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

DLA PIPER

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 (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.

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.

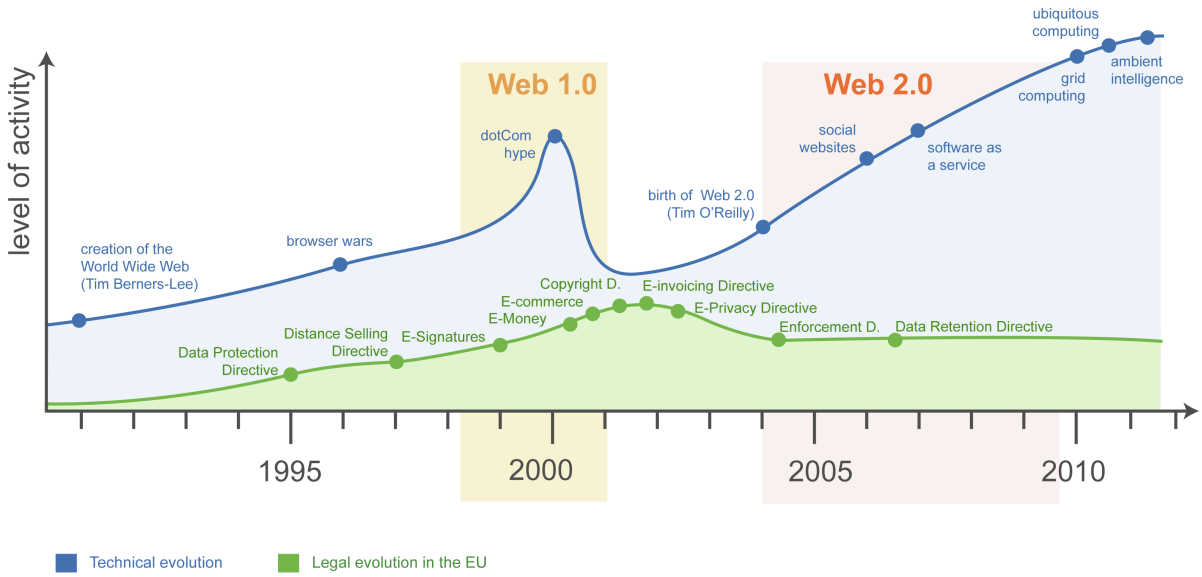

Figure 1: technological versus legislative activities in the field of information technology

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.

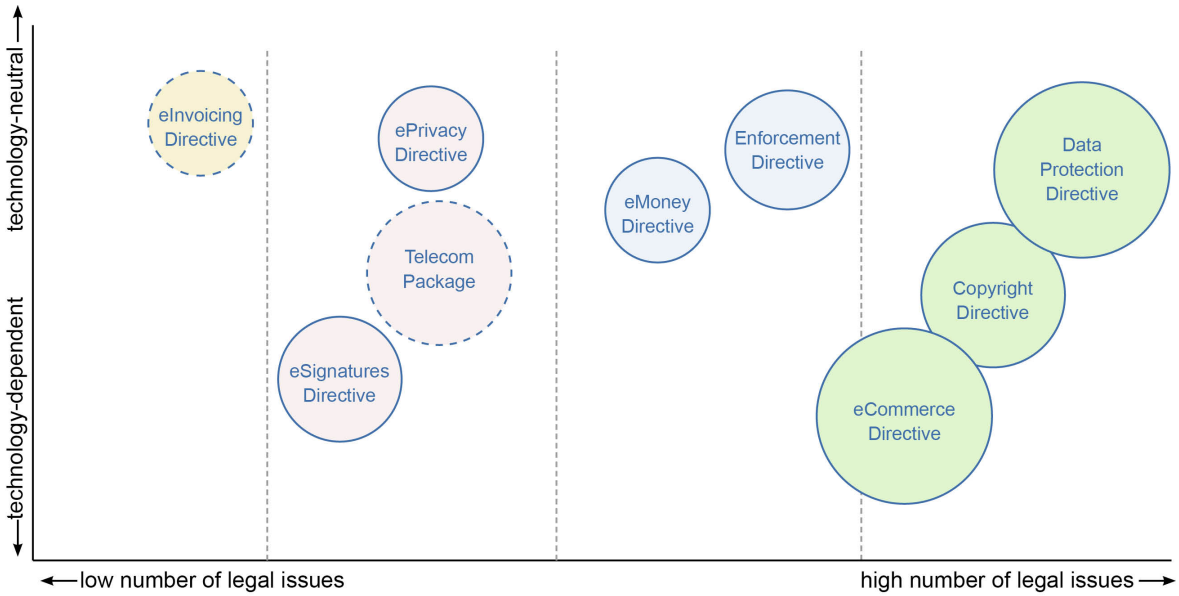

Figure 2: technological neutrality and number of legal issues of each Directive

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 laywers 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.