact most technical standards meet all the criteria that are commonly required for a rule to be considered “law”. Most standards are generally applicable to all situations, and are not decided upon on an ad hoc basis. Also, most technical standards are publicly known and available to citizens. Technical standards also have a prospective character, by applying to future situations, and not only to past behaviour. Finally, technical standards are generally consistent with existing higher ranked laws and legal doctrine. Technical standards are therefore a kind of self-regulation in their own way.

### 4.4. Labelling systems, user rating systems and reputation techniques

Labelling systems, user rating systems and similar reputation-based techniques involve a platform where either content is rated, or the quality of service providers is rated (quality of products, richness of information provided, responsiveness after customer care services, ...). Often, comments can also be attached and warnings can be issued about the content or the service provider, which can then be used as guidance for other customers.

**Traditional labelling systems** involve a self-regulatory group that examines content and attaches a certain label, in accordance with predefined rules. They are recommended by the European

---

149 P. BALBONI, o.c., p. 63  
150 P. BALBONI, o.c., p. 14  
151 C. MARSDEN, o.c., p. 225  
152 C. MARSDEN, o.c., p. 234  
153 M. BONNICI, o.c., p. 135  
154 M. BONNICI, o.c., p. 163  
155 The actual use of the standard may, however, require licensing.
Commission\textsuperscript{156} in the context of the Audiovisual Media Services Directive. Examples include the Internet Content Rating Association (ICRA) and the Netherlands Institute for the Classification of Audio-visual Media (NICAM), which are further discussed below.

\textbf{User rating systems}\textsuperscript{157}, on the other hand, constitute a typical example of the consumer use of Web 2.0 technologies to counter the information asymmetry in the environment for trust. They rely on the collective goodwill of participating users. Practice shows, however, that a significant amount of users is willing to make such small contributions to foster the improvement of the community\textsuperscript{158}. Some websites have also adopted these user ratings for rating their own products, services and content\textsuperscript{159}. Other than rating service providers, products and services, they can also used to filter harmful content, select useful comments\textsuperscript{160}, or report inappropriate behaviour\textsuperscript{161}.

\section{5. Importance of self-regulation}

Self-regulation is seen as an important regulation strategy for the EU. It has been advocated by the European Commission, Member States and various experts, and has been invoked by the Commission. Moreover, it is already used in different EU legal instruments.

\subsection{5.1.1. European Commission}

The European Commission is a strong supporter of self-regulation, and has repeatedly recommended self-regulation as a way to improve consumer confidence and gradually resolve issues in the online world\textsuperscript{162}.

In the \textit{“Interinstitutional Agreement on Better Lawmaking”}\textsuperscript{163}, the European Parliament, Council and Commission agreed that co-regulation constitutes an alternative method of regulation, which fits well with the obligation to legislate only where it is necessary and to the principles of subsidiary and proportionality\textsuperscript{164}.

Various documents emanating from the Commission reflect this position, such as the Council Resolution and Commission Communication on illegal and harmful content on the Internet\textsuperscript{165} and the Commission Green Paper on the protection of minors and human dignity in audiovisual and information services\textsuperscript{166}.

\begin{footnotesize}
\begin{enumerate}
\item Examples include epinions.com, ciao.co.uk, www.bizrate.com, www.consumerreview.com, etc.
\item ENISA Position Paper No.1, \textit{Security Issues and Recommendations for Online Social Networks}, October 2007, p. 20
\item C. MARSDEN, \textit{o.c.}, p. 232. Well-known examples include the product ratings on Amazon.com and iTunes
\item \textit{e.g.}, on a discussion forum with many reactions
\item ENISA, \textit{o.c.}, p. 20
\item V. REDING, speech at the ISFE Expert Conference, 26 June 2007
\item 2003/C 321/01
\item HANS BREDOW INSTITUTE, \textit{o.c.}, p. 19
\item See, respectively, OJ C70 6, March 1997 and COM (1996) 487, 16 October 1996
\item COM (1996) 483, 16 October 1996
\end{enumerate}
\end{footnotesize}
5.1.2. Previous studies

Self-regulation has also been recommended by numerous studies undertaken on behalf of the Commission. For example,

- the Bangemann Group Report\(^{167}\) referred to self-regulation as an interesting legal instrument that supports the argument that the EU should only directly regulate itself to ensure the competitiveness and regulatory position of the internal market;

- the use of self-regulation has also been recommended by a recent study on the effectiveness of self-regulation on the Internet, undertaken on behalf of the Commission. In their final report, the contractors argue that "wherever possible, policy should incorporate analysis of [co-regulation and self-regulation organisations], and should be designed with positive incentives for compliance and innovation by [these organisations]"\(^{168}\);

- at the presentation of the study on co-regulation in the media sector and Internet industry, commissioner REDING stated that "self-and co-regulation offer very real alternatives to traditional legislative approaches in the media sector today. Where such self and co-regulatory models are credible and efficient, the European Commission will encourage their use, in particular for the online environment."\(^{169}\).

5.1.3. Existing legal instruments that refer to self-regulation

Self-regulation is already advocated by several Directives in the information society.

- Article 16 of the e-Commerce Directive requires Member States to encourage trade, professional and consumer associations / organisations to draw up codes of conduct to facilitate the implementation of the Directive. Member States should also encourage the involvement of other stakeholders (such as consumer organisations, associations representing the visually impaired and disabled) in the drafting process. Article 16 also requires that these codes of conduct are made accessible by electronic means.

Furthermore, article 10.2 of the eCommerce Directive requires an online service provider to indicate all relevant codes of conduct to which it subscribes and information on how those codes can be consulted electronically.

- Article 27 of the Data Protection Directive instructs Member States to encourage the drawing up of codes of conduct to implement national data protection provisions. The national data protection authorities and Working Party 29 must review the compliance of national or community-level codes of conduct submitted to them.

- In the recital of the Audiovisual Media Services Directive\(^{170}\), it is noted that "experience has shown that both co- and self-regulation instruments, implemented in accordance with the different legal traditions of the Member States, can play an important role in delivering a high level of consumer protection. Measures aimed at achieving public interest objectives in the emerging audiovisual media services sector are more effective if they are taken with the active support of the


\(^{168}\) J. CAVE, o.c., p. xiv


\(^{170}\) nr. 36
service providers themselves" and that "Member States should, in accordance with their different legal traditions, recognise the role which effective self-regulation can play as a complement to the legislative and judicial and/or administrative mechanisms in place".

Article 3.7 of the Directive encourages the adoption of broadly accepted co-regulatory and/or self-regulatory regimes at the national level, which provide for effective enforcement.

6. Advantages and limitations of self-regulation

6.1. Advantages of self-regulation

**Speed** – Self-regulation is typically quicker to establish or change rules, compared to state regulation. Nevertheless, this can diminish with the size and scope of membership and the range of interests represented.

**Expertise** – States may not always have the necessary technical expertise to deal with complex (cross-border) issues, which makes both the adoption and enforcement of state legislation difficult in more difficult scenarios. Conversely, industry players that are involved in self-regulation typically have a detailed knowledge of the issues at stake, as well as possible solutions. In general, the knowledge and expertise is therefore used more effectively in self-regulation schemes.

**Maintaining industry reputation** – Self-regulation can maintain the reputation of an industry sector among customers and consumers. By adhering to a code of conduct, service providers may expect enhanced trust and confidence in their services.

**No unnecessary regulatory costs** – Public policy literatures states that there is always a hidden price for regulation (e.g., in the form of distortion, cost, institutionalisation, agenda creep, etc.). The risk of incurring such societal hidden costs is less pronounced with self-regulation.

**Reduction in state costs associated with regulation** – States are increasingly keen to shift part of the regulatory costs (drafting and enforcement) to the private sector. Although states frequently contribute to self-regulatory initiatives, self-regulatory initiatives can generally reduce legislation costs.

**Cross-border enforcement** – Although the effective enforcement of self-regulatory initiatives is a disadvantage rather than an advantage of self-regulation (see below, section 6.2), it should be pointed out that self-regulatory initiatives that integrate realistic sanctions in their enforcement model, can better apply cross-border enforcement, compared to state legislation. Furthermore, state law enforcement agencies do not always have the necessary technical tools and access to enforce the state rules on the Internet.

**Laying the groundwork** – When states would eventually introduce legislation in an area that is already regulated by self-regulatory initiatives, states often recognise the usefulness of the self-regulation rules, and adopt them in their legislation. Even when state regulation would eventually uphold a different position than the position taken by self-regulation, self-regulation can still be an important source for the development of new legal frameworks.

---

171 See, in general, J. CAVE, o.c., p. 48
172 M. BONNICI, o.c., p. 85
173 For example, the UDRP or .EU procedures, where the cancellation or transfer of the disputed domain name is obviously a very effective sanction.
174 M. BONNICI, o.c., p. 75
state position. It will, as a minimum, provide a point of departure for the route state regulation will — or will not — follow\textsuperscript{175}.

**Assisting state regulation enforcement** – Self-regulatory initiatives can assist the enforcement of state regulation, for example by offering "hotlines" and reporting channels where members or third parties can submit complaints of breaches.

### 6.2. Primary disadvantages and limitations of self-regulation

#### 6.2.1. Difficulties to enforce

Even though self-regulation can deliver interesting results when all members comply with the agreed rules, the effective enforcement of the rules by the members remains a brittle point, particularly when the self-regulatory organisation lacks effective sanctions, or lacks the information necessary to verify non-compliance\textsuperscript{176}.

Enforcement can come from different angles:

- **Reputation** – Internet service / access providers cannot afford a bad reputation, because reputation is one of their most significant intangible resources\textsuperscript{177}. They will therefore often be inclined to sign up to a self-regulatory initiative and comply with the agreed rules, in order to preserve their good reputation.

- **State** – In some cases, the state requests compliance with the self-regulatory rules. For example, the Australian Communications Authority requests member of the Australian Internet Industry Association and the Australian Direct Marketing Association to comply with the rules developed by these organisations\textsuperscript{178}.

- **Contract** – Self-regulation organisations may have contractually agreed that a non-complying member will pay monetary damages, or lose certain securities.

- **Code** – Enforcement can also occur through software code. Although this may not be immediately apparent, the technical architecture of the Internet has become an instrument of control. Indeed, software (programming code) can control activities more perfectly and more completely than traditional state rules and sanctions\textsuperscript{179}. Software has therefore assumed a central role in the Internet governance debate\textsuperscript{180}. It can define who can access a certain website, who can access certain content protected by technical protection measures\textsuperscript{181}, etc.

As a result, self-regulatory organisations must not necessarily rely on state authorities to achieve effective enforcement through software code ("self-enforcement")\textsuperscript{182}. When they can make their

\textsuperscript{175} M. BONNICI, o.c., p. 57-58

\textsuperscript{176} J. CAVE, o.c., p. 48

\textsuperscript{177} S.C. ZYGLOPOULOS, "The social and environmental responsibilities of multinationals: evidence from the Brent Spar case", *Journal of Business Ethics*, Vol. 36, issue 1, p. 141-152

\textsuperscript{178} M. BONNICI, o.c., p. 66

\textsuperscript{179} M. BONNICI, o.c., p. 132

\textsuperscript{180} Summarised in the phrase "code is law", after Lawrence Lessig's *Code and Other Laws of Cyberspace*

\textsuperscript{181} See, for example, the Content Scramble System (CSS) used on DVDs, the protection of Adobe Acrobat eBook Readers, or the "FairPlay" content protection system used by Apple's iTunes.

\textsuperscript{182} PATRIKIOS II, p. 131
members dependent on specific software, they can enforce compliant behaviour through software. Of course, it should be recognised that not all of online behaviour can be controlled through code.  

6.2.2. Getting all players on board

Related to the issue of enforcement, is the issue that self-enforcement can only be really effective when a majority of relevant entities sign up to the self-regulatory initiative. Even though it is not necessary to attract all players in the first stage – the attractiveness of the self-regulatory regime often attracts remaining players in a second stage – there is the issue that the real "baddies" never join the self-regulatory initiative.

6.3. Secondary disadvantages and limitations of self-regulation

Protecting the users – Self-regulation is often used as a mechanism by industry players to balance interests, or to prevent state intervention in a certain area. Although self-regulation is at several levels intended to protect users, it should be recognized that it does not always sufficiently protect the fundamental rights of users, who are typically not involved in the drafting process of the rules. Conversely, the democratic institutions of countries are said to ensure a proper degree of user involvement and protection in the drafting process of traditional legislation.

Binding the users – Another criticism is that self-regulation can indirectly bind end-users, although these users have not been involved in the drafting process. It should be pointed out, however, that this indirect binding is not the case for all types of self regulation. In fact, self-regulatory initiatives often leave the decision up to users (as is the case with, for example, privacy filters, content filters and rating systems).

Protecting the public interest – Similar to the objection that self-regulation would not adequately protect the user, it is argued that self-regulation does not adequately protect the public interest, as self-regulation primarily protects the interests of a specific group of industry players.

Legitimacy and accountability – There are concerns about the degree to which self-regulation organisations are willing to adhere to principles of good regulation, such as transparency, accountability, proportionality and consistency.

Anti-competitive effects – Depending on its purpose and participants, self-regulation may have anti-competitive effects. For example, when well-established companies enter into agreements within a co-regulatory framework, this may hinder the market entry of competitors.

Possible lack of clarity – Self-regulatory initiatives are often taken in response to specific issues. Rules of self-regulation may therefore develop in an ad hoc and accidental manner, effectively creating a decentralised patchwork of initiatives. Consumers (and others) may be confused about the level of

183 SCHONBERGER, p. 17
184 J. CAVE, o.c., p. 29
185 E.g., codes of conduct that establish how online service providers should deal with a user's personal data.
186 M. BONNICI, o.c., p. 61
187 J. CAVE, o.c., p. 50
188 J. CAVE, o.c., p. 48
189 M. BONNICI, o.c., p. 67
compliance to expect or the consequences of dealing with non-complying or non-participating firms. The risk of confusion is magnified when industry players are unable to agree on a single code or standard 190.

7. Some examples of self-regulation

7.1. Internet content

States are often reluctant to regulate harmful content, as they risk being accused of censorship. Internet content regulation is also problematic on an international level, where countries are often unable to agree on regulation to deal with harmful content 191. What can be considered illegal in one country, may be considered merely harmful (or even perfectly legal) in another country 192.

Self-regulation can therefore play an important role in the fight against illegal content. Funding self-regulation initiatives can then prove to be a more practical approach 193.

Self-regulation is indeed often the first to provide a set of rules to regulate internet content. This has been the case, for example, with the development of notice-and-takedown rules, which were first adopted by internet access providers, and were subsequently adopted in national legislation and the eCommerce Directive 194.

7.1.1. EU-level

The EU has long recognised that the only real option for regulating harmful content is through self-regulation. In the Green Paper on the protection of minors and human dignity on the Internet 195, it was stated that “because of the varying cultural and social norms, self-regulation (...) will provide the most suitable solution for the regulation of harmful content”. As from 1997, the European Commission has funded initiatives to support illegal content hotlines, with the Safer Internet Action Plan is the most important example.

7.1.2. National level

On a national level, there are several examples of successful self-regulatory regimes to deal with harmful content.

PhonePayPlus – PhonePayPlus (formerly "ICSTIS") is an independent regulatory body responsible for creating a Code of Practice, which must be complied with by all UK premium rate service providers. There is a range of sanctions than can be imposed (including very powerful financial penalties) if a service provider is found to have breached the Code of Practice. The Code of Practice also includes general requirements for network providers to assist in its regulation of companies offering premium rate services. PhonePayPlus runs a complaints hotline which received over 131,000 calls in 2006 and 2007 196.

190 J. CAVE, o.c., p. 48
191 See M. BONNICI, o.c., p. 36
192 M. BONNICI, o.c., p. 36
193 M. BONNICI, o.c., p. 46-47
194 M. BONNICI, o.c., p. 82
195 OJ C287, 22 September 1997, p. 11
196 C. MARSDEN, o.c., p. 146
ICRA – ICRA, the Internet Content Rating Association, has developed a set of content descriptors to label or rate content. These descriptors were determined through a process of consultation with various stakeholders. Online service providers can use the ICRA logo (for example, on their website) if the content they publish is in accordance with the ICRA descriptors, and also complies with ICRA’s terms and conditions. ICRA is an example of a filtering system that strives for minimal self-regulation, permitting maximum end-user choice.

There seems to be agreement that ICRA is a technology that is a great idea, but lacks effectiveness due to the lack of mandatory participation. While interest in ICRA was high in the late 1990s, interest seems to have declined since that time.

NICAM – The Netherlands Institute for the Classification of Audio-visual Media (NICAM) classifies media content in the Netherlands. It grew from a consensus decision on a pan-media system of self-regulation, in order to replace the state regulation model in place. The system is mandated by Parliament, and reports to Parliament. More than 2,200 companies and organisations are affiliated to NICAM, which is considered a transparent and widely adopted system.

NICAM is responsible for the "Kijkwijzer" scheme, through which media content providers code their programming according to fixed categories of content type. Kijkwijzer warns parents and educators about a television programme or film which can be harmful to children of different ages. Any citizen can complain to the Kijkwijzer system, following which a commission evaluates the complaint. If the complaints are upheld, the Complaints Committee can enforce fines on the participating organisations.

Although the intention was initially to phase out the involvement of the government, an entirely self-regulatory body was not found to be desirable for classifying audiovisual content. Therefore, it was decided to keep some oversight and financial contributions from the Dutch Ministry. Participation is voluntary, there is strong participation level among audiovisual companies, as companies that do not participate will fall under the governmental regulatory regime.

7.1.3. Japan

In Japan, online malls such as Rakuten (www.rakuten.co.jp) have been developed, on which thousands of retailers are established. Rakuten can be considered a new type of trustmark, as millions of customers trust the online retailers that are admitted to the online mall. Rakuten guarantees that customers get their money back when a product or service would be defect, or when a service provider would go bankrupt.

Rakuten is therefore yet another example of the possible success of trustmarks, and the requirement that trustmarks must give some added value on top of merely suggesting trustworthiness.

7.2. Technical standards

As noted in section 4.3, technical standards have always played an essential role on the Internet. Successful technical standards organisations are therefore not difficult to find.

---

197 Ibid., p. 80
198 Ibid., p. 159
199 Ibid., p. 165
200 Ibid., p. 160
IETF – The principal standards-setting body for the Internet is the Internet Engineering Task Force (IETF), which is an open international organisation of parties involved in network infrastructure\textsuperscript{201}. The IETF’s main activity is developing and publishing “Requests For Comment” documents\textsuperscript{202}. The IETF is a volunteer organisation which has been enormously successful at driving the continued evolution of the Internet, and introducing many standards. It is also heralded as one of the most open and transparent organisations involved in standardisation.

W3C – Another important organisation involved in technical standards on the Internet is W3C, which has as its central mission the development of standards for the world wide web (e.g., HTML). Contrary to the IETF, the W3C is sometimes criticised for being a victim of its own success, with the accusation that it is captured by its corporate clients, and is not sufficiently focused on developer needs in the start-up community\textsuperscript{203}. Even so, it is also recognised for its introduction of many important standards, which are – for example – used in all web browsers.

8. Second-level self-regulation on online platforms

Online platforms are an interesting new territory for the application of self-regulatory principles, as they raise the question to which extent the users of the platforms can take self-regulatory initiatives and/or participate in the governance of the platform. In effect, such initiatives could be called “second-level” self-regulation, as they emanate by the users in the platform. This section 8 provides an overview of self-regulatory initiatives on online platforms, with particular focus on user involvement.

8.1. Social communities

Recently, several self-regulatory initiatives have been undertaken by social community websites:

- **Safer Social Networking Principles** – On 10 February 2009, several leading social community websites — including Facebook, MySpace, Netlog and Google/YouTube — adopted the “Safer Social Networking Principles for the EU”, developed in consultation with the European Commission and a number of nongovernmental organisations, in the framework of the “Safer Internet Programme”. The Principles focus on the safety and protection of children and young people, with specific focus on cyber-bullying, grooming and risky behaviour, like revealing personal information. The Principles aim to mitigate such risks, inter alia by providing a “report abuse” button on the website, making sure that the privacy settings of minors are set to private by default, ensuring that private profiles of minors are not searchable, and guaranteeing that privacy options are prominent and accessible at all times.

- **Facebook user involvement** – In response to fierce user reactions following the surreptitious changing of its terms & conditions, social community site Facebook announced in February 2009 a new approach as to how the company would create future policies that impact user privacy. Facebook has developed a set of self-regulatory controls, and has also invited users to comment on these controls\textsuperscript{204}. The new approach is described as “a set of values that will guide the development of the service, and Statement of Rights and Responsibilities that make clear Facebook's and users' commitments related to the service." A core part is that Facebook will notify the community of all

\textsuperscript{201} Ibid., p. 51
\textsuperscript{202} Ibid., p. 56
\textsuperscript{203} Ibid., p. 61
\textsuperscript{204} See www.facebook.com/press/releases.php?p=85587
policy changes in the website, and will allow a period of time for Facebook users to comment. If these user comments or interest would reach a certain threshold, then the change could even be voted on by the community. Facebook also announced that it would establish a "user council" to participate more closely in the development and discussion of policies and practices.

- **MySpace agreement with US attorney generals** – On 14 January 2008, social networking website operator MySpace announced a joint effort with 49 state Attorneys General to better protect children online\(^\text{205}\). Similar to the EU Safer Social Networking Principles, this effort tries to combat harmful material (such as pornography, harassment, cyberbullying and identity theft), better educate parents and schools about online threats, cooperate with law enforcement, and introduce various other security measures (e.g., mechanisms to protect minors, age verification, as well as an opt-out registry for parents).

## 8.2. Wikipedia

Wikipedia is the well-known free, multilingual encyclopaedia project supported by the non-profit Wikimedia Foundation. Wikipedia's more than 13 million articles have been written collaboratively by volunteers around the world, and almost all of its articles can be edited by anyone who can access the Wikipedia website\(^\text{206}\). The intrinsic openness of Wikipedia attracted increasing numbers of contributors and quickly developed a life of its own\(^\text{207}\).

**Early governance model** – In the early stages of Wikipedia, Wikipedia's administrators argued that there was a need for participants more than rules, as well as a need to gain experience with how wikis worked, so the only rule was that "there is no rule" to use Wikipedia. In a first stage, "force of personality" and "shaming" were the only means used to control contributors, which was coined "good natured anarchy"\(^\text{208}\).

**Evolving model** – However, in a study on the conflict and coordination costs of Wikipedia, it was noted that there was a significant increase in regulatory costs over time: "...direct work on articles is decreasing, while indirect work such as discussions, procedure, user coordination, and maintenance activity (such as reverts and anti-vandalism) is increasing"\(^\text{209}\). To cope with this, the "zero rule" was replaced with a set of permissions, obligations, rules and norms, documented in guidelines and etiquettes, as well as embedded in code. Nevertheless, there are relatively few means of formal control, so that the community mainly relies on informal or "soft" controls. The openness of the wiki platform and the low cost of joining and leaving precludes formal control as a primary means for governance\(^\text{210}\).

**Editing possibilities** – Wikipedia recognises special "editors", who generally have detailed knowledge about specific subjects, hold electable positions and have special rights on the website (e.g., the ability to delete a page or protect it from being edited by others). As a result, editors can exercise a certain degree of authority. However, even editors do not hold privileged positions in the community: many Wikipedia


\(^{208}\) P. 6


\(^{210}\) C. GOLDSPIN, o.c., p. 14
participants consider the editors as mere janitors, whose behaviour is held to certain higher standards, but whose authoritative power is fairly limited\textsuperscript{211}.

After all, even Wikipedia's policy pages can be edited, like any other encyclopaedia article. The prerogatives of the administrators (and the founder) are not well defined. Whenever a user is no longer satisfied with the governance model or evolution of Wikipedia, he can "fork" the project (i.e., take all the content and copy it to a new website).

**Evaluation** – Wikipedia's model of governance seems very difficult to categorize: characterizations range from anarchy to democracy, dictatorship, a hybrid model, or an adhocracy (i.e., self-governing institution)\textsuperscript{212}. Even so, compared with platforms run by commercial entities, Wikipedia is self-controlled, and allows ample opportunities of user involvement.

### 8.3. Virtual worlds

#### 8.3.1. Overview

Although virtual worlds have existed for quite some time, they have only really taken off since about 2003. The most ubiquitous examples of virtual environments are multiplayer online games such as "Second Life" and Massive Multiplayer Online Role Playing Games (MMORPGs).

For those who are unfamiliar with virtual worlds, these problems may seem largely theoretical or of little economic relevance. However, in-world disputes have the potential to extend into the real world. For example, in 2008, Second Life had over fifteen million users who collectively spent more than twenty million dollars in the virtual world every month. When the virtual banking industry collapsed in Second Life, users lost an estimated $750,000 in real-world money in the virtual economy. Linden Lab initially refused to take action to solve this problem\textsuperscript{213}, although it eventually set up a Second Life Securities Exchange Act, to provide market stability and investor confidence\textsuperscript{214}.

**User participation** – In general, the rules of the virtual world, as well as the possibility for users to participate in the rule making process, are made by the virtual world provider, which does not typically offer any guarantee of transparency or democratic participation to the users.

However, there are also numerous examples of failed attempts to introduce such democratic participation\textsuperscript{215}. Faced with this issue, providers therefore choose to retain control\textsuperscript{216}. As a result, virtual world providers find it very difficult to create an enforcement process that is both efficient and responsive to the expectations of users\textsuperscript{217}.

**Enforcement through code** – Virtual world providers can easily rely on software ("code is law") to enforce rules. Participants who violate the rules can be expelled from the virtual world\textsuperscript{218}, which can be

---


\textsuperscript{212} P. KONIECZNY, *o.c.*, p. 5


\textsuperscript{214} C. MARSDEN, *o.c.*, I, p. 198


\textsuperscript{216} V. MAYER-SCHÖNBERGER and J. CROWLEY, *o.c.*, p. 23

\textsuperscript{217} V. MAYER-SCHÖNBERGER and J. CROWLEY, *o.c.*, p. 25; STOUP, *o.c.*, p. 330

\textsuperscript{218} V. MAYER-SCHÖNBERGER and J. CROWLEY, *o.c.*, p. 17
an effective enforcement mechanism because participants will incur significant costs when they are forced to leave\textsuperscript{219}.

### 8.3.2. LambdaMOO

An early example of a virtual world is LambdaMOO, an online virtual reality system to which multiple users (players) are connected at the same time. It can be considered a predecessor of today's online games.

**The Mr. Bungle incident** – LambdaMOO is famous for its governance incident regarding a user\textsuperscript{220} called "Mr. Bungle"\textsuperscript{221}, who committed virtual rape against other users of LambdaMOO. While the community was arguing on how to react to these virtual crimes, a senior administrator took unilateral action by destroying the character of Mr. Bungle, thus permanently eliminating the character from the community. This case led to a kind of political awakening on LambdaMOO\textsuperscript{222}, which made users realise that they needed rules to govern their virtual community. As a result, a petition mechanism was installed, which allowed the community to propose and vote on new policies and other administrative actions. However, this system suffered quite a lot of evolution, and was ultimately reduced to a state where administrators ("wizards") took back the control of the users, although the ballot system was maintained as a way for the users to express their opinions\textsuperscript{223}.

### 8.3.3. Second Life

Second Life is an online virtual world developed by Linden Lab, which launched in 2003. Its users, ("residents") can interact with each other through their alter ego's ("avatars") to explore the virtual worlds, meet other residents, participate in activities, and create and trade virtual property and services\textsuperscript{224}.

**Governance** – Linden Lab applies a set of terms & conditions, in which it reserves the right to maintain control of in-world activity by suspending or terminating accounts\textsuperscript{225}. Linden Lab also imposes compliance with the "Community Standards" agreement\textsuperscript{226}. The latter agreement sets forth six behaviours that may result in account suspension or expulsion from Second Life\textsuperscript{227}.

However, Linden Lab has taken the position to minimise its "in-world" authority. It considers itself as a platform, rather than an administrator or government, leaving dispute resolutions to its residents\textsuperscript{228}. Even though Linden Lab encourages the development user governance initiatives, and offers moderators to resolve disputes, it considers Second Life a private space, which should be left to private rulemaking. This should not surprise, because the massive scale of Second Life makes it very difficult for Linden Lab to effectively monitor all user interactions\textsuperscript{229}. In any case, Linden Lab is hesitant to terminate user

\textsuperscript{219} They have to leave their identity (avatar), their virtual property, their network of virtual friends, etc.

\textsuperscript{220} actually, it concerned a group of undergraduates sharing a single identity

\textsuperscript{221} See L. LESSIG, Code v 2.0, p. 98

\textsuperscript{222} See J. GOLDSMITH and T. WU, Who controls the Internet? Illusions of borderless world, p. 15

\textsuperscript{223} See http://en.wikipedia.org/wiki/Lambdamoo

\textsuperscript{224} See http://en.wikipedia.org/wiki/Second_Life


\textsuperscript{226} C. MARSDEN, o.c. I, p. 196

\textsuperscript{227} intolerance, harassment, assault, disclosure, indecency, and disturbing the peace. See CHIN, p. 1325

\textsuperscript{228} V. MAYER-SCHÖNBERGER and J. CROWLEY, o.c., p. 25

\textsuperscript{229} P. STOUP, o.c., p. 328
accounts, as there have already been precedents where state court proceedings have been initiated against Linden Lab due to a dispute with a resident\textsuperscript{230}.

As a result, self-regulation in the form of norms established by users have become very important, and many residents take active part in the monitoring of offending behaviour\textsuperscript{231}. Some argue, however, that Linden Lab should create a more comprehensive penal code, which needs to outline the specific punishment for a particular behaviour. Such penal code would have the additional benefit of educating real-world courts about the important norms or objectives in the virtual world\textsuperscript{232}.

\section*{8.4. Conclusion}

The creation of legal rules on user involvement of online platforms is largely undiscovered legal territory. Although user involvement initiatives are slowly creeping into online platforms, these initiatives seem to be largely taken out of self-interest, for example due to threats for imminent legislation (\textit{e.g.}, MySpace\textsuperscript{233}) or for commercial reasons (\textit{e.g.}, the public outcry of Facebook's user community after the surreptitious modification of the terms & conditions).

While these initiatives introduce some democratic elements in the online platforms, the actual participation remains largely superficial. As rightfully pointed out by by L. LESSIG: \textit{"These [platforms] are all democracy-like. But they are not democracy. Democracy is the practice of the people choosing the rules that will govern a particular place. And with the exception of Wikipedia, and there are very few major Internet or cyberspace institutions that run by the rule of the people"}\textsuperscript{234}

For the time being, the legal terms & conditions of platforms run by commercial entities qualify as the "Constitution" of the online platform, which can be unilaterally changed by the service provider, with only marginal involvement of the users. These terms & conditions are often supplemented by rules of conduct, which dictate the appropriate behaviour and rights of users and the service providers themselves. Together, the terms & conditions and rules of conduct constitute the crossover between cyberspace and the real world\textsuperscript{235}. Although platform owners can use software code to enforce user behaviour, terms & conditions can be more time and cost efficient, if online because codes only limit (do not eliminate) conflicts.

When the social importance of the online platforms will keep growing, the question arises whether this situation should not be regulated — if not by state regulation, then by self-regulation. Although we think it is too early to interfere with these platforms (particularly virtual worlds), this issue should be monitored, as anecdotal evidence suggests that issues are rising.

It may, however, be interesting to adopt self-regulation which creates norms and minimum rights for user involvement in large online communities.

\begin{thebibliography}{9}
\bibitem{230} P. STOUP, o.c., p. 331
\bibitem{231} P. STOUP, o.c., p. 328
\bibitem{232} P. STOUP, o.c., p. 337
\bibitem{233} For example, the attorneys general with whom MySpace had entered into an agreement, confirmed that they wanted to avoid legal action against social-networking sites, because \textit{"litigation is costly, time-consuming, (and) uncertain in its result"}.\textsuperscript{234}
\bibitem{234} L. LESSIG, \textit{Code v2.0}, p. 285
\bibitem{235} B. CHIN, p. 1317
\end{thebibliography}
9. General evaluation of self-regulatory initiatives

9.1. Success criteria

From the analysis above, the following success criteria can be deducted for self-regulation to flourish:

- **Difficulty to receive political consensus** – as the drafting process of the Cybercrime Convention showed, it can be very difficult to achieve a political agreement between a large number of countries. For those situations where regulation is necessary, but political agreements are not viable in the near future (e.g., regulation of harmful content), self-regulation can be an important option.

- **Difficulty to enforce regulation** – Self-regulation can also be an important type of regulation when traditional, state-emanated regulation cannot properly enforce regulation, either due to technical difficulties, or due to the inherent cross-border nature of the Internet.

- **Interference with emerging technologies** – Interfering with emerging technologies is generally not a recommended policy option that enables further maturing of the technology. Self-regulation can constitute an important alternative, as it allows the sector to regulate those areas that are most important, while keeping flexibility options open in the future.

- **National level is too limited** – Self-regulation constitutes an interesting tool for those areas where the national level is too limited. For example, although a Member State could impose various quality criteria on its national web shops, these quality criteria will not increase the trust of foreign consumers. Conversely, EU-level trustmarks or codes of conduct can diminish the threshold for a consumer to shop in foreign web shops.

- **Distribution of monitoring workload** – Self-regulation is also particularly useful when the workload to monitor compliance is very high, as is – for example – the case with labelling harmful content. Self-regulatory regimes can distribute the workload among many parties, and also install “hotlines” where users and other third parties can submit complaints.

9.2. Requirements for all self-regulation initiatives

**Consensus between all stakeholders** – To be efficient, self-regulation must reflect a consensus between all relevant stakeholders. Self-regulatory organisations must involve consumers, enforcement bodies and other stakeholders throughout the preparation of the rules. This is a key success factor in making sure that consumer codes of practice are relevant to real consumer needs.

**Effective sanctions** – Self-regulators must adopt a range of sanctions for handling non-compliance by members. Preferably, more than one possible sanction is adopted, whereby the various sanctions can be escalated (e.g., warning letters, fines, termination of membership, for dealing with non-compliance, ...), or combined. All sanctions must be commensurate with the nature of the breach, as well as the repetition/frequency of breaches by the same member. Furthermore, systems and policies for handling breaches should be built into the design of the self-regulatory initiative.

---

236 For example, the drafting process of the Cybercrime Convention – which took more than five years – demonstrates the (almost) unassailable differences between the treaty states. As regards illegal content, the only consensus reached concerned child pornography.

237 Commission communication B2B, p. 8; Office of Fair Trading, p. 11

238 R. DE BRUIN et al, o.c., p. 7

239 Office of Fair Trading, p. 40
Dispute resolution – (Where relevant), the self-regulatory initiative must install a low-cost, responsive, transparent and user-friendly alternative dispute resolution mechanism, which is binding on members. Where possible, the redress scheme should be free to consumers, must be independent from the self-regulation organisation, and must not mandate assistance of a legal representative240.

Governance – Self-regulation organisations must be accountable and capable of following open procedures. Particularly trustmark schemes must be transparent in order to increase consumer trust241. For example, the criteria used to assign a trustmark, and the way in which compliance is verified, must be transparent and effectively applied.

EU-level. Self-regulatory initiatives should, preferably, target the entire EU, and should provide bilingual or multilingual information to foster cross-border confidence242.

10. Conclusions

1. As is the case with many other complex issues on the Internet, there is no silver bullet in internet regulation. The digital and cross-border nature of the Internet challenges many of the assumptions underlying traditional regulation, in particular the jurisdictional reach of a country and the possibility to enforce measures.

2. Self-regulation is not a new answer to these challenges, and has actually been part of the Internet since its early conception, although it has not been the sole form of regulation on the Internet243. There are several examples where self-regulation has flourished in specific areas, but even more examples where self-regulation has proved to be largely unsuccessful. Hence, self-regulation is still in the learning curve, and there is obvious room for improvement of each characteristic244.

3. Self-regulation on the Internet is mainly a bottom-up procedure, where private parties take the initiative to address specific needs. However, states also participate in the creation of self-regulatory rules, either by creating the general background legal framework, by providing financial sponsoring, practical or legal guidance, or other assistance. Self-regulation and state legislation do not merely co-exist: they often complement each other and are intertwined245, whereby self-regulation can "plug into" the more general rules set forth by state law.

4. Self-regulation has been recognised as a recommended approach by the European Commission, the Member States. Moreover, it is already recommended by various legal instruments that apply to the online environment, including the eCommerce Directive, the Copyright Directive, the Data Protection Directive and the Audiovisual Media Services Directive.

5. From a legal point of view, the basic framework is already available for most areas where self-regulation can be beneficial. Although the legal framework is available, the actual implementation is often still problematic, particularly in the area of participation, enforcement and proper governance of self-regulatory organisations.

11. Recommendations

240 Office of Fair Trading, p. 30
241 R. DE BRUIN et al, o.c., p. 7
242 R. DE BRUIN et al, o.c., p. 9
243 M. BONNICI, o.c., p. 2
244 M. BONNICI, o.c., p. 216
245 Ibid.
11.1. Supporting self-regulatory initiatives

Both the European Commission and the Member States have supported various self-regulatory initiatives, through financial assistance, assistance with the drafting and enforcement of codes of conduct, training of staff members, promotion of self-regulatory initiatives, etc. As self-regulatory initiatives can be very useful policy tools, we think such support is strongly recommended, and should in fact be further strengthened.

In order to foster the uptake of self-regulatory initiatives, streamline the drafting process and create uniformity between industry players, it could be envisaged to create EU-level self-regulation "templates", in which sound governance principles (such as transparency, accountability and involvement of all stakeholders) are embedded, which are legally compliant and also reflect best practices, as outlined in this section 11. These templates can then be used to efficiently build up EU-wide, national or sector-specific self-regulation initiatives.

11.2. Incorporation in technology

Similar to our recommendation regarding the (re-)launch of a privacy configurations in software\textsuperscript{246}, we think it would be useful to integrate a service provider's compliance with trustmarks and codes of conducts in software. Such software should allow its users to configure his browser for trustmark compliance settings, and subsequently convey warnings when a service to be used is not in line with these predefined settings. Provided the software offers an attractive and user-friendly interface and apply the "lessons learned" from previous (failed) attempts, we think there is a realistic possibility that users and developers will use these features.

11.3. Increased use of standards

As pointed out in section 4.3 above, technical standards can be considered a type of self-regulation. In light of the disadvantages and limitations to self-regulation set out in section 6.2, one can indeed see remarkable similarities between self-regulation (in general) and technical standards. We therefore think it is useful to stimulate a convergence between self-regulation and standards.

**Parallels with standardisation** – Standardisation is a voluntary effort among industry, consumers and public authorities to develop consensus-based technical specifications in a certain domain. The EU has introduced a formal legal framework to support the EU-level standardisation process in certain areas. Three organisations (CEN, CENELEC and ETSI) are formally recognised, each with their own specific area of expertise, and are complemented by national standards bodies\textsuperscript{247}.

The formal EU standardisation bodies have done a good job in the past and have generally reached their objectives, while respecting the principles of openness and neutrality\textsuperscript{248}. However, several factors have come to undermine the standardisation monopoly of the formal EU standardisation bodies. In particular, the ICT sector has witnessed the rise of de facto standards\textsuperscript{249}, i.e. the creation of hundreds of standardisation bodies outside the formal standardisation process, as well as the rise of non-formal ICT standardisation bodies with a global reach.

\textsuperscript{246} See section 8.2.1 of Chapter 4 - privacy and data protection

\textsuperscript{247} See Annex II to Directive 98/34/EC for a list of recognized National Standardisation Bodies

\textsuperscript{248} See consideration 24 of Directive 98/34/EC

\textsuperscript{249} H. SCHEPEL and J. FALKE, *Legal aspects of standardisation in the Member States of the EC and EFTA*, vol. 1, European Communities, 2000, p. 97
As a result, the know-how and technical expertise related to standardisation in the ICT domain is often more available in non-formal bodies than in the formal bodies. Although the formal standardisation bodies have tried to adapt themselves to these new initiatives, it cannot be denied that the standardisation centre of gravity has shifted. At the same time, the non-formal bodies are criticized for their lack of consumer involvement, the underrepresentation of SMEs and the reduced long-term maintenance of standards.

<table>
<thead>
<tr>
<th>Self-regulation</th>
<th>Standardisation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Official bodies</strong></td>
<td>States</td>
</tr>
<tr>
<td></td>
<td>CEN, CENELEC and ETSI</td>
</tr>
<tr>
<td><strong>Unofficial bodies</strong></td>
<td>Self-regulation organisations</td>
</tr>
<tr>
<td></td>
<td>De facto standardisation bodies</td>
</tr>
<tr>
<td><strong>Issues relating to unofficial bodies</strong></td>
<td>Involvement of all stakeholders</td>
</tr>
<tr>
<td></td>
<td>Governance model</td>
</tr>
<tr>
<td></td>
<td>Volatile nature of many initiatives</td>
</tr>
<tr>
<td></td>
<td>Enforcement</td>
</tr>
<tr>
<td></td>
<td>State intervention</td>
</tr>
<tr>
<td><strong>Strengths of unofficial bodies</strong></td>
<td>Cross-border nature</td>
</tr>
<tr>
<td></td>
<td>Industry expertise</td>
</tr>
<tr>
<td></td>
<td>Speed and flexibility</td>
</tr>
<tr>
<td></td>
<td>Cross-border nature</td>
</tr>
<tr>
<td></td>
<td>Industry expertise</td>
</tr>
<tr>
<td></td>
<td>Speed and flexibility</td>
</tr>
</tbody>
</table>

**Future model of standardisation** – Following the recommendations of a independent study, the European Commission now proposes to launch a high-level policy dialogue platform, where all standardisation stakeholders would be represented, and which would meet several times a year. This platform should then provide the European Commission with expert advice regarding matters concerning ICT standardisation policy and its implementation. The non-formal standardisation bodies would be integrated in the formal procedures. Although the European Commission recognises the importance of private fora and consortia, it worries that non-formal bodies may not offer sufficient guarantees of eligibility.

**Link with self-regulation** – Considering the striking similarities between standards and self-regulatory initiatives, with respect to both their advantages and disadvantages, we think it can be useful to investigate to which extent self-regulatory initiatives can be linked to standardisation efforts. Such link can, first, be that self-regulatory initiatives are adopted as formal standards, through the new standardisation procedures that are currently being developed by the European Commission. A second possibility would be to mirror some of the new governance structures, for adoption by self-regulatory initiatives.

---

250 Towards an increased contribution from standardisation to innovation in Europe, o.c., p. 5
252 *ibid.*, p. 8
253 Open decision making process, based on collaborative and consensus-based activity, accessible to all stakeholders on a non-discriminatory basis, with all technical information being made available in a transparent way.
12. Recommended uses for self-regulation

Taking into account the success and failure criteria for self-regulation\(^{254}\), we recommend the use of self-regulation in the following fields:

12.1. Traditional web shops

Traditional web shops, on which various products and services can be ordered, are the prototypical example of an area where self-regulation can flourish. Although there already exist various trustmarks for web shops in the Member States, these trustmarks are only used by a minority of web shops, and are generally limited to the national level (which does not increase trust for foreign consumers).

We recommend the creation of EU-level trustmarks and codes of conduct, in order to decrease the threshold for a consumer of one Member State to order products or services from a web shop in another Member State. However, all trustmarks must comply with the requirements set out in section 9.2, in particular the governance model, the cross-border nature, and the independence of the trustmark organisation.

Another interesting idea is the creation of trusted online malls, similar to the Japanese Rakuten example described in section 7.1.3 above.

12.1.2. Data protection issues

The internet presents numerous difficulties and complexities in the field of online privacy and data protection\(^{255}\). We think that self-regulation can play an important role in the field of data protection, for example with respect to the following issues:

- **Content, style and presentation of privacy policies** – As outlined in the chapter on online data protection\(^{256}\), we think that online service providers should be encouraged to draft multi-layered privacy policies, which provides clear and concise information on the use of personal data by the service provider. Taking into account that privacy policies are poorly drafted at this moment, it can be envisaged to develop templates on how privacy policies should be drafted. As these templates can vary between types of service providers (web shops, data storage services, online communities, ...), self-regulatory efforts may prove beneficial.

- **Standards should be developed for specific data protection tasks**, such as the right to access and correction, as well as information obligations. Standards should also be developed for **storage terms** (per industry sector or per category of personal data) and for **data export formats**\(^{257}\).

- **Self-regulation can also deal with direct marketing and unsolicited commercial communications issues**, particularly for "grey areas", where it is not clear to which extent certain practices are allowed by data protection legislation. Such is, for example, the case with viral marketing initiatives, behavioural advertising\(^{258}\), and "tell-a-friend" systems.

---

\(^{254}\) See section 9 above


\(^{256}\) See section 7.2.1

\(^{257}\) When the right of data portability would be recognised.

Security – The Data Protection Directive requires data controllers to take security measures that are commensurate with the nature of the data, the costs and the associated risks. As the Directive does not impose any further guidelines or standards, we think there is an interesting opportunity for industry players to develop standards and/or undertake self-regulatory initiatives to provide guidance on which security measures are appropriate for specific online services.

12.1.3. Harmful content

As pointed out in section 7.1, the EU and several Member States have long recognised that the only real option for regulating harmful content is through self-regulation. These efforts should be maintained and further enhanced. The uptake of user rating and labelling systems should be encouraged, preferably on an EU-level or global level.

12.1.4. Social communities

Social communities have mushroomed over the last of couple of years. Children, teenagers and adults spend an increasing amount of their time on these communities.

However, social communities present many challenges, particularly in the field of data protection and child protection. As noted above, the European Commission has already taken initiatives in this regard with the Safer Social Networking Principles. Such initiatives should be encouraged. The effectiveness of self-regulatory initiatives should be monitored, so that social communities can further flourish without overly burdensome state regulation. Such state regulation may, however, become necessary when self-regulation would prove to be ineffective.

12.1.5. Services targeted at children and teenagers

Another area where self regulation can play an important role, is in online services that are targeted at children, teenagers or other target groups that require special protection. Self-regulation initiatives can, for example, provide guidance with respect to:

- age verification systems;
- age labelling systems (e.g., user rating systems such as PEGI);
- information requirements towards the target audience;
- "blacklisted" practices towards the target audience; and
- involvement of parents and guardians.

12.1.6. Online advertising

In light of the cross-border nature of the Internet, EU-level initiatives should be further developed to deal with online advertising, particularly in emerging markets such as targeted internet advertising.

Note that some Member States also resort to blocking (highly) illegal content at the level of internet access providers, as pointed out in Chapter 7 (net neutrality).

See also the keynote speech of EU commissioner M. KUNEVA on 31 March 2009 (SPEECH/09/156): "I invite industry to develop a framework that applies consumer policy principles and that will establish the principles of acceptable behaviour along the lines of what is being discussed today."
Although there already exists a set of international advertising guidelines (ICC code)\(^{261}\), a general pan-European code is not yet in effect. Instead, each Member State applies a set of national rules or principles, in accordance with its local culture, economy and society.

Similarly, there exist well-functioning self-regulatory advertising entities on a national level\(^{262}\), as well as a coordinating European Advertising Standards Alliance. However, these initiatives ultimately boil down to national interpretation and enforcement of rules, which can become cumbersome in real cross-border advertisements. Furthermore, not all of national self-regulatory entities already deal with internet advertising. Also, in some countries, advertising is subject to detailed legislation, to such an extent that the scope left for self-regulation is quite limited.

12.1.7. New technologies

Self-regulation is also recommended to deal with emerging technologies, in order to avoid over-regulation of such technologies in an early state.

This is, for example, the approach followed by the European Commission with respect to RFID. Few technologies have triggered such attention from consumer organisations as RFID devices, which are considered as the building blocks of a global “nervous system” that will make possible new types of applications combining information of the virtual world with a perception of the physical world. In the public debate, serious concerns have been expressed that RFID may endanger privacy, as it can be used to collect information that is linked to natural persons.

Yet, in its Communication of 15 March 2007\(^ {263}\) and subsequent Communication of 15 February 2009\(^ {264}\), it pointed to self-regulation as a means to regulate this new technology, and would not revert to traditional legislation, unless self-regulation would prove to be ineffective. We think this approach should receive approval, unless new technologies would present an immediate and acute danger to public concerns (such as consumer health). The Commission has recommended Member States to ensure that a framework for privacy and data protection is developed by all stakeholders, which should be submitted for endorsement to the Working Party 29.

12.1.8. Dispute resolution

Finally, online dispute resolution can also greatly benefit from self-regulatory initiatives. This is further discussed in Chapter II.9 (dispute resolution).

12.1.9. Copyright

As explained in Chapter 2 on digital content, Europe’s content sector is suffering from geographical fragmentation, so that parties must undertake costly negotiations to make digital content available online. Self-regulation and cross-industry agreements between industry players can help to maximise the circulation and exploitation of digital content rights\(^ {265}\). Furthermore, the European Commission and the

---

\(^{261}\) E.g., the Consolidated ICC Code of Advertising and Marketing Communication Practice

\(^{262}\) E.g., the Jury d’Ethique Publicitaire in Belgium; the Deutscher Werberat in Germany; the Advertising Standards Authority in the UK; etc.

\(^{263}\) COM (2007) 96 final

\(^{264}\) C(2009) 3200 final on the implementation of privacy and data protection principles in applications supported by radio-frequency identification

Member States must encourage the creation of codes of conduct to address issues such as transparency and fairness of contractual terms. They could also act as an incentive for all stakeholders to voluntarily comply with contractual terms regarding digital content.
EU study on the

Legal analysis of a
Single Market for the Information Society

New rules for a new age?

14. Annex

November 2009
### Annex

**Detailed overview of selected Directives**

#### I. eCommerce Directive (2000/31/EC)

##### I.1. Current provisions

<table>
<thead>
<tr>
<th>Art. #</th>
<th>Article description</th>
<th>Issue?</th>
<th>Possible solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1 - 1.3</td>
<td>Objectives of the Directive</td>
<td>/</td>
<td>/</td>
</tr>
<tr>
<td>1.4</td>
<td>No additional rules on private international law or jurisdiction</td>
<td>/</td>
<td>/</td>
</tr>
<tr>
<td>1.5</td>
<td>Scope exclusions</td>
<td>Are the exclusions of subitem (d) (particularly gambling) still relevant?</td>
<td>Reconsider the exclusion of online gambling.</td>
</tr>
<tr>
<td>1.6</td>
<td>No impact on cultural, linguistic and pluralism measures</td>
<td>/</td>
<td>/</td>
</tr>
<tr>
<td>2.a</td>
<td>Definition “information society services”</td>
<td>The central definition of “information society services” is a subcategory of the general concept of “services”, as defined to article 50 of the EC Treaty. However, the scope of article 50 of the EC Treaty may be too narrow for the purposes of the eCommerce Directive. For example, it not only excludes many governmental services offered online, but also risks to exclude many new types of services (particularly “freemium” services), which may then be exposed to unnecessary third party content liability issues, and would then not benefit from the freedom of establishment and the freedom of online service delivery.</td>
<td>When this ambiguity would not be resolved by case law, we recommend to consider adopting a different criterion. In the short or medium term, this different criterion could be used to define the scope of the special liability regime. However, in order to also use this different criterion for the freedom of establishment and the</td>
</tr>
<tr>
<td>Art. #</td>
<td>Article description</td>
<td>Issue?</td>
<td>Possible solutions</td>
</tr>
<tr>
<td>-------</td>
<td>---------------------</td>
<td>--------</td>
<td>--------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>freedom of service delivery, a change of the EC Treaty will be necessary. Such will, obviously, only be possible in the long term.</td>
</tr>
<tr>
<td>2.b, 2.d</td>
<td>Definitions of &quot;service provider&quot;, &quot;recipient of the service&quot;</td>
<td>(As both definitions rely on the definition of &quot;information society services&quot;, see #2.a for issues)</td>
<td></td>
</tr>
<tr>
<td>2.c</td>
<td>Definition of &quot;established service provider&quot;</td>
<td>/</td>
<td>/</td>
</tr>
<tr>
<td>2.e</td>
<td>Definition of &quot;consumer&quot;</td>
<td>/</td>
<td>/</td>
</tr>
<tr>
<td>2.f</td>
<td>Definition of &quot;commercial communication&quot;</td>
<td>This definition is limited to communications for the promotion of goods, services or the image of a company, organisation or person &quot;pursuing a commercial, industrial or craft activity or exercising a regulated profession&quot;. This scope excludes: - communications from non-profit organisations and associations - communications with content that does not intent to &quot;promote&quot; (e.g., random junk mails, mails intended to infect recipients with malware, as well as &quot;stock dump mails&quot; which deliberately stain the image of listed companies)</td>
<td>Reconsider scope of this definition. The wording of the new article should be technology-neutral.</td>
</tr>
<tr>
<td>2.g</td>
<td>Definition of &quot;regulated profession&quot;</td>
<td>/</td>
<td>/</td>
</tr>
<tr>
<td>2.h</td>
<td>Definition of &quot;coordinated field&quot;</td>
<td>The exact scope of the coordinated field is ambiguous: some authors suggest that it encompasses only what is explicitly regulated by the eCommerce Directive itself. Others – particularly those who have written about this matter immediately after the date of enactment of the eCommerce Directive – see it more broadly, and consider that any law that somehow impacts online service providers is included in the coordinated field (the only exceptions being those that are explicitly set forth by the eCommerce Directive, such as the offline delivery of goods).</td>
<td>Publish a comprehensive register that includes all national rules that are notified by Member States as derogations from the freedom of service principle. Clarify that national rules that have not been notified do not apply to service providers established in other Member States. Confirm that the coordinated field of the eCommerce Directive covers</td>
</tr>
<tr>
<td>Art. #</td>
<td>Article description</td>
<td>Issue?</td>
<td>Possible solutions</td>
</tr>
<tr>
<td>-------</td>
<td>---------------------</td>
<td>--------</td>
<td>--------------------</td>
</tr>
<tr>
<td>3</td>
<td>Internal market provisions</td>
<td>The scope of the coordinated field is not clear (see #2.h). The &quot;contractual obligations concerning consumer contacts&quot; exclusion set forth in the Annex of the Directive is not clear: it is, for example, argued by some authors that this exclusion is limited to post-contractual obligations (due to the words &quot;contracts concluded by consumers&quot; in recital 56), excluding any precontractual obligations.</td>
<td>see #2.h</td>
</tr>
<tr>
<td>4</td>
<td>Principle excluding prior authorisation</td>
<td>/</td>
<td>/</td>
</tr>
<tr>
<td>5</td>
<td>General information to be provided</td>
<td>It is not always possible to provide the requested information when using some technologies (e.g., SMS, virtual worlds) or devices (e.g., devices without a screen / devices with a small screen). The interpretation by the Court of Justice of article 5.c (the service provider must provide his details, including his electronic mail address, which allow him to be contacted rapidly) may cause obstacles for electronic commerce. According to the decision of the European Court of Justice of 16 October 2008, a service provider is virtually obliged to also specify a telephone number, as online contact forms, instant messaging tools and chat functionality can only satisfy the eCommerce Directive's requirements most of the time (provided answers to questions are sent reasonably fast).</td>
<td>Change the transparency obligations of the eCommerce Directive in order to make them compatible with current business models.</td>
</tr>
<tr>
<td>6</td>
<td>Information to be provided</td>
<td>Similar to #5, it is not always possible to provide the requested information when using some technologies (e.g., SMS, virtual worlds) or devices (e.g., devices without a screen / devices with a small screen).</td>
<td>Change the transparency obligations of the eCommerce Directive in order to make them compatible with current business models.</td>
</tr>
<tr>
<td>7</td>
<td>Unsolicited commercial communications</td>
<td>Mostly replaced by the ePrivacy Directive (see discussion on ePrivacy Directive below)</td>
<td>Merge with the ePrivacy Directive provisions on unsolicited commercial communications</td>
</tr>
<tr>
<td>8</td>
<td>Regulated professions</td>
<td>/</td>
<td>/</td>
</tr>
<tr>
<td>Art. #</td>
<td>Article description</td>
<td>Issue?</td>
<td>Possible solutions</td>
</tr>
<tr>
<td>-------</td>
<td>---------------------</td>
<td>--------</td>
<td>--------------------</td>
</tr>
<tr>
<td>9.1</td>
<td>Contracts concluded by electronic means must be allowed</td>
<td>/</td>
<td>/</td>
</tr>
<tr>
<td>9.2</td>
<td>Possible exceptions to #9.1 (real estate, court / public authority involvement, surety / securities, family law / succession rights)</td>
<td>Exception for exception (b) (regarding contracts that require the involvement of courts, public authorities or professions exercising public authority), it is questionable whether these exceptions are still relevant in today's society, where contracts are increasingly negotiated and signed using electronic means. Furthermore, these exceptions convey the message that electronic contracting is only adequate for minor transactions. Although these exceptions were relevant at the time the eCommerce Directive was adopted, the time may have come to consider abolishing these exceptions, in particular because they can undermine harmonisation across Member States.</td>
<td>Consider abolishing these exceptions, particularly (a), (c) and (d)</td>
</tr>
<tr>
<td>9.3</td>
<td>Exception notification duty of Member States</td>
<td>/</td>
<td>/</td>
</tr>
<tr>
<td>10.1</td>
<td>Information to be provided</td>
<td>While these requirements were answers to valid concerns at the time the eCommerce Directive was drafted, they have now either become too evident, have become a stumbling block for new technologies and business models, mainly lead to increased compliance costs and/or overly protect consumers. Furthermore, they discriminate against the offline contracting process, which is free from formalities in most cases and in most Member States. Moreover, the eCommerce Directive does not deal with real issues nowadays, such as unreadable and lengthy terms and conditions.</td>
<td>Remove article 10.1</td>
</tr>
<tr>
<td>10.2</td>
<td>Codes of conduct must be indicated</td>
<td>/</td>
<td>/</td>
</tr>
<tr>
<td>10.3</td>
<td>Customers must be able to store and reproduce contractual terms</td>
<td>This article may be a difficult to reconcile with new technologies, such as SMS contracts concluded by cell phones.</td>
<td>Remove article 10.3</td>
</tr>
<tr>
<td>10.4</td>
<td>Contracts concluded exclusively by exchange of electronic mail</td>
<td>/</td>
<td>/</td>
</tr>
<tr>
<td>11</td>
<td>Placing of the order</td>
<td>See #10.1</td>
<td>Remove article 11</td>
</tr>
</tbody>
</table>
| 12.1  | No liability for "mere conduit" | I is not clear whether traffic filtering, insertion of advertisements and textual filtering of chat | The "selection or modification of
<table>
<thead>
<tr>
<th>Art. #</th>
<th>Article description</th>
<th>Issue?</th>
<th>Possible solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>services</td>
<td>conversations can be considered as such &quot;manipulations of a technical nature&quot;</td>
<td>information&quot; criterion for mere conduit providers should be changed to avoid that minor selections or modifications undermine the applicability of the special liability regime.</td>
</tr>
<tr>
<td>12.2</td>
<td>Clarification of &quot;transmission&quot; and &quot;access provision&quot;</td>
<td>/</td>
<td>/</td>
</tr>
</tbody>
</table>
| 12.3  | Mere conduit service providers can be requested to prevent infringements | - Member States differ in the range of measures that can be imposed by national courts;  
- there is varying case law across Member States regarding the possibility to impose injunctions: some courts seem openly sympathetic towards the plaintiff, other courts consider the injunctions to be disproportionate;  
- the prevention of future infringements often leads de facto to a general monitoring obligation for the hosting provider, which may conflict with article 15;  
- even when a service provider would not be held liable, the practical consequences of an injunction will often lead to similar effects (lawsuits, exposure, costs, etc.) | Harmonise the possibility to impose injunctions on online intermediaries.  
In addition to harmonisation, it could be envisaged to only allow third party content injunctions as a last resort or in urgent circumstances, and to remunerate intermediaries for all costs incurred. |
| 13.1  | No liability for "caching" services | The definition is ambiguous. Although this article clearly targeted one specific technology (proxy-servers), its wording also allows it to apply to other technologies (such as Usenet newsgroups, DNS systems or even peer-to-peer services), although this may not be in line with the original intentions of the European legislator. | (Modification does not seem urgent in the short term.) |
| 13.2  | Caching service providers can be requested to prevent infringements | See 12.3 | See 12.3 |
| 14.1  | No liability for "hosting services" | The definition is ambiguous:  
- the "consists of" criterion does not specify to which extent a service should relate to hosting: is it sufficient that some aspects of the service deal with hosting, should the majority of aspects deal with hosting, or should all aspects of the service deal with hosting?  
- the "illegal activity" criterion requires service providers to make a legal assessment of what does and what does not constitute illegal information;  
- it is not clear what constitutes "have actual knowledge" or "are aware of facts or circumstances". It is left to national courts to determine which level of knowledge or | Extend the special liability regime, to protect all online third party information processors against liability claims, excluding service providers that induce their users to infringe third party rights. |
<table>
<thead>
<tr>
<th>Art. #</th>
<th>Article description</th>
<th>Issue?</th>
<th>Possible solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.2</td>
<td>Liability exemption does not apply when recipient acts under authority / control of the provider</td>
<td>According to some case law, good-faith control over third party content (e.g., cleaning up offending user comments on a blog; removing spam messages from a forum; monitoring offensive language in a chat room; etc.) can lead to a loss of liability protection.</td>
<td>Online service providers that exercise good-faith control over third party content hosted by them.</td>
</tr>
<tr>
<td>14.3</td>
<td>Hosting providers can be requested to prevent infringements</td>
<td>see 12.3</td>
<td>see 12.3</td>
</tr>
<tr>
<td>15</td>
<td>No general obligation to monitor</td>
<td>The prevention of future infringements (on the basis of 12.3, 13.2 or 14.2) often leads <em>de facto</em> to a general monitoring obligation for the hosting provider, which may conflict with article 15.</td>
<td>see 12.3</td>
</tr>
<tr>
<td>16</td>
<td>Codes of conduct</td>
<td>/</td>
<td>/</td>
</tr>
<tr>
<td>17</td>
<td>Dispute resolution</td>
<td>/</td>
<td>/</td>
</tr>
<tr>
<td>18</td>
<td>Court actions</td>
<td>/</td>
<td>/</td>
</tr>
<tr>
<td>19</td>
<td>Cooperation between Member States</td>
<td>/</td>
<td>/</td>
</tr>
<tr>
<td>20-24</td>
<td>Other provisions</td>
<td>/</td>
<td>/</td>
</tr>
</tbody>
</table>

### 1.2. Gaps

<table>
<thead>
<tr>
<th>Art. #</th>
<th>Description</th>
<th>Possible solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>12-14</td>
<td>No mandatory liability exemption for search engines (only in some)</td>
<td>As few case law was reported with respect to search engines and hyperlinking, we do not deem it a priority in the short term to harmonise the protection of search engines and hyperlinks.</td>
</tr>
<tr>
<td>Art. #</td>
<td>Description</td>
<td>Possible solutions</td>
</tr>
<tr>
<td>--------</td>
<td>------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>12-14</td>
<td>No mandatory liability exemption for hyperlinking (only in some Member States)</td>
<td>In the medium to long term, we would consider it appropriate to replace the current three-fold structure of the special liability regime by a two-fold structure, consisting of (i) mere conduit service providers, and (ii) third party information processors.</td>
</tr>
<tr>
<td>12-14</td>
<td>The special liability regime is too focused on (only) three types of services</td>
<td>A harmonised, detailed and clear notice-and-takedown procedure should be introduced, which balances the rights of the online service providers, the service users, as well as the plaintiffs. Although the notice-and-takedown procedures used in Finland, Hungary, Lithuania, Japan and the US can be used as a model, these existing procedures must be altered to mitigate the incentive for service providers to immediately take down the material (e.g., by involving the user in the takedown process).</td>
</tr>
<tr>
<td>12-14</td>
<td>No uniform notice-and-takedown procedure</td>
<td></td>
</tr>
</tbody>
</table>


2.1. **Current provisions**

<table>
<thead>
<tr>
<th>Art. #</th>
<th>Article description</th>
<th>Issue?</th>
<th>Possible solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Scope</td>
<td>/</td>
<td>/</td>
</tr>
<tr>
<td>2</td>
<td>Reproduction right</td>
<td>The reproduction rights are overly broad, and overlap with the right of communication to the public.</td>
<td>New statutory provisions must be adopted that allow consumers to undertake some minimum actions on digital content. Consider to harmonise all exceptions and make them mandatory across all Member States.</td>
</tr>
<tr>
<td>3</td>
<td>Right of communication / making</td>
<td>/</td>
<td>/</td>
</tr>
<tr>
<td>Art. #</td>
<td>Article description</td>
<td>Issue?</td>
<td>Possible solutions</td>
</tr>
<tr>
<td>-------</td>
<td>--------------------</td>
<td>--------</td>
<td>--------------------</td>
</tr>
<tr>
<td>4</td>
<td>Distribution right</td>
<td>The exhaustion principle is limited to <em>tangible</em> goods only, excluding on-line services and intangible goods that incorporate digital content.</td>
<td>Consider to harmonise all exceptions and make them mandatory across all Member States.</td>
</tr>
<tr>
<td>5</td>
<td>Exceptions and limitations</td>
<td>The exceptions are not mandatory. Member States have ample discretionary margin to decide if and how to implement the exceptions and limitations. Accordingly, there is indeed much variation in the way Member States have implemented the exceptions and limitations in their national law. No harmonisation of private use exceptions. Few exceptions fit properly in the digital environment.</td>
<td>Clarify these concepts.</td>
</tr>
<tr>
<td>5.1</td>
<td>Temporary reproduction exception</td>
<td>&quot;No independent economic significance&quot; is ambiguous, in particular when combined with the broad scope of the reproduction right. &quot;Lawful use&quot; is also ambiguous, because the lawfulness rests in criteria found outside article 5. Article 5.1 Copyright Directive is not technologically neutral: it seems to have been written with internet access providers in mind.</td>
<td>Clarify these concepts.</td>
</tr>
<tr>
<td>5.2.</td>
<td>Other exceptions concerning reproduction</td>
<td>Article 5.2.b does not clearly indicate whether Member States can allow the third parties to actually produce the digital copies.</td>
<td>Clarify concepts</td>
</tr>
<tr>
<td>6</td>
<td>Technological protection measures (TPM)</td>
<td>The Copyright Directive does not provide specific guidelines for the implementation of TPMs. Ambiguity regarding the meaning of &quot;adequate&quot; legal protection; who is entitled to invoke it; when does a device have only a limited commercially significant purpose or use other than to circumvent. TPM exceptions do not apply to online services under &quot;agreed&quot; contractual terms. This discrepancy could lead to the development of a dual analogue v. digital system. As the exceptions are not mandatory, right holders can prohibit acts that are not restricted by law through the use of technological measures and licenses. This creates a two-track policy, which &quot;silences&quot; the lawful use of copyrighted works in an online environment. The use of TPM can conflict with a user's data protection rights and privacy rights, by tracing the use of the protected work and monitoring a user's behaviour. No differentiation is made between the reasons for <em>applying</em> TPMs and the reasons for <em>circumventing</em> them. Acts of circumvention done for legitimate purposes are not protected.</td>
<td>Adopt statutory provisions to encourage the development of privacy enhancing technologies. Adopt rules that prohibit TPMs from depriving users of lawful uses of works. Encourage the adoption of open standards for technological protection measures (TPMs), so that stakeholders can create compatible equipment and services. Reflect new consumer requirements in the list of exceptions and limitations.</td>
</tr>
<tr>
<td>Art. #</td>
<td>Article description</td>
<td>Issue?</td>
<td>Possible solutions</td>
</tr>
<tr>
<td>--------</td>
<td>---------------------</td>
<td>--------</td>
<td>--------------------</td>
</tr>
<tr>
<td>7</td>
<td>Rights-management information</td>
<td>/</td>
<td>/</td>
</tr>
<tr>
<td>8.1 - 8.2</td>
<td>Sanctions and remedies</td>
<td>/</td>
<td>/</td>
</tr>
<tr>
<td>8.3</td>
<td>Injunctions against intermediaries</td>
<td>It is not clear to which extent the provisions of article 8.3 of the Copyright Directive conflicts with the prohibition of a general monitoring obligation set forth in article 15 of the eCommerce Directive.</td>
<td>Only allow third party content injunctions as a last resort or in urgent circumstances, and to remunerate intermediaries for all costs incurred.</td>
</tr>
<tr>
<td>9-15</td>
<td>[Other provisions]</td>
<td>/</td>
<td>/</td>
</tr>
</tbody>
</table>

## 2.2. Gaps

<table>
<thead>
<tr>
<th>Art. #</th>
<th>Description</th>
<th>Possible solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Lack of basic consumer rights</td>
<td>Adopt new statutory provisions that allow consumers to undertake some minimum actions on digital content.</td>
</tr>
<tr>
<td></td>
<td>The Copyright Directive does not deal with the topic of choice of law or with the competent court. It is not always predictable in advance which law or court shall apply.</td>
<td>Amend the current EU legal instruments on jurisdiction (Brussels I) and applicable law (Rome I - II) to include criteria that are suitable for today's complex information society services. Include rules on the applicable law for defamation and data protection issues in the Rome II Regulation. Adopt uniform and clear criteria for the applicable law across all legal instruments relevant for the information society, preferably using the country of establishment / residence as the connecting factor.</td>
</tr>
<tr>
<td></td>
<td>Getting legal certainty to reuse content</td>
<td>The lack of formalities often makes it difficult for someone who wants to use an existing work to find the content owner and to obtain the permission required. This &quot;gap&quot; in the current legal rules could lead to the limitation of creativity, since those willing to develop digital content may find it difficult to build upon previous works that are not registered or recorded in any repository.</td>
</tr>
</tbody>
</table>
### 3. Data Protection Directive (95/46/EC)

#### 3.1. Current provisions

<table>
<thead>
<tr>
<th>Art. #</th>
<th>Article description</th>
<th>Issue?</th>
<th>Possible solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Objectives of the Directive</td>
<td>/</td>
<td>/</td>
</tr>
<tr>
<td>2.a</td>
<td>Definition of &quot;personal data&quot;</td>
<td></td>
<td>Realign the interpretation of &quot;personal data&quot; with the (online) reality.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Clarify to which extent abstract profiling is subject to the Data Protection Directive</td>
</tr>
<tr>
<td>2.b</td>
<td>Definition &quot;processing&quot;</td>
<td></td>
<td>Reconsider the scope of &quot;processing&quot; (e.g., restrict to structured data).</td>
</tr>
<tr>
<td>2.c</td>
<td>Definition &quot;personal data filing system&quot;</td>
<td>/</td>
<td>/</td>
</tr>
<tr>
<td>2.d-e</td>
<td>Definitions &quot;controller&quot; and &quot;processor&quot;</td>
<td></td>
<td>Change the definition of &quot;data controller&quot; into a definition that is predictable, flexible and apt for the online context, and minimises situations with concurrent data controllers for the same type of processing.</td>
</tr>
</tbody>
</table>

- Article 2.a discusses the definition of "personal data" and highlights the ambiguity in interpreting "identifiable". It proposes realigning the interpretation to better fit the online context.
- Article 2.b addresses the broad definition of "processing" in the context of the Internet, suggesting a restriction to structured data.
- Article 2.c mentions the "personal data filing system" but does not specify an issue or solution.
- Articles 2.d-e address the distinction between controllers and processors, recommending changes to make the definition more predictable and flexible for the online context.
<table>
<thead>
<tr>
<th>Art. #</th>
<th>Article description</th>
<th>Issue?</th>
<th>Possible solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.f</td>
<td>Definition &quot;third party&quot;</td>
<td>/</td>
<td></td>
</tr>
<tr>
<td>2.g</td>
<td>Definition &quot;recipient&quot;</td>
<td>/</td>
<td></td>
</tr>
<tr>
<td>2.h</td>
<td>Definition &quot;data subject's consent&quot;</td>
<td>The definition of consent is not problematic as such. However, in practice, the consent of data subjects often does not meet the criteria of this definition, i.e. a freely given specific and informed indication of wishes.</td>
<td>/</td>
</tr>
<tr>
<td>3</td>
<td>Scope</td>
<td>It is difficult to apply the &quot;household&quot; exemption (article 3.2, second bullet) to the online context, as any publicly available website would not fall within the scope of this exemption according to Working Party 29, even when it would not be contested that the actual purpose of this website is for purely personal or household activities. Exempting household activities from all data protection obligations may no longer be appropriate, in light of the amount of personal data processed for purely personal / household reasons.</td>
<td>Change the &quot;household exception&quot;. Clarify the distinction between private and public use in view of the online environment.</td>
</tr>
<tr>
<td>4.1.a</td>
<td>Applicable national law - establishment</td>
<td>The first criterion used for determining the applicability of the Directive is the fact whether a controller has an establishment within the EU. However, several Member States have implemented this requirement in a way that differs from the Directive's wording. Moreover, certain Member States maintain their own very extensive interpretation of the concept &quot;establishment&quot;, which creates uncertainty towards data controllers.</td>
<td>Clarify this article and harmonise its interpretation. Restrict the application of the EU data protection rules to online services that actively target EU citizens.</td>
</tr>
<tr>
<td>4.1.b</td>
<td>Applicable national law - international public law</td>
<td>/</td>
<td>/</td>
</tr>
<tr>
<td>4.1.c</td>
<td>Applicable national law - equipment</td>
<td>The concept &quot;use of equipment&quot; is interpreted rather extensively, so that EU law often applies beyond the territorial boundaries of the Member States. Moreover, several Member States have used variations of the concept equipment in their national law, by using a term which translates into &quot;means&quot; rather than into &quot;equipment&quot;, which has a far more comprehensive meaning. This extensive interpretation is especially problematic in an online context, due to the application of the concept &quot;equipment&quot; to cookies. Working Party 29 is of the opinion that a user's computer qualifies as &quot;equipment&quot;. Hence, any website operator which uses cookies on its website, is deemed to use the user's computer for the processing of personal data.</td>
<td>Restrict the application of the EU data protection rules to online services that actively target EU citizens.</td>
</tr>
<tr>
<td>Art. #</td>
<td>Article description</td>
<td>Issue?</td>
<td>Possible solutions</td>
</tr>
<tr>
<td>-------</td>
<td>---------------------</td>
<td>--------</td>
<td>--------------------</td>
</tr>
<tr>
<td>4.2</td>
<td>Representative</td>
<td>/</td>
<td>/</td>
</tr>
<tr>
<td>5</td>
<td>Lawfulness of processing</td>
<td>/</td>
<td>/</td>
</tr>
<tr>
<td>6.1.a-d, 6.2</td>
<td>Data quality principles</td>
<td>/</td>
<td>Accept the processing of personal data for reasons of compliance with a third country's legal obligations as a lawful ground for processing.</td>
</tr>
<tr>
<td>7</td>
<td>Legal basis for processing</td>
<td>/</td>
<td>Change the definition of &quot;sensitive data&quot; into either a purpose-based approach or a contextualised approach.</td>
</tr>
<tr>
<td>8.1</td>
<td>Definition sensitive data</td>
<td>/</td>
<td>/</td>
</tr>
<tr>
<td>8.2</td>
<td>Legal basis for processing sensitive data</td>
<td>/</td>
<td>/</td>
</tr>
<tr>
<td>8.3-8.7</td>
<td>Processing of specific types of sensitive data</td>
<td>/</td>
<td>/</td>
</tr>
<tr>
<td>9</td>
<td>Freedom of expression</td>
<td>/</td>
<td>Encourage online service providers to draft multi-layered privacy policies.</td>
</tr>
<tr>
<td>10-11</td>
<td>Information to be given to data subject</td>
<td>/</td>
<td>/</td>
</tr>
<tr>
<td>Art. #</td>
<td>Article description</td>
<td>Issue?</td>
<td>Possible solutions</td>
</tr>
<tr>
<td>--------</td>
<td>---------------------</td>
<td>--------</td>
<td>-------------------</td>
</tr>
<tr>
<td>12</td>
<td>Right of access</td>
<td>/</td>
<td>/</td>
</tr>
<tr>
<td>13</td>
<td>Exemptions and restrictions</td>
<td>/</td>
<td>/</td>
</tr>
<tr>
<td>14</td>
<td>Right to object</td>
<td>/</td>
<td>/</td>
</tr>
<tr>
<td>15.1</td>
<td>Prohibition on automated individual decisions</td>
<td>It is unclear if and to which extent this article applies to profiling data, both as regards personal and abstract profiles.</td>
<td>Clarify the scope of this article.</td>
</tr>
<tr>
<td>15.2</td>
<td>Allowed automated individual decisions</td>
<td>It cannot be assumed that the fulfilment of a data subject's request for entering into or executing a contract will never be problematic. For example, in the context of a credit loan application, a person may be granted a loan at better conditions if the decision is not taken based on the data processed.</td>
<td>Clarify the scope of the exception.</td>
</tr>
<tr>
<td>16-17</td>
<td>Confidentiality and security</td>
<td>/</td>
<td>/</td>
</tr>
<tr>
<td>17.3</td>
<td>Data processing contractual provisions</td>
<td>/</td>
<td>/</td>
</tr>
<tr>
<td>18-21</td>
<td>Notification</td>
<td>The notification obligation imposed on data controllers implies an administrative burden both for business and for data protection authorities, whilst the aims of the notification are very rarely achieved: notifications do not enhance transparency towards data subjects, nor do they help raise awareness of controllers as regards compliance with data protection requirements.</td>
<td>Abolish the notification duty.</td>
</tr>
<tr>
<td>22-24</td>
<td>Remedies, liability and sanctions</td>
<td>/</td>
<td>/</td>
</tr>
<tr>
<td>25-26</td>
<td>Transfer</td>
<td>The Directive imposes rigid obligations for transfers of personal data outside the EU. The assumptions this article was originally based on, however, may no longer hold true. Servers are now located all across the world, and with the advent of Web 2.0 and its distributed computing concepts (cloud computing, SaaS), the physical location of personal data is no longer controllable. The exceptions which allow transfers outside the EU can create considerable administrative overhead for data exporters: EU model clauses are not efficient in case of multiple party contracts and procedure for approval of binding corporate rules (BCR) is not harmonized and often requires approval in each Member State from which a company intends to transfer data.</td>
<td>Optimise and streamline the binding corporate rules (BCR) procedure, in particular with regard to the mutual recognition procedure. Consider the creation of &quot;safe harbor&quot; schemes with third countries, similar to the US safe harbor list. Initiate discussions on an international data protection treaty</td>
</tr>
</tbody>
</table>
### 27 Code of conduct
The benefits of this possibility to adopt codes of conduct have not yet been fully realised.

Possible solutions: Promote and encourage self-regulation.

### 28 Supervisory authorities
The enforcement of data protection laws in Member States is often not effective, due to lack of appropriate enforcement legislation, lack of personnel and ineffective measures to enforce data protection compliance.

Possible solutions: Encourage the Member States to widen the competence of national data protection authorities and bring their staffing and budget to a level which enables them to effectively conduct their enforcement tasks.

### 29-30 Working Party
It is not clear which is the legal value of the opinions of Working Party 29, and to which extent they must be complied with.

Possible solutions: Clarify the legal value of Working Party 29's opinions.

### 3.2 Gaps

<table>
<thead>
<tr>
<th>Art. #</th>
<th>Description</th>
<th>Possible solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>12-14</td>
<td>No right to be forgotten</td>
<td>A &quot;right to be forgotten&quot; should be included as an additional right for data subjects, to give each data subject the right to remove personal data, even when the data were initially collected with the data subject's consent. Such right can be particularly useful in the context of community sites.</td>
</tr>
<tr>
<td>12-14</td>
<td>No right of data portability</td>
<td>The Data Protection Directive currently only includes a right to access and does not yet require data controllers to provide data subject with an actual copy of their personal data if they request so. A &quot;right of portability&quot; should be included, to give data subjects the right to request copies of their personal data being held and processed.</td>
</tr>
</tbody>
</table>

### 4.1. Current provisions

*Note: the ePrivacy Directive is currently being revised. The table below only covers issues under the current Directive, which have not been resolved by the new proposal.*

<table>
<thead>
<tr>
<th>Art. #</th>
<th>Article description</th>
<th>Issue?</th>
<th>Possible solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Scope and aim</td>
<td>/</td>
<td>/</td>
</tr>
<tr>
<td>2</td>
<td>Definitions</td>
<td>/</td>
<td>/</td>
</tr>
<tr>
<td>3</td>
<td>Services concerned</td>
<td>/</td>
<td>/</td>
</tr>
<tr>
<td>4.1</td>
<td>Obligation to take appropriate measures to safeguard security of communication</td>
<td>/</td>
<td>/</td>
</tr>
<tr>
<td>4.2</td>
<td>Security breach notification duty</td>
<td>The notification duty is limited to network operators.</td>
<td>Introduce an information security breach notification duty for all data controllers.</td>
</tr>
<tr>
<td>5</td>
<td>Confidentiality of communications</td>
<td>/</td>
<td>/</td>
</tr>
<tr>
<td>6</td>
<td>Traffic data</td>
<td>/</td>
<td>/</td>
</tr>
<tr>
<td>7</td>
<td>Itemised billing</td>
<td>/</td>
<td>/</td>
</tr>
<tr>
<td>8</td>
<td>Calling and connected line identification</td>
<td>/</td>
<td>/</td>
</tr>
<tr>
<td>9</td>
<td>Location data other than traffic data</td>
<td>/</td>
<td>/</td>
</tr>
<tr>
<td>10</td>
<td>Exceptions</td>
<td>/</td>
<td>/</td>
</tr>
<tr>
<td>11</td>
<td>Automatic call forwarding</td>
<td>/</td>
<td>/</td>
</tr>
<tr>
<td>12</td>
<td>Directories of subscribers</td>
<td>/</td>
<td>/</td>
</tr>
<tr>
<td>13</td>
<td>Unsolicited communications</td>
<td>Legal uncertainty about the meaning of the concept of “sale” (does this term also include services offered free of charge?).</td>
<td>Do not focus on legislative intervention in the short term.</td>
</tr>
<tr>
<td>Art. #</td>
<td>Article description</td>
<td>Issue?</td>
<td>Possible solutions</td>
</tr>
<tr>
<td>-------</td>
<td>--------------------</td>
<td>-------</td>
<td>--------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Simplify and clarify the current anti-spam rules, and extend them to include new forms of spam. Convert the rules on spam to a maximum harmonisation legal framework.</td>
</tr>
<tr>
<td>14-21</td>
<td>(Other provisions)</td>
<td>/</td>
<td>/</td>
</tr>
</tbody>
</table>

4.2. Gaps

<table>
<thead>
<tr>
<th>Art. #</th>
<th>Description</th>
<th>Possible solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>13</td>
<td>gaps with regard to new technologies and new forms of spam (e.g. spam via instant messaging, spam via Bluetooth-enabled electronic devices and spam on message forums)</td>
<td>Make article 13 more technology-neutral to cover new forms of spam.</td>
</tr>
<tr>
<td>13</td>
<td>confusion with respect to the applicable law (compliance with the Member State from which, or to which the communication is sent?)</td>
<td>Adopt uniform and clear criteria for the applicable law across all legal instruments relevant for the information society, preferably using the country of establishment / residence as the connecting factor.</td>
</tr>
</tbody>
</table>
EU study on the

Legal analysis of a Single Market for the Information Society

New rules for a new age?

15. References

November 2009
# Table of contents

References............................................................................................................................................2

1. Books ..................................................................................................................................................2

2. Articles..................................................................................................................................................4

3. European Commission ..........................................................................................................................11

   3.1. Commission Staff Working Documents .......................................................................................11

   3.2. Commission Recommendations .................................................................................................11

   3.3. Commission Communications and reflection documents ..........................................................12

   3.4. Reports ...........................................................................................................................................13

   3.5. Commission proposals ..................................................................................................................14

   3.6. Green papers and action plans ......................................................................................................14

   3.7. Studies sponsored by the Commission ..........................................................................................15

   3.8. Press releases ...............................................................................................................................15

   3.9. Speeches .......................................................................................................................................15

4. Council of Europe ..................................................................................................................................16

5. European Parliament ..............................................................................................................................16

6. Working Party 29 ..................................................................................................................................17

7. Other reports and studies .....................................................................................................................17

8. Conference material .............................................................................................................................19

9. Position papers .....................................................................................................................................20

10. Legislation ..........................................................................................................................................21

   10.1. Directives ....................................................................................................................................21

   10.2. Council Decisions .......................................................................................................................23

   10.3. Regulations ..................................................................................................................................23

   10.4. Framework decisions ..................................................................................................................23

   10.5. Treaties ........................................................................................................................................23

11. Case law ..............................................................................................................................................24

   11.1. European Court of Justice ..........................................................................................................24

   11.2. European Court of Human Rights .............................................................................................24

   11.3. Belgium .......................................................................................................................................24

   11.4. Denmark .....................................................................................................................................25

   11.5. France ..........................................................................................................................................25

   11.6. Germany .....................................................................................................................................25

   11.7. Italy ..............................................................................................................................................25

   11.8. The Netherlands ..........................................................................................................................25

   11.9. Spain ..........................................................................................................................................26

   11.10. Sweden ....................................................................................................................................26

   11.11. United Kingdom ........................................................................................................................26

   11.12. United States ............................................................................................................................26

12. Miscellaneous documents ...................................................................................................................27

   12.1. ENISA ..........................................................................................................................................27

   12.2. OECD .........................................................................................................................................27

   12.3. Organization for Security and Co-operation in Europe (OSCE) ...................................................27

   12.4. France .........................................................................................................................................27

   12.5. Netherlands ...............................................................................................................................28

   12.6. United Kingdom .........................................................................................................................28

   12.7. Australia .....................................................................................................................................28

   12.8. Canada ........................................................................................................................................28

   12.9. United States .............................................................................................................................28
References

1. Books

- P. AHONEN, P. ALAHUHTA, B. DASKALA e.a., Safeguards in a world of ambient intelligence, Springer, 2008, p. xxi and 1
- C. ANDERSON, Free: the future of a radical price, 2009, p. 75-93
- C. ANDERSON, The long tail, edition 2009, p. 233
- M. BONNICI and G. PIA, Self-regulation in cyberspace, 2007, p. 25
- FP. DEEK and J.A.M. McHUGH, Open source. Technology and policy, Cambridge University Press, p. 159
- J. GANTZ and J.B. ROCHESTER, Pirates of the digital millennium, p. 78-88
- J. GOLDSMITH and T. WU, Who controls the Internet? Illusions of borderless world, p. 15
F. HAYEK, *The Road to Serfdom*, University Of Chicago, 1994


L. LESSIG, *Code and other laws of cyberspace*, 1999, p. 87


M. MILLER, *Cloud computing. Web-based applications that change the way you work and collaborate online*, Que, 1st edition, 2008, p. 26


2. Articles


- E. BARBRY and O. PROUST, "Le Web 2.0 passe la barre des prétoires", *Gazette du Palais*, 18 October 2007, p. 10
- J. BERLEUR and Y. POULLET, "Réguler Internet", *Études* 2002/11, Tome 397, p. 472
- T. BERNERS-LEE, *Net Neutrality: This is serious*, available at dig.csail.mit.edu/breadcrumbs/node/144
- M. CHAWKI and M. S. A. WAHAB, "Identity Theft in Cyberspace: Issues and Solutions", *Lex Electronica*, vol. 11 n° 1, p. 29
- C. DE PRETER, "Wie heeft nog boodschap aan de boodschap? De aansprakelijkheid van tussenpersonen onder de Wet Elektronische Handel", *Auteurs & Media* 2004, p. 265-266
M. DEMOULIN, "Information et transparence sur les réseaux" in *Le Commerce Électronique sur les rails?*, Bruylant, Brussels, 2001, p. 124

J. DUMORTIER and C. GOEMANS, "Online data Privacy and Standardization: Towards a More Effective Protection?", in *A Decade of Research @ the Crossroads of Law and ICT*, Larcier, Brussels, 2001, p. 57


V. FON and F. PARISI "On the Optimal Specificity of Legal Rules", *Journal of Institutional Economics* 2007, p. 4


J. GRIMMELMANN, "How to Fix the Google Book Search Settlement", *JILL*, vol. 12, nr. 10, p. 11
- M. GUILBAULT and N. HELBERGER, "Copyright law and consumer protection", European Consumer Law Group, February 2005, p. 11
- J. HARRINGTON, "Information society services: what are they and how relevant is the definition?", Computer Law & Security Report, Vol. 17, no. 3, 2001, p. 179
- O. ITO and N. PARKER, "Data protection law in Japan: a European perspective", World Data Protection Report 2008/12, p. 3-4


M.S. MARTIN, "Keep it online: the Hague Convention and the need for online alternative dispute resolution in international business-to-consumer e-commerce", *Boston University International Law Journal*, 2002:20, 125, p. 155


E. MONTERO, "Les responsabilités liées au web 2.0", in *Revue du Droit des Technologies de l'information* - n° 32/2008, p. 368

E. MONTERO, "La responsabilité des prestataires intermédiaires sur les réseaux", in *Le commerce électronique européen sur les rails?*, Bruylant, Brussels, 2001, p. 276

T. MOORES, "Do Consumers Understand the Role of Privacy Seals in eCommerce?", *Communications of the ACM*, March 2005, Vol. 48 No 3


T. O'REILLY, "Web 2.0 Principles and Best Practices", *O'Reilly Radar Report*


§ M. PEGUERA, "I just know that I (actually) know nothing": actual knowledge and other problems in ISP liability case law in Spain", EIPR, 2008, issue nr. 7, p. 281

§ Y. POULLET, "Pour une troisième génération de réglementation de protection des données", in M.V. PEREZ ASINARI and P. PALAZZI (eds.), Challenges of privacy and data protection law, Brussels, Bruylant, 2008, p. 38


§ A. RENDA, "I Own the Pipe, You Call the Tune: The Net Neutrality Debate and Its (Ir)relevance for Europe", CEPS, 2008, available at ssm.com/abstract=1291027, p. 23


§ N.C. ROWE and E.J. CUSTY, "Deception in Cyber Attacks", in Cyber Warfare and Cyber Terrorism, 2008, p. 94


§ P. TORREMANS, *Private International Law aspects of IP - Internet Disputes*, p. 24


§ L. THOUMYRE, "Responsabilité 2.0 ou l'éternel recommencement", *Revue Lamy Droit de l'Immatériel*, 2007/33, n° 1098


§ C. VASSILIOU - *Electronic payment systems and marketing: a literature review*, 2004


X, "Legal Issues in Open Source Software", LEGALIST, Issue date: 07/06/2005, p. 32

3. European Commission

3.1. Commission Staff Working Documents


- Commission Staff Working Document (SEC/2008/0511 final), Report on fraud regarding non cash means of payments in the EU: the implementation of the 2004-2007 EU action plan


3.2. Commission Recommendations

- Commission Recommendation of 12 May 2009 on the implementation of privacy and data protection principles in applications supported by radio-frequency identification, C(2009) 3200 final

3.3. Commission Communications and reflection documents

- Commission Communication on How to transform the ‘digital dividend’ into consumer benefits and up to €50 billion in economic growth for Europe?, 10 July 2009
- Commission Communication on An area of freedom, security and justice serving the citizen, COM (2009) 0262 final
- Commission Communication on Towards a general policy on the fight against cyber crime, 22 May 2007, COM(2008) 448 final
- Commission Communication on Creative content online in Single market, COM (2007) 836, p.6

- Commission Communication on *Unsolicited commercial communications or "spam"*, COM (2004) 28 final, 22 January 2004, p. 4
- Commission Communication on *Illegal and harmful content on the Internet called upon Member States to co-operate in exchanging information and defining minimum standards on criminal content*, COM (1996) 487

3.4. Reports

3.5. Commission proposals


3.6. Green papers and action plans


3.7. Studies sponsored by the Commission


- **Study on the implementation and effect in member states' laws of the Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society**, Institute for Information Law, final report, February 2007, p. 8

- **Study on the requirements imposed by the Member States, for the purpose of charging taxes, for invoices produced by electronic or other means**, by PriceWaterHouseCoopers, available at [http://ec.europa.eu/taxation_customs/taxation/vat/key_documents/reports_published/index_en.htm](http://ec.europa.eu/taxation_customs/taxation/vat/key_documents/reports_published/index_en.htm)


- **Intellectual property guidelines**, version 1.0, Minerva EC Working Group, September 2008, p. 31

3.8. Press releases


- **Electronic money: Commission consults on how the E-Money Directive applies to mobile phone services**, 10 May 2004, IP/04/620

- **E-commerce: EU law boosting emerging sector**, 21 November 2003, IP/03/1580

3.9. Speeches

V. REDING, SPEECH/08/616, *Digital Europe: the Internet Mega-trends that will Shape Tomorrow's Europe.*


V. REDING, SPEECH/06/697, *From Service Competition to Infrastructure Competition: the Policy Options Now on the Table*, 16 November 2006


4. **Council of Europe**


5. **European Parliament**


6. Working Party 29

- Opinion 5/2009 on online social networking (WP 136), 12 June 2009

7. Other reports and studies

- J. CAVE, C. MARSDEN, S. SIMMONS, Options for and Effectiveness of Internet Self and Co-Regulation, Report prepared for the European Commission, 2008, p. 8
- C. CALLANAN and M. GERCKE, Cooperation between law enforcement and internet service providers against cybercrime: towards common guidelines, Council of Europe Project against Cybercrime, final version, 25 June 2008
- COMPTIA (The Computer Technology Industry Association), CompTIA EU Electronic Invoicing and VAT compliance requirements Publication, 2005, available at www.comptia.org


I. FREDESWINDA, The Admissibility of Digital evidence in Court (A.E.E.C.): Fighting against High-Tech Crime, Results of a European Study


H. SCHEPPEL and J. FALKE, Legal aspects of standardisation in the Member States of the EC and EFTA, vol. 1, European Communities, 2000, p. 97

S. SIMITIS, Revisiting sensitive data, 1999

TIME.LEX, Study on activities undertaken to address threats that undermine confidence in the Information Society, such as spam, spyware and malicious software, ordered by the Commission, SMART 2008/ 0013, from , 10 February 2009
- P. VAN EECKE, P. PINTO and T. EGYEDI, EU Study on the specific policy needs for ICT standardisation, study commissioned by the European Commission, available at www.ictstandardisation.eu
- T. VERBIEST, G. SPINDLER, G.M. RICCIO, A. VAN DER PERRE, Study on liability of Internet intermediaries, ordered by the European Commission, November 2007, p. 34

8. Conference material

- J. HÖRNLE, ”Online Dispute Resolution - More than the Emperor's new clothes.”, Proceedings of the UNECE forum on ODR, 2003, p. 25
9. Position papers

- AIB (Associazione Italiana Biblioteche), *Comments to the Green Paper on Copyright in the Knowledge Economy at the European Commission*, p. 3
- ALCS (Authors’ Licensing & Collecting Society), *Submission to the All Party Internet Group Inquiry into Digital Rights Management*, 17 January 2006
- ALLIANCE AGAINST IP THEFT, *Comments to the Green Paper on Copyright in the Knowledge Economy at the European Commission*, p. 1
- BSA (Business Software Alliance), *Comments to the Green Paper on Copyright in the Knowledge Economy at the European Commission*, p. 2
- CENL (Foundation Conference of European National Librarians) *Response on the Green Paper on Copyright in the Knowledge Economy*, p. 6
- CEPI, (European Coordination of Independent Producers), *Comments to the Green Paper on Copyright in the Knowledge Economy at the European Commission*, p. 3
- CEPIC (Council of European Professional Informatics Societies), *Co-ordination of European Picture Agencies Press Stock Heritage Response to EC Green Paper on Copyright in the Knowledge Economy*, p. 6
- DACS (Designs and Artists Copyright Society), *Comments to the Green Paper on Copyright in the Knowledge Economy at the European Commission*, p. 2
- EIF (European Internet Foundation) *Opinion shared by the European Internet Foundation, The digital world in 2025 - indicators for European Action*, p. 22, available at www.eifonline.org/site/download.cfm?SAVE=10859&LG=1
- FOBID, *Comments to the Green Paper on Copyright in the Knowledge Economy at the European Commission*, p. 6
- GOOGLE, *Comments to the Green Paper on Copyright in the Knowledge Economy at the European Commission*, p. 8
- ICMP (International Confederation for Music Publishers), *Comments to the Green Paper on Copyright in the Knowledge Economy at the European Commission*, p. 2

ICRI (Interdisciplinary Centre For Law And ICT at the K.U. Leuven), *Comments to the Green Paper on Copyright in the Knowledge Economy at the European Commission*, p. 3

UNIVERSITY OF LODZ, *Comments to the Green Paper on Copyright in the Knowledge Economy at the European Commission*, p. 4

10. Legislation

10.1. Directives

- Directive 2006/112/EC of 28 November 2006 on the common system of value added tax, OJ L 347/1
- Directive 2005/60/EC on the prevention of the use of the Financial system for the purpose of money laundering and terrorist financing, OJ L 309/15
- Directive 98/84/EC of 20 November 1998 on the legal protection of services based on, or consisting of, conditional access, OJ L 320
- Directive 97/7/EC of 20 May 1997 on the protection of consumers in respect of distance contracts, OJ L 144/19 ("Distance Selling Directive")
- Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281/31 ("Data Protection Directive")
- Directive 92/100 EEC of 19 November 1992 on rental right and lending right and on certain rights related to copyright in the field of intellectual property, OJ L 346/61
10.2. Council Decisions

- Decision 456/2005/EC of 9 March 2005 establishing a multiannual Community programme to make digital content in Europe more accessible, usable and exploitable, OJ L 79/1

10.3. Regulations

- Regulation 593/2008 of 17 June 2008 on the law applicable to contractual obligations, OJ L 177/6 (“Rome I Regulation”)
- Regulation 864/2007 of 11 July 2007 on the law applicable to non-contractual obligations, OJ L 199/40 (“Rome II Regulation”)
- Regulation 861/2007 of 11 July 2007 establishing a European small claims procedure, OJ L 199/1
- Regulation 460/2004 of 10 March 2004 establishing the European Network and Information Security Agency, OJ L 77/1
- Regulation 2006/2004 of 27 October 2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, OJ L 364/1
- Regulation 874/2004 of 28 April 2004 laying down public policy rules concerning the implementation and functions of the .eu Top Level Domain and the principles governing registration, OJ L 162/40
- Regulation 2887/2000 of 18 December 2000 on unbundled access to the local loop, OJ L 336/4

10.4. Framework decisions

- Council Framework Decision 2001/413/JHA of 28 May 2001 on combating fraud and counterfeiting of non-cash means of payment, OJ L 149/1

10.5. Treaties

There are several key legal documents related to intellectual property and data protection that are important in the context of a Single Market for an Information Society:

- **Agreement on Trade - Related Aspects of Intellectual Property Rights of 15 April 1994 (TRIPs),** available at [www.wto.org/english/tratop_e/trips_e/agt02_e.htm](http://www.wto.org/english/tratop_e/trips_e/agt02_e.htm)
- **Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe of 28 January 1981,** available at

### 11. Case law

#### 11.1. European Court of Justice

- ECJ, C-553/07, *Rijkeboer*, 7 May 2009
- ECJ, C-42/07, *Bwin vs. Santa Casa*, 8 September 2009
- ECJ, C- 275/06, *Productores de Musica de Espana (Promusicae) v. Telefonica de Espana SAU*
- ECJ, T-201/04 *Microsoft vs. The Commission*, 17 September 2007
- ECJ, C-243/01, *Piergiorgio Gambelli et al.*, 6 November 2003
- ECJ, C-109/92, *Stephan Max Wirth v Landeshauptstadt Hannover*, 7 December 1993
- ECJ, T-320/91, *Corbeau*, 19 May 1993
- ECJ, C 352/85, *Bond van Adverteerders v the Netherlands*, 1988

#### 11.2. European Court of Human Rights


#### 11.3. Belgium

- Court of Commerce (Brussels), 31 July 2008, (A/07/06032)
- Court of First Instance, *Sabam v. Tiscali/Scarlet*, 26 November 2004 and 29 June 2007
11.4. Denmark

- Court of Copenhagen, *Tele2*, 25 October 2006

11.5. France

- Court of Appeal (Paris), *SARL Publison System v SARL Google France*, 19 March 2009
- Tribunal de grande instance, (Paris), *Olivier Martinez, Robert Martinez v Société MGN Limited*, 16 July 2009
- Tribunal de grande instance (Troyes), *Hermès International v. eBay*, 4 June 2008
- District Court (Puteaux), *Ava v. Inforie and others*, 28 September 1999
- Tribunal de Grande Instance (Nanterre), *Lacoste/Multimania, Esterel and Cybermedia*, 8 December 1999
- Tribunal de Grande Instance (Paris), *Calvacom, Eunet, Axone, Compuserve, Francenet et Imaginet*, 12 June 1996

11.6. Germany

- Oberlandesgericht (Hamburg), 2 July 2008;
- District Court of Düsseldorf, 23 January 2008;
- LG Düsseldorf, 23 May 2007, 12 O 151/07, MMR 2007, 534 (535)
- District Court of Munich I, *Open Source – effectiveness of GPL*, 19 May 2004
- Bundesgerichtshof, 23 September 2003, VI ZR 335/02, NJW 2003, 3764

11.7. Italy


11.8. The Netherlands

- Court of Amsterdam, 12 March 2009
- Court of Amsterdam, *Jensen v Google Netherlands*, 26 April 2007
- Court of The Hague, 5 January 2007
11.9. Spain
- Court of First Instance (Madrid), *Palomo v Google Inc.*, 13 May 2009

11.10. Sweden
- Stockholm District Court, Division 5, Unit 52, 17 April 2009, handed down in Stockholm, ref. B 13301-06, p. 15 available at www.ifpi.org

11.11. United Kingdom
- Youth Court (Wimbledon), *R v. a minor*, 2 November 2005
- Queen's Bench Division, *Godfrey v. Demon Internet*, [1999] 4 All ER 342

11.12. United States
- Supreme Court, *SGAE v. Asociacion de Internautas*, case pending
- Supreme Court (California), *Barrett v. Rosenthal*, 146 P.3d 510, 527 (Cal. 2006)
- Supreme Court, *National Cable & Telecommunications Association et al. v. Brand X Internet Services et al.*, 27 June 2005
- Supreme Court, Griswold v. Connecticut, 381 U.S. 479 (1965)
- Court of Appeals, *Rossi v. Motion Picture Ass’n of America*, 391 F.3d 1000, 1004-05 (9th Cir. 2004)
- Court of Appeals, *Doe v. GTE*, 347 F.3d 655 (7th Cir. 2003)
- Court of Appeals (California), *Gentry v. eBay, Inc.*, 121 Cal. Rptr. 2d 703, 717 (Ct. App. 2002)
- Court of Appeals, *A&M Records, Inc. v. Napster*, Inc., 239 F.3d 1004 (9th Cir. 2001)
- Court of Appeals, *Zeran v. America Online, Inc.*, 129 F.3d 327 (4th Cir. 1997), at 331
- Federal District Court (California), *Lenz v. Universal Music Corp.*, 572 F. Supp. 2d 1150 (N.D.Ca. 2008)
- District Court (Virginia), *America Online, Inc. v. IMS*, 24 F.Supp.2d 548 (E.D., Va., 1998)

12. **Miscellaneous documents**

12.1. **ENISA**

12.2. **OECD**
- *Consumer dispute resolution and redress in the global marketplace*, OECD, 2006, p. 28

12.3. **Organization for Security and Co-operation in Europe (OSCE)**

12.4. **France**

12.5. Netherlands

12.6. United Kingdom

12.7. Australia

12.8. Canada
- Office of the Privacy Commissioner of Canada, What is deep packet inspection?, available at dpi.priv.gc.ca

12.9. United States
- Internet Freedom Preservation Act of 2009
- Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (US CAN-SPAM Act)
- Uniform Money Services Act of 4 August 2000, p. 5, available at www.law.upenn.edu/bll/ulc/moneyserv/ms00ps.htm
