

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

Table of contents

Chapter 10 Spam	2
1. Introduction.....	2
2. Overview	2
2.1. <i>Problems caused by spam</i>	2
2.2. <i>Reasons for spamming</i>	4
2.3. <i>Definition of spam</i>	4
2.4. <i>Legal treatment of spam under current EU framework</i>	6
2.5. <i>Legal issues under the current legal framework</i>	8
2.6. <i>Enforcement</i>	15
2.7. <i>Retention of spam</i>	18
3. Conclusions.....	19
4. Recommendations	19
4.1. <i>Short term</i>	20
4.2. <i>Mid-term</i>	23
4.3. <i>Long term</i>	25
Chapter 11 Cybercrime	27
1. Introduction.....	27
2. Applicable legal instruments.....	27
2.1. <i>CyberCrime Convention</i>	27
2.2. <i>Framework Decision on Attacks against Information Systems</i>	29
2.3. <i>Data Retention Directive</i>	31
2.4. <i>Data protection legislation</i>	32
2.5. <i>Other legal instruments</i>	33
3. International cooperation.....	33
3.1. <i>ENISA</i>	33
3.2. <i>The G8 High-Tech Crime Sub-Group 24/7</i>	33
3.3. <i>Organization for Security and Co-operation in Europe</i>	34
4. Are all types of cybercrime harmonised?	34
4.1. <i>Phishing</i>	34
4.2. <i>Identity theft</i>	35
4.3. <i>DoS attacks</i>	37
4.4. <i>Spyware and other malware</i>	38
5. Conclusions.....	38
6. Recommendations	39
6.1. <i>Supporting the Cybercrime Convention</i>	39
6.2. <i>Supporting a harmonised implementation of the Framework Decision</i>	39
6.3. <i>Strengthening cooperation between authorities</i>	39
6.4. <i>Encouraging authorities to take action</i>	40
6.5. <i>Additional responsibility for access providers</i>	40
6.6. <i>Public-private sector cooperation</i>	40

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

I. 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-mail¹. Following the shutdown, various security firms reported a steep decline of 75 percent in the volume of unsolicited e-mail sent worldwide².

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 solution³.

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 investigated⁴.

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 traffic⁵. In addition, one in 317 e-mails was identified to contain malware, and one in 404 e-mails comprised a phishing attack⁶.

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 recipient⁷. 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?spamyyear for a graphical illustration of the impact of the McColo shutdown on the amount of unsolicited e-mail.

³ IViR, *Regulating spam - Directive 2002/58 and beyond*, section 1.1; OECD, *Report of the OECD task force on spam: anti-spam toolkit of recommended policies and measures*, April 2006, available at www.oecd-antispam.org/article.php3?id_article=265, p. 24

⁴ The word "spam" will be used to refer collectively to all of these manifestations of unsolicited communications.

⁵ See www.messagelabs.com/download.get?filename=MLIRReport_2009_05_May_FINAL.pdf

⁶ See Chapter 11 - Cybercrime

⁷ Preamble 40 ePrivacy Directive

pharmaceuticals 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 time⁸. 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 whole⁹. 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 botnets¹⁰. A botnet is a network consisting of computers that have been infected by malicious code allowing them to be remotely controlled. Spammers build (or rent¹¹) 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 attacks¹².

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 costs¹³.

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, etc¹⁴.

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 individuals¹⁵. One recent report estimates that spam will cost a total of 91,6 billion EUR worldwide in 2009¹⁶.

⁸ See Commission communication, *on fighting spam, spyware and malicious software*, COM (2006) 688 final, p. 3

⁹ Commission communication, *on unsolicited commercial communications or "spam"*, p. 4

¹⁰ See www.messagelabs.com/mlireport/MLIReport_2009.06_June_FINAL.pdf

¹¹ See http://news.zdnet.com/2100-9595_22-312957.html

¹² See Chapter 11 - Cybercrime

¹³ M.Y. SCHAUB, "Unsolicited e-mail, does Europe allow spam? The state of the art of the European legislation with regard to unsolicited commercial communications", *Computer Law & Security Report* Vol. 18 no. 2, 2002, p. 101

¹⁴ Commission communication, *on unsolicited commercial communications or "spam"*, p. 8

¹⁵ OECD, *Report of the OECD task force on spam: anti-spam toolkit of recommended policies and measures*, April 2006, available at www.oecd-antispam.org/article.php3?id_article=265, p. 22

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 Group¹⁷ 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 offered¹⁸. A recent study showed that spammers can expect to receive one response for every 12.5 million e-mails they send¹⁹.

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 bulk²⁰. Certain definitions also stress the commercial nature of spam²¹.

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 message²². 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 sent²³.

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.maaawg.org/home

¹⁸ <http://arstechnica.com/web/news/2009/07/12-of-e-mail-users-try-to-buy-stuff-from-spam-e-mail.ars>

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.

²² iViR, *Regulating spam - Directive 2002/58 and beyond*, 2004, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=607183, section 1.3

²³ iViR, *Regulating spam - Directive 2002/58 and beyond*, 2004, o.c., section 1.3

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 difficult²⁴.

Regulators sometimes use a specific number of messages that is being sent as a touchstone for regulatory intervention²⁵. 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 messages²⁶. 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 legitimate²⁷.

- **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."

²⁷ See <http://www2.opta.nl/asp/en/publications/document.asp?id=2801>

related activity, a message constitutes spam only if it is both unsolicited and bulk²⁸. 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-phishing²⁹.

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 in 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 Directive³⁰ aims to protect the consumer's right to privacy by barring or limiting the use of certain particularly intrusive means of communication³¹. 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 resulted in the adoption of the European ePrivacy Directive and the adoption of the US CAN SPAM Act 2003³².

Opt-in requirement – The 2002 ePrivacy Directive harmonised the opt-in requirement, and refined the provisions of the eCommerce Directive in relation to spam.

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

³⁰ See Preamble 17 of Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts, OJ L 144, 4.6.1997, p. 19–27

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 prohibit 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 practices³³. 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 practice³⁴.

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".

³³ Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive'), O.J. L 149 of 11.06.2005, p. 22

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 reasons³⁶:

- 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 mail³⁷, 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 regime³⁹. 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 removed⁴⁰.

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

³⁵

³⁶ Article 29 Working Party, *Working document "Privacy on the Internet" - An integrated EU Approach to On-line Data Protection*, 21 November 2002, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2000/wp37en.pdf, p. 77

³⁷ Article 13.1 of the ePrivacy Directive

³⁸ Article 2.h of the ePrivacy Directive

³⁹ Article 13.3 of the ePrivacy Directive

⁴⁰ 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 bots⁴¹. 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)⁴². 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 played⁴³. Since the software enabling the automated calls probably qualifies as an "automated calling machine", VoIP spam is covered by the Directive⁴⁴.
- **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 advertisements⁴⁵. 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.

⁴² See http://news.cnet.com/Gnutella-girds-against-spam-attacks/2100-1023_3-244331.html

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 spam⁴⁶. Therefore, we propose to implement another, more technology-neutral definition of spam⁴⁷. 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 neutrality⁴⁸.

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 newspaper⁴⁹.

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 artificial⁵⁰. 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)⁵¹. 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 apply⁵². 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

⁵⁰ L. F. ASSCHER and S.A. HOOGCARSPEL, *Regulating spam*, Cambridge University Press., 2006, p. 40

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 matter⁵³.

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 occurs⁵⁴. 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 Directive⁵⁵ as well as in the ePrivacy Directive⁵⁶, but in practice it is often unclear what actions are required to record a sufficient consent.

⁵³ L. F. ASSCHER, S.A. HOOGCARSPPEL, *Regulating spam*, Cambridge University Press., 2006, p. 171

⁵⁴ ECJ C 21/76, *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 subject⁵⁷.

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 conditions⁵⁸:

- 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 authority⁵⁹, 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 place⁶⁰. 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

⁵⁹ See www.ddma.nl/index.php?pag=2&nieuws=153

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 years⁶¹.

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 laws⁶². 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 behaviour⁶³.

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 litigation⁶⁴. 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 parties⁶⁵. 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 defendant⁶⁶. 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 sent⁶⁷. For messages which do not contain misleading header information, damages are fixed at 25 \$ per message⁶⁸. 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

⁶⁴ See *Statutory Private Rights of Action in Canada: A Statutory Private Right of Action against Spammers in Canada*, Report to Industry Canada's Task Force on Spam, December 17, 2004, available at www.ic.gc.ca/eic/site/ecic-ceac.nsf/eng/gv00303.html

⁶⁵ www.oecd-antispam.org/article.php3?id_article=239

⁶⁶ U.S.C. § 7706(g)(1)

⁶⁷ U.S.C. § 7706(g)(3)(A)(i)

⁶⁸ U.S.C. § 7706(g)(3)(A)(ii)

misleading header information, the total amount of damages is capped at 1.000.000 \$⁶⁹. Damages can be raised or lowered, in case of aggravating or mitigating circumstances⁷⁰.

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 action⁷¹. 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.

⁶⁹ U.S.C. § 7706(g)(3)(B)

⁷⁰ For example, if 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.

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 legislation⁷².

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 required⁷³.

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 legislation⁷⁴. In addition, a voluntary agreement was drawn up in February 2005 to establish a common procedure to facilitate cross-border handling of spam complaints⁷⁵. 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

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/fsj/privacy/docs/wpdocs/2006/wp118_en.pdf

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.

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>

⁷⁵ OECD, *o.c.*, p. 40

exchange and co-operation and the possibility of requesting action from their counterparts in other Member States⁷⁶.

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 countries⁷⁷. 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 application⁷⁸. 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 viruses⁷⁹. 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 stakeholders⁸⁰.

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 spammers⁸¹.
- 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

⁷⁶ Commission communication, on *unsolicited commercial communications or "spam"*, p. 18

⁷⁷ Regulation 2006/2004 of the European Parliament and of the Council of 27 October 2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, OJ L 364 09.12.2004, p. 1-11

⁷⁸ The Distance Selling Directive, eCommerce Directive and Unfair Commercial Practices Directives are within the scope of the Regulation.

⁷⁹ See www.londonactionplan.com/?q=node/1

⁸⁰ *Annex to the Communication on the European Electronic Communications Regulation and Markets 2005* (COM (2006) 68 final), p. 67

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 service⁸².

- 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 €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 software⁸⁴.

In a recent Commission-funded study on spam, spyware and malicious software⁸⁵ 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"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 limited⁸⁷. The fact that the European legal framework is focused on spam with commercial intent, can be expected to strengthen this trend⁸⁸. 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

⁸² See www.out-law.com/page-4306

⁸³ The decision to impose the fine (only available in French) is available at www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000020444356&fastReql=252983250&fastPos=1

⁸⁴ Communication from the Commission, *Progress report on the single European Electronic Communications Market 2008 (14th report)*, (COM (2009) 140, final), p. 17

⁸⁵ "Study on activities undertaken to address threats that undermine confidence in the Information Society, such as spam, spyware and malicious software", SMART 2008/ 0013, from Time.Lex CVBA, dated 10/2/2009

⁸⁶ Ibidem, paragraph 1.1.2, p. 11

⁸⁷ Commission communication, *on fighting spam, spyware and malicious software*, COM (2006) 688 final, p. 6

⁸⁸ See Section 2.5.1

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 useful⁸⁹. 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 penalties⁹⁰.

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-mails⁹¹.

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 authority⁹². 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 persons⁹³. 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 Directive⁹⁴ requires internet access providers and telecom operators⁹⁵ 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.

⁸⁹ 12th report on the Implementation of the Telecommunications Regulatory Package, COM(2007) 155, available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0155:FIN:EN:PDF>

⁹⁰ 13th Report on the Implementation of the Telecommunications Regulatory Package, COM (2008) 153, available at http://ec.europa.eu/information_society/policy/ecom/doc/library/annualreports/13th/com_2008_153_en_final.pdf

⁹¹ Commission Staff Working Document (SEC(2009) 376), p. 66, available at http://ec.europa.eu/information_society/policy/ecom/doc/implementation_enforcement/annualreports/14threport/annex1.pdf

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 Directive 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 levels⁹⁷. Due to legal and technical difficulties, there is no simple solution or "silver bullet" to stop spam⁹⁸.
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. 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 effectively⁹⁹. 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^{100 101}.

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 security¹⁰². 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 conduct¹⁰³. A similar system – which involves no money at all – is advocated by Microsoft: computational spam-fighting¹⁰⁴. 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 privacy¹⁰⁵.

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 members¹⁰⁶.

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 legislation¹⁰⁷.

¹⁰² OECD, o.c., p. 29

¹⁰³ See www.ironport.com/pdf/ironport_2002-06-25.pdf

¹⁰⁴ See <http://research.microsoft.com/en-us/projects/pennyblack/spam-com.aspx>

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 marketing¹⁰⁸.

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 spam¹⁰⁹. 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 Providers¹¹⁰. 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 spammers¹¹¹. 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"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"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 rules¹¹⁴. 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 reported¹¹⁵
¹¹⁶

¹⁰⁸ Commission communication, on *unsolicited commercial communications or "spam"*, p. 22

¹⁰⁹ See www.microsoft.com/presspass/press/2004/jun04/06-22ASTAPR.mspx

¹¹⁰ See www.euroispa.org

¹¹¹ See www.spotspam.com

¹¹² Available at http://gsmworld.com/documents/code_of_practice.pdf

¹¹³ Section 5 of the Code of Practice

¹¹⁴ See section 2.5.11

¹¹⁵ OECD, *o.c.*, p. 45

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 priorities¹¹⁷. The Commission has supported the use of dedicated mailboxes through the funding of the SPOTSPAM initiative¹¹⁸.

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 legislation¹¹⁹. 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 Party¹²⁰. 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

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 system¹²¹. 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:

¹²¹ Position of the European Parliament adopted at second reading on 6 May 2009 with a view to the adoption of Directive 2009/.../EC of the European Parliament and of the Council amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws.

(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 above¹²³. 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 Plan¹²⁴. 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 2005¹²⁵. 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

¹²⁴ World Summit on the Information Society, *Declaration of principles*, 12 December 2003, p. 37, available at www.itu.int/wsis/docs/geneva/official/dop.html

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 I I

Cybercrime

I. 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 date¹²⁶. The much smaller Storm botnet, which contained around 75000 computers, was estimated to bring in 2,4 million euros in revenue per year¹²⁷. The Organization for Security and Cooperation in Europe (OSCE) estimates that cybercrime costs the global economy \$100 billion a year¹²⁸.

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 Cybercrime¹²⁹. 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-operation¹³⁰.

¹²⁶ See www.f-secure.com/weblog/archives/00001584.html

¹²⁷ See <http://arstechnica.com/security/news/2008/11/study-storm-botnet-brought-in-daily-profits-of-up-to-9500-ars>

¹²⁸ See www.diplomaticcourier.org/kmitan/articleback.php?newsid=327

¹²⁹ See <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>

¹³⁰ Council of Europe, Explanatory Report to the Convention on Cybercrime, available at <http://conventions.coe.int/treaty/en/reports/html/185.htm>

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 offences¹³¹.

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 committed¹³². 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 Cybercrime¹³³. A significant number of European Member States are among the signatories that have yet to ratify the

¹³¹ Liability arises for aiding or abetting where the person who commits a crime is aided by another person who also intends that the crime be committed. For example, although the transmission of racist and xenophobic material through the Internet requires the assistance of service providers as a conduit, a service provider that does not have the criminal intent cannot incur liability under the Protocol. See Council of Europe, Explanatory Report to the Additional Protocol to the Convention on Cybercrime, available at <http://conventions.coe.int/treaty/EN/Reports/Html/189.htm>

¹³² S. KIERKEGAARD, "Cracking Down on Cybercrime - Global Response: The Cybercrime Convention", 2005, *CIIMA Journal* Volume 5 Issue 1, p. 60

¹³³ An overview of the signatories and the ratification status of the Convention is available at <http://conventions.coe.int/Treaty/Commun/ListeTableauCourt.asp?MA=49&CM=16&CL=ENG>

Convention¹³⁴. The situation with regard to the Additional Protocol to the Convention is similar¹³⁵. 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 Protocol¹³⁶.

The Council of Europe itself has cited the low number of ratifications of the Convention as its biggest weakness¹³⁷. 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 attack¹³⁸. 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 cybercrime¹³⁹. Also in 2007, the European Council called for the development of a policy framework in the field¹⁴⁰. 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 proceed¹⁴¹.

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 Cybercrime¹⁴². 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 Systems¹⁴³. 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 decision¹⁴⁴.

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

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>

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.

¹³⁷ Report of the Committee on Legal Affairs and Human Rights, *How to prevent cybercrime against state institutions in member and observer states?*, 26 June 2007, available at <http://assembly.coe.int/Documents/WorkingDocs/Doc07/EDOC11325.pdf>

¹³⁸ See section 4.3

¹³⁹ See www.infoworld.com/d/security-central/ec-urges-coordinated-effort-against-cybercrime-267

¹⁴⁰ See www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/ec/94932.pdf

¹⁴¹ Report of the Committee on Legal Affairs and Human Rights, *How to prevent cybercrime against state institutions in member and observer states?*, 26 June 2007, available at <http://assembly.coe.int/Documents/WorkingDocs/Doc07/EDOC11325.pdf>, p. 6; COM (2007) 267 final, *Towards a general policy on the fight against cyber crime*, 22 May 2007, not published in the O.J., p. 3; L. JANCZEWSKI, A. M. COLARIK, *Cyber warfare and cyber terrorism*, Idea Group Inc, 2008, p. 470; J. A. LEWIS, *Cyber security: turning national solutions into international cooperation*, Center for Strategic and International Studies, Washington, 2003, p. 28

¹⁴² Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, 21 January 2001, not published in the O.J. (COM (2000) 890 final)

¹⁴³ Council Framework Decision 2005/222/JHA of 24 February 2005 on Attacks against Information Systems, O.J. L 069, 16.03.2005, p. 67 - 71. The motivation behind the adoption of the Framework Decision is set out in recital 2

¹⁴⁴ Report from the Commission to the Council, Based on Article 12 of the Council Framework Decision of 24 February 2005 on attacks against information systems, 17 June 2008, not published in the O.J. (COM(2008) 448 final)

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 systems¹⁴⁵. 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 neutrality¹⁴⁶. 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 offence¹⁴⁷. 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 imprisonment¹⁴⁸.

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 nationals¹⁴⁹. 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 week¹⁵⁰.

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 incomplete¹⁵¹. 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 Spain¹⁵².

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

¹⁵¹ Report from the Commission to the Council, Based on Article 12 of the Council Framework Decision of 24 February 2005 on attacks against information systems, 17 June 2008, not published in the *O.J.*, p. 2 (COM (2008) 448 final)

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 States¹⁵³. 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"¹⁵⁴.

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 offences¹⁵⁵. In some Member States, similar problems exist with respect to the description of illegal system and illegal data interference¹⁵⁶.

2.3. Data Retention Directive

The aim of the Data Retention Directive¹⁵⁷ 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 e-mail. All affected parties need 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

¹⁵⁶ Report from the Commission to the Council, Based on Article 12 of the Council Framework Decision of 24 February 2005 on attacks against information systems, COM (2008) 448 final, 17 June 2008, not published in the *O.J.*, p. 5 - 6

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 vote¹⁵⁸.

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 information¹⁵⁹. 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 Directive¹⁶⁰, this article would be further optimised to target spyware.
- In the current parliament proposal to amend the ePrivacy Directive¹⁶¹, 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 Directive¹⁶².

¹⁵⁸ ECJ C-301/06, *Ireland v Parliament and Council*, O.J. C 82 of 04.04.2009, p. 2

¹⁵⁹ IviR, o.c., section 3.1

¹⁶⁰ See www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P6-TA-2009-0360

¹⁶¹ See www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P6-TA-2009-0360

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 recognise fraud involving any form of non-cash means of payment as a criminal offence in all EU Member States¹⁶³. 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 States¹⁶⁴. 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 established¹⁶⁵. 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 States¹⁶⁶. 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 issues¹⁶⁷.

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 crime¹⁶⁸. In 1998, the subgroup developed and established a

infringements, including an electronic communications service provider protecting its legitimate business interests, may bring legal proceedings in respect of such infringements. Member States may also lay down specific rules on penalties applicable to providers of electronic communications services which by their negligence contribute to infringements of national provisions adopted pursuant to this Article."

¹⁶³ Council Framework Decision 2001/413/JHA of 28 May 2001 on combating fraud and counterfeiting of non-cash means of payment, *O.J. L* 149, 2.6.2001, p. 1 – 4

¹⁶⁴ Council framework Decision 2004/68/JHA of 22 December 2003 on combating the sexual exploitation of children and child pornography. *O.J. L* 13, 20.1.2004, p. 44 – 48

¹⁶⁵ Regulation (EC) No 460/2004 of the European Parliament and of the Council of March 10, 2004, establishing the European Network and Information Security Agency, *O.J. L* 77 of 13.04.2004, p. 1

¹⁶⁶ Commission Communication, *Towards a general policy on the fight against cyber crime*, 22 May 2007, not published in the *O.J.* (COM (2007) 267 final)

¹⁶⁷ See www.enisa.europa.eu

¹⁶⁸ See http://ec.europa.eu/justice_home/fsj/crime/structures/fsj_crime_structures_en.htm

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 cybercrime¹⁶⁹. 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 cybercrime¹⁷⁰.

3.3. Organization for Security and Co-operation in Europe

The Organization for Security and Co-operation in Europe (OSCE) is an *ad hoc* organisation under the United Nations Charter consisting of fifty-six states in Europe, Central Asia, and America¹⁷¹. The OSCE Action Against Terrorism Unit (ATU) has a mandate to combat the use of the Internet for terrorist purposes¹⁷². 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 Cybercrime¹⁷³. The Ministerial Council's decision, which served as an update to an existing decision on combating the use of the Internet for terrorist purposes¹⁷⁴ also encouraged member states to participate in the G8 24/7 Network of Contacts for High-Tech Crime¹⁷⁵.

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 Convention¹⁷⁶. Below, it will be verified whether contemporary criminal activities committed in or through cyberspace are sufficiently covered by the Convention and the Framework Decisions.

4.1. Phishing

Concept – "Phishing" is a form of cybercrime that is carried out to make a victim disclose personal or secret information¹⁷⁷. By sending out e-mails that look like an e-mail from a legitimate source (such as a

¹⁶⁹ Stein SCHJOLBERG, "The History of Global Harmonization on Cybercrime Legislation - The Road to Geneva", 2008, p.13, available at www.cybercrimelaw.net/documents/cybercrime_history.pdf

¹⁷⁰ See www.usdoj.gov/criminal/cybercrime/g82004/g8_background.html

¹⁷¹ See the cyber security organization catalog, available at www.cistp.gatech.edu/catalog/oneOrg.php?id=61

¹⁷² Organization for Security and Co-operation in Europe (2001) The Bucharest Plan of Action for Combating Terrorism. MC(9).DEC/1, available at www.osce.org/documents/cio/2001/12/670_en.pdf

¹⁷³ Organization for Security and Co-operation in Europe (2006) Decision No. 7/06: Countering the Use of the Internet for Terrorist Purposes, available at www.osce.org/documents/mcs/2006/12/22559_en.pdf

¹⁷⁴ Organization for Security and Co-operation in Europe (2004) Decision No. 3/04: Combating the Use of the Internet for Terrorist Purposes. 2nd Day of the 12th Meeting, available at www.osce.org/documents/mcs/2004/12/3906_en.pdf

¹⁷⁵ See Section 3.2

¹⁷⁶ M. CHAWKI and M. S. A. WAHAB, "Identity Theft in Cyberspace: Issues and Solutions", *Lex Electronica*, vol. 11 n° 1, p. 29

¹⁷⁷ 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

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 user¹⁷⁸. 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"¹⁷⁹. 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 property¹⁸⁰.

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, it is often combined with sophisticated and even automated attacks at a manageable cost¹⁸¹.

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 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 counter¹⁸². The breach saw 4.2 million credit card numbers taken, and more than 1,800 of those numbers have been reported as having been used¹⁸³.

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 details¹⁸⁴.

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 perpetrator¹⁸⁵. 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

¹⁸² See <http://homeland.house.gov/SiteDocuments/20090331141915-60783.pdf>

¹⁸³ See www.bankinfosecurity.com/articles.php?art_id=810

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 theft¹⁸⁶. Such a separate provision on identity theft was recently adopted by Norway.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 requests¹⁸⁸. 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 technologies¹⁸⁹.

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 attacks¹⁹⁰. 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 interference¹⁹¹. 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 botnets¹⁹². 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,

¹⁸⁶ Commission Communication, *Towards a general policy on the fight against cyber crime*, 22 May 2007, not published in the O.J., p. 8 (COM (2007) 267 final)

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"

¹⁸⁸ N.C. ROWE and E.J. CUSTY, "Deception in Cyber Attacks", in *Cyber Warfare and Cyber Terrorism*, 2008, p. 94

¹⁸⁹ See www.guardian.co.uk/world/2007/may/17/topstories3.russia

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.

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.

¹⁹² Report from the Commission to the Council, Based on Article 12 of the Council Framework Decision of 24 February 2005 on attacks against information systems, 17 June 2008, not published in the O.J., p. 11 (COM (2008) 448 final)

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 legislation¹⁹⁴.

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 harmonisation¹⁹⁵.

The lack of harmonisation affects cooperation between national law enforcement authorities, which benefits from a harmonisation of crime definitions¹⁹⁶. 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.

¹⁹³ See [http://technet.microsoft.com/nl-nl/library/dd632948\(en-us\).aspx](http://technet.microsoft.com/nl-nl/library/dd632948(en-us).aspx)

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 cases¹⁹⁷. 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 cybercrime¹⁹⁸.

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 Decision¹⁹⁹. 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

¹⁹⁷ *Ibid.*, p. 6

¹⁹⁸ *Ibid.*, p. 7

¹⁹⁹ Report from the Commission to the Council, Based on Article 12 of the Council Framework Decision of 24 February 2005 on attacks against information systems, 17 June 2008, not published in the *O.J.*, (COM (2008) 448 final)

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.

