REGULATING SPAM

Directive 2002/58 and beyond

Foreword

This report is the result of a research project carried out at the Institute for Information Law between September 2003 and March 2004.

The Institute for Information Law (IViR) is part of the Faculty of Law of the University of Amsterdam. The Institute is the largest research facility in the field of information law in Europe. It employs over 25 qualified researchers who actively study and report on a wide range of subjects in the field of information law. The activities of the Institute include:

- research in the field of information law, initiated by the Institute or commissioned by third parties, including the European Commission, the WIPO and the Council of Europe;
- training of research assistants;
- organizing conferences and symposia;
- practical training (postgraduate courses, professional training, seminars);
- maintenance of a specialized library.

More information about IViR can be found at: www.ivir.nl

The idea of this research project followed from a round table conference organized by Solid Ground Public Relations in Haarlem, The Netherlands, in May, 2003. This study aims to present an evaluation of recent legislative initiatives against Unsolicited Commercial E-mail (spam) in the European Union. It provides an analysis of the meaning and interpretation of the new regulatory regime for unsolicited communications within the EU. As the scope of our research was limited in terms of time and scope of the research questions addressed, this report can only present a quick scan of the relevant regulations.

The report was prepared by

- Lodewijk F. Asscher PhD.

With contributions by

- Judith van Erve LLM.

The report was discussed and commented on in an expert panel consisting of

- Professor Egbert J. Dommering
- Assistant Professor Nico A.N.M. van Eijk
- Wilfred A.M. Steenbruggen LLM.

Miss Sabina Gorini has been kind enough to proofread the draft version of this report.

The project was supported by the European Forum for Electronic Business (EEMA) and European Digital Rights (EDRI). The research project was funded by Sybari Software Inc.

Sybari commissioned the IViR study on the Directive on Privacy and Electronic Communications upon realizing that most European citizens and organizations were having difficulties in interpreting the European Spam policy. Sybari is pleased

to participate in this project with the IViR, giving the needed guidance, in the European legal and corporate communities, to help further the fight against spam

Amsterdam, April 2004.

1 Regulating Spam

1.1 Introduction

This study analyses the legal framework regulating unsolicited commercial communications or spam in the European Union. Our focus is on the *Directive on privacy and electronic communications*[1] of 12 July 2002 (the E-Privacy Directive), as this directive has introduced new rules on the regulation of spam.

There are a number of reasons for carrying out this research project in this form and at this time. First of all, the economic impact of spam is rising and so is the awareness of spam's cost to society.[2] Secondly and not coincidentally, the attention of the legislator towards spam came to a peak during 2002-2003, with the EU adopting its E-Privacy Directive, with a transposition deadline of 31 October 2003, and the US adopting their CAN SPAM Act 2003.[3] It is therefore fair to say that spam is currently also very much on the political agenda as lawmakers realize that junk e-mail has become a huge cost factor for businesses and a significant nuisance to voters.

This study is addressed to several related parties. Businesses must be aware of the legal changes and should use this report to focus on the practical changes which will follow from the new legal environment. Consumers, on their part, should be aware of the real advantages of the new Directive but also of its inherent restrictions.

We present this study shortly after a number of relevant occasions. First of all, the deadline for the transposition of the E-Privacy Directive has passed, and the European Commission has announced infringement procedures against nine (now: eight) Member States for not implementing the Directive correctly within the prescribed deadline.[4] Secondly, the European Commission has presented a Communication on the regulation of spam in January 2004. And thirdly, the OECD has started a Spam Project to enhance international cooperation in this field, which was launched on 2-3 February 2004. As it is our objective that this study be of use in discussions surrounding the abovementioned occasions, a short term research project was chosen. This implies that we have had to restrict the research objectives and pose a limited research question. After shortly introducing our research focus we will account for what is left outside the scope of this study.

On a more general level, attempts to regulate spam pose questions that are very interesting for a number of reasons. First, the proliferation of spam in publicly available networks puts some communications law principles in a whole new light. For example, one of the classical ground rules used to be the obligation to transport all mail offered to the postal service provider indiscriminately.[5] The twin principle of communications secrecy and the obligation to carry for a common carrier have evolved into an almost dogmatic aspect of the relevant field of law. Now that most or all of the communication service providers consist of private

[1] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (E-Privacy Directive).
[2] See Communication 2004, p. 6-7.
[3] A bill to regulate interstate commerce by imposing limitations and penalties on the transmission of unsolicited commercial electronic mail via the Internet, S.877, 2003, zie voor de volledige wetsteksten www.spamlaws.com.
[4] Press Release European Commission, 5 December 2003, IP/03/1663; followed by a press release on 1 April, 2004, IP/04/435.
[5] See for example De Sola Pool 1983, chapter 5.

parties and now that their networks are overflowed with unsolicited e-mails, it is fair to take a new look at old principles. Also, as everybody concedes that the solution to spam is to be found in a combination of technology and law, the problem of how to cope with spam might shed light on the future development of the interaction between law and information technology. The fact that law and technology are intertwined and that law and information technology look at each other to provide answers is in a way symbolic of a lot of other problems of tech regulation.

Our main research objective is to assess the practical legal consequences of the new regulatory regime. The question we therefore have to answer is: What are the consequences of the new regulatory regime of unsolicited communications, as introduced in (Article 13 of) the new E-Privacy Directive?

Main research question:

How does the new regulatory regime change Spam law within the EU?

To answer that question we have to answer a number of sub-questions. First of all, we need to compare the new regime with the legal landscape before the E-Privacy Directive. This requires us to assess the other relevant European Directives as well as related initiatives. Secondly, if we want to be able to say something about the consequences that the Directive will have, we will need to find out what the Directive does *not* regulate. In other words, we will have to find the gray areas or weak spots in the new regulation. We will also take a look at the definitions used in the Directive.

What does it say about virus-spam? And how about SPIM? Are popup messages covered? And who is addressed by this new regime and who is protected by Article 13? Related but different is the question as to what margin of regulation is left to Member States. It is a question of EU law whether any room is left for national interpretation or national choices to be made in implementing new European legislation. Therefore we will have to map the space left for national choices. In order to make a valuable assessment of the new regime we will have to take a close look at the wording, exceptions and history of the main article of material law, Article 13. This implies an analysis of the meaning of Article 13's sections and their relation to other parts of the new regulatory framework. Article 13's relation with other sections of the E-Privacy Directive will subsequently be addressed. In order to evaluate the practical consequences, the next question we will have to answer is what new obligations the Directive has created for Member States, businesses and consumers and what consequences that has for liability issues. This should lead to a concise answer to our main research question and to a number of conclusions and recommendations.

Sub questions:

- How should spam be defined?
- What is the meaning of article 13 of the e-privacy directive?
- What is the meaning of other articles of the e-privacy directive?
- Is email address harvesting legal?
- What margin of appreciation is left to Member States?
- How is the new law enforced?
- What alternatives are there to article 13?

The question we strive to answer in this study touches several fields of law. Therefore this study cannot only focus on telecommunications law but also has to take into account some European constitutional law aspects. Also, in order to make a qualified assessment of the liabilities or obligations created we touch on aspects of civil law. Finally, regulating spam raises several fundamental rights issues. When we look at the harvesting of e-mail addresses by spammers, important questions of data protection law arise. Not only is spam regulated in a directive harmonizing *privacy* law, but prohibiting spam also has implications for freedom of *speech*[6],whereas ISP monitoring of e-mail traffic might mean restricting the right to *confidentiality* of communications. Apart from a legal problem, spam is very much a technical problem. We do point out the interaction between technical and legal solutions at some points throughout this report. Our focus however remains on the legal aspects of the regulation of spam.

Relevant fields of law:

Telecommunications Law
EU constitutional law
Fundamental rights law
Data protection law
Civil tort/liability law

We have chosen to leave several aspects of spam regulation out of our research plan. Importantly, we will not look into the law of individual Member States for a number of reasons. First of all, the law of most Member States implementing the Electronic Privacy Directive has not been fully adopted, is still in the process of being adopted or is still open to change. We already mentioned the announced infringement procedures by the Commission. Secondly, the EU is itself closely monitoring legislative initiatives in individual Member States and will report on that monitoring separately.[7]

Also, in this study we focus solely on EU law. Even though we recognize that for a practical solution to the spam problem international cooperation with third countries, especially with the US, is crucial, we restrict ourselves to an analysis of the European developments. However, in our concluding Chapter we cannot ignore the supra European dimensions of the spam phenomenon. Another *caveat* at this point is that we do not strive to present the full regulatory framework on the regulation of electronic communications in this study. We focus solely on the regulation of unsolicited communications which means that we do not pay attention to general questions of telecom regulation as for example the debate on the exact scope of a `Publicly available Network` or the future position of National Regulatory Authorities. This study does not strive to present an updated evaluation of the technological solutions to spam or a `how to` manual on preventing spam from entering the reader's mailbox. In our concluding Chapter we will pay attention to the complementing factors of technological solutions to spam and consumer awareness issues but the focus of this study remains on legal questions.

[6] On spamming and free speech, see inter alia Geisler 2001.
[7] See also 9th Implementation report

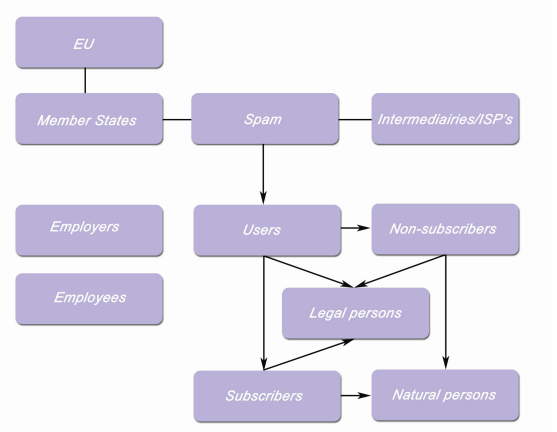
Outside the scope of our study:
- General Framework on electronic communications
- National implementations
- Technological aspects
- Economical Analysis
- How-to manual
- Third country aspects

The contents of this report are as follows. This first Chapter will introduce the spam problem and will take a look at current definitions of spam and the parties involved as well as past spam regulation. In Chapter 2, we will analyze Article 13 of the E-Privacy Directive. Chapter 3 deals spam and security, whereas Chapter 4 analyses the problem of email address harvesting. Chapter 5 covers issues of implementation and enforcement, followed by a Chapter on other aspects of the fight against spam. Chapter eight then contains our conclusions and recommendations.

In our final Chapter, an overall analysis of the consequences of the new regulatory regime is presented. Focus will be on practical legal consequences for consumers, businesses and governments. Recommendations will be presented as to where legal uncertainties should be cleared up and what the role of national governments can be in that process. Finally, in the annexed management summary a checklist of relevant legal questions to be used by businesses after implementation of the Directive is presented.

1.2 Spam: introducing the legal problem

The term spam, a trademark for canned ham by the firm Hormel, is said to be derived from a Monty Python sketch which took place in a restaurant, in which canned ham was present on the menu. Somewhere in the mid-1980's the word spam was posted repeatedly on Usenet, causing technical difficulties. Such postings became known as 'spamming'. Gradually, since the beginning of the 1990's, the term spam became commonly used to describe unwanted e-mail, often consisting of advertisements for products and services of a dubious nature.[8] Even though the term spam is associated with unsolicited e-mail, it could also be used to describe all unwanted messages such as voicemail, fax and possibly other media. Spam however is not an official notion as such.



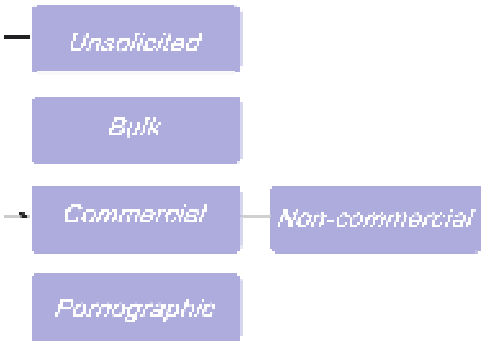
Spam affects many interested and interrelated parties. As a result, different viewpoints exist with respect to the problems relating to spam. These are the perspectives of users of communications services such as the internet, intermediaries and of course the State. Users can be divided into: subscribers and non-subscribers, natural and legal persons, recipients and spammers. Intermediaries can be internet service providers or network service providers, or both. Finally, the State has to implement the rules of this Directive. All of these

[8] Magee 2003, p.3.

parties have obligations, and obligations may imply liability. Another category consists of vendors, the corporations that hire spammers to exercise spam runs on their behalf. We will examine the possibilities to hold them liable as well.

1.3 Defining spam

The problem of spam can be viewed from different angles. First, spam poses an economic problem, shifting the burden of the cost of advertisement from the advertiser to the recipient as well as to the companies that are transporting the advertisement. From another point of view spam is also a human rights issue, with conflicting interests regarding freedom of speech and the right to privacy.



To put spam in a definition proves rather difficult. Various definitions of spam have surfaced over the years. The best known short definitions are Unsolicited Bulk E-mail (UBE) and Unsolicited Commercial E-mail (UCE), but also Unsolicited Commercial Bulk E-mail and just Unsolicited Electronic Mail have been used.[9] In its 2004 Communication the European Commission aptly notes that: "Spam" is a term more often used than defined. In short, it is commonly used to describe unsolicited, often bulk e-mails. […] … the concept of 'spam' is used in this Communication as a shortcut for unsolicited commercial electronic mail.'[10] Most definitions of spam contain the following elements: unsolicited, bulk, commercial. Two recurring combinations in the literature on spam are: UCE (unsolicited commercial e-mail) and UBE (unsolicited bulk e-mail). This invokes questions as: can non-commercial unsolicited e-mail be spam? Can a single e-mail be spam? The E-Privacy Directive does not give a definition of spam. The Directive refers to unsolicited communications for direct marketing purposes (recital 40). This report will not focus on finding the ultimate definition of spam either. However, the so-called utopian definition of spam springs to mind: 'All e-mails which are of no benefit to the recipient from the point of view of the recipient'.[11]

"Unsolicited" seems to be the keyword of any method to describe, to prevent and to fight spam. The elements 'bulk' and 'commercial' only gain meaning in relation to the unsolicited nature of the message. The use of bulk as a defining element seems to be blind to content relates to the problems caused by the massive amounts of spam being sent. That element poses the question of whether one single e-mail can be spam. To a particular user it does not matter if and how many others receive the same message. Also, a user does not want to have to find out

[9] Sorkin 2000, p. 328.
[10] Communication 2004, p. 5.
[11] Khong 2000, p.3.

whether other users have received the same message, before action can be taken. And how many people must receive a message before a spam run is considered to fulfill the notion of bulk? A fixed threshold would be circumvented by spammers and legitimize all spam runs beneath that level.[12] The lack of a definition of spam in the E-Privacy Directive points to an approach based on the principle of permission, not quantity, as Recital 40 of the E-Privacy Directive seems to imply.

Using the notion 'commercial' as a manner to distinguish spam from other unsolicited communications poses several problems. The E-Privacy Directive uses the notion 'direct marketing', a notion which contains other difficulties, as we will see in Chapter 4. What are the questions raised by the use of the notion 'commercial' as a distinguishing element?

First, different jurisdictions use different interpretations of the notion commercial. For instance, are semi-privatized 'public' services as education and health care, for which a fee is paid, commercial?[13] National legislation has to clarify what belongs in this category and what does not. Secondly, it is to be considered whether a political statement can also be considered a commercial message. A Dutch Court labeled a spam run on Members of Parliament as 'commercial' since the company behind the spam run had a financial interest in influencing the opinion of the Members of Parliament and their votes.[14] The latter criterion would render e-mails without a direct offer or advertorial content commercial. Thirdly, it is to be seen whether a request for a donation by a non-profit organization is to be considered a commercial message. In our opinion *non-profit* does not necessarily mean that a professional charity organization does not have any financial interests. Most professional non-profit organizations have a paid staff alongside volunteers. Employees have to be paid; therefore there is a "commercial" interest to stay in business.

There is a danger in trying to define spam by content, apart from the above mentioned risks of censorship and breach of confidentiality of communication. The burden of spam is not defined by the commercial nature of it per se. People can be annoyed by non-commercial messages just as well. And intermediaries suffer from the overload of spam, irrespective of content.[15]

A new and emerging problem is created by convergence of spam and computer viruses. In some cases, viruses seem to be used to distribute spam through the computer facilities of unknowing users, thus turning spam into a security threat in its own right.[16] This poses the question whether messages that are distributed by means of a virus fit the (or a) definition of spam. Those messages are unsolicited, sent in bulk and they might have a commercial element, for instance if the virus strikes out a competitive software system, or results in an attack of the website of a competitor (Denial of Service attack). And to reverse the question, whether spam can be a security risk is also relevant for the legal prohibition of sending out spam. Does a spammer have to act deliberately?[17] Is there a duty to make sure your machine is secure? It is also important to know whether a user that does not use firewall or anti-virus software can as a result of this be held liable for spam runs sent from his computer (without his knowledge). New developments in which spam and viruses will grow into new shapes of nuisance will necessarily result in new legal questions. At this point it suffices to conclude that in this study we will

[12] Sorkin 2000, p. 333.
[13] Khong 2000, p. 2.
[14] Staat vs Rath, Court Almelo, 13 september 2000, *Mediaforum* 2002-11/12, p.366-370, with a comment by Catrien Noorda.
[15] Bergfeld & Lodder 2002, p. 1051-1052.
[16] E.g. the 1999 Melissa virus; Sorkin 2002, p. 336.
[17] Bergfeld & Lodder 2002, p. 1051-1052.

follow the approach taken by the E-Privacy Directive on what is spam, i.e. we will use "unsolicited communications for direct marketing purposes" as our general definition.

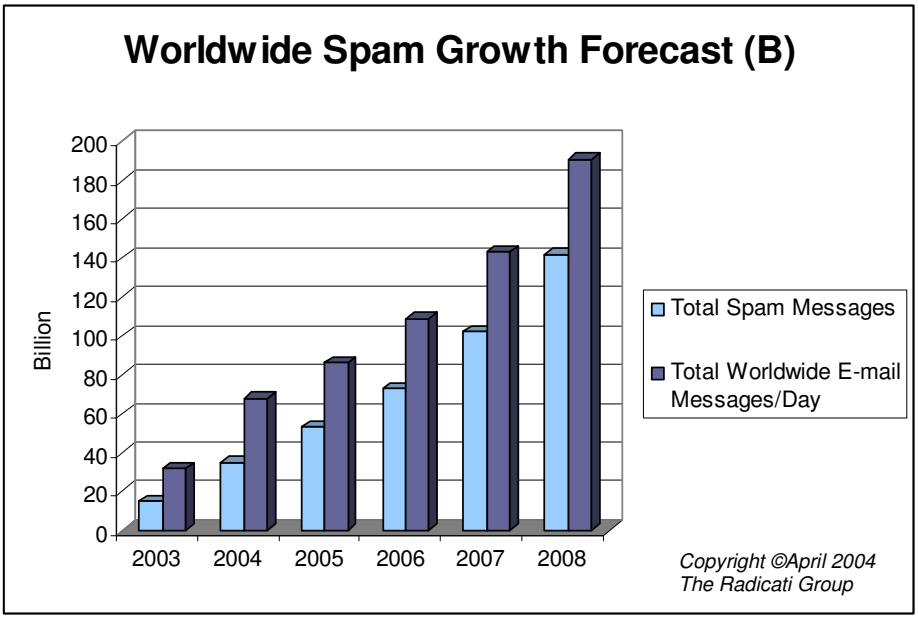
1.4 Spam: the economics

If one looks at the economic consequences of spam, it is obvious that spam is a very cheap medium for marketing all kinds of goods and services.[18] Telemarketing in general has become increasingly popular as a direct marketing strategy. Direct marketing is an important tool to approach customers. E-mail may well be the cheapest vehicle for direct marketing; costs do not vary according to distance and repeated e-mails have very low additional costs. The more e-mails a spammer can send, the greater the profit, while costs remain nearly constant.[19] In sum, e-mail marketing can be very cheap. That is, cheap for the advertiser. The cost of sending out one million e-mails is minimal compared to the cost of obtaining a comparable level of exposure through paper advertisements or television commercials. The main reason for this imbalance is that part of the costs is imposed on other parties, namely the transporting intermediaries and the recipients. This is called cost-shifting.

Users of communication services have to pay to download the advertisement to their mailboxes, either through dial-up time or through an all-in package, the size of which has to be increased with the amount of e-mail and consequently the amount of bits the user receives. Apart from these costs, every minute spent on deleting spam is a waste of time, and therefore money. The intermediaries transporting the message also pay for the cost of spam. They need to increase their bandwidth and server storage capacity to keep up with the increase of e-mail traffic. These costs are eventually compensated by higher fees for their services. The recipients are therefore paying more for their access subscription.[20] Free e-mail services might disappear.[21] The internet gets more expensive for its users, and therefore becomes a less accessible medium than it originally was.

Finally, apart from recipients and intermediaries who directly pay the costs of spam, another paying party is comprised of bona fide companies that do not send unsolicited e-mails.[22] Their solicited messages disappear into the enormous amount of unsolicited advertisements. Their image as an advertiser is compromised by advertisements which are annoying recipients through costs and content. The use of illegal spam runs by some companies as a means to advertise their products or service gives them an unfair competitive advantage. Getting rid of spam would be of benefit to the so-called permission marketers. An opt-in regime would add to the promotion of European e-commerce.[23] In recent years, spam has reached worrying numbers. Despite variations in statistics, it is generally estimated that more than 50 percent of global e-mail traffic is 'spam'.

[18] Gauthronet & Drouard 2001, p. 2.
[19] OECD 2004.
[20] Sorkin 2000, p. 336-337.
[21] Magee 2003, p. 4.
[22] Schaub 2002, p.3.
As was the point of view of several committees during the discussion of the proposal of the E-Privacy Directive, see: Magee 2003, p.17.



Cleaning up mailboxes to remove spam is both time consuming for the user and increasing users' costs when filtering and other software facilities are needed.[24] Furthermore, spam creates considerable costs for businesses.

Spam can also prompt liability for the entity receiving it. A company, for instance, could be held liable for failing to take steps to prevent the creation of a hostile work environment in case an employee receives unsolicited pornographic e-mail. But also 'false positives' – blacklisting the wrong e-mail – can create considerable damage.

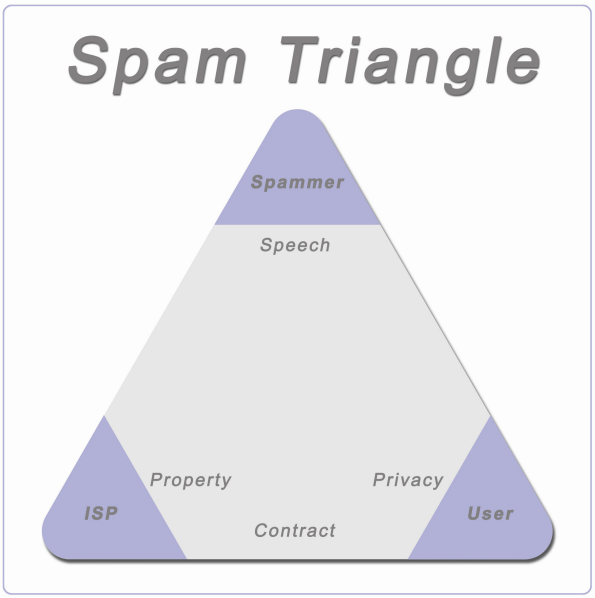
The European Commission has stated that it is very difficult to calculate the total cost of spam. Nevertheless, it is clear that the total damage is a multi-billion Euro matter. Apart from that, the Commission is also and rightfully worried about the consequences of spam for consumer confidence.[25]

1.5 Spam and fundamental rights

Spam is also a fundamental rights problem. From the viewpoint of individuals, spam can be deemed an invasion of privacy. From the viewpoint of a spammer, quite often freedom of speech is involved. The most important fundamental rights involved in regulating spam are therefore freedom of expression and privacy. These fundamental rights apply to recipients as well as spammers and their clients. The fundamental rights in question are relevant with respect to state legislation and enforcement thereof, i.e. the vertical application of fundamental rights. Fundamental rights can also have effect between private parties; this is called the horizontal application of fundamental rights. This may be the case with regard to the relation between recipients and spammers and their clients, but also between recipients and spammers on one side and intermediaries that filter e-mail

[24] Communication 2004, p. 6-7. Do people care? Perhaps, the number of complaints is an indication. According to the 2004 Communication, the French SpamBox had attracted 325.000 messages in three months. A similar experience in Belgium led to 50.000 complaints in 2.5 months. Communication 2004, p. 7.
[25] Communication 2004, p. 8.

on the other. The fundamental rights issues with regard to spam because of the triangular relation between user, spammer and ISP.



The "Spam Rights Triangle: the spammer will claim he is using his right to freedom of expression. The user sees his privacy interfered with. Both relational privacy in terms of filling his mailbox without his consent and informational privacy because his email address is being used and processed without his consent. The provider has a contractual relationship with both the spammer and the user and can under certain circumstances claim property rights in his network. On the other hand, the user may have a contractual claim against the provider to get his e-mail without spam. Therefore, a number of rights collisions are part of the spam problem.

The right to freedom of expression is *inter alia* protected by Article 10 of the European Convention on Human Rights (ECHR).[26] The right to freedom of expression is not restricted to individuals. In principle, legal persons enjoy freedom of expression too. Apart from corporations, also charity organizations and political parties make use of direct e-marketing. Political statements are more strongly protected under the flag of freedom of expression than commercial messages. As the European Commission of Human Rights put it in the Scientology case:

'Although the Commission is not of the opinion that commercial "speech" as such is outside the protection conferred by Article 10(1), it considers that the level of protection must be less than that accorded to the expression of "political" ideas, in the broadest sense, with which the values underpinning the concept of freedom of expression in the Convention chiefly are concerned.'[27]

Businesses have the right to market their products through advertisements. They enjoy freedom of expression. The European Court of Human Rights has

[26] European Convention on Human Rights, Rome, 4 November 1950. *Text completed by Protocol No. 2 (ETS No. 44) of 6 May 1963 and amended by Protocol No. 3 (ETS No. 45) of 6 May 1963, Protocol No. 5 (ETS No. 55) of 20 January 1966 and Protocol No. 8 (ETS No. 118) of 19 March 1985.*
[27] *Yearbook of the European Convention of Human Rights*, 1979, p. 252.

acknowledged this in several cases over the past 25 years.[28] As a consequence, the test of Article 10(2) is available and obligatory for the assessment of the admissibility of national restrictions on commercial advertising. This test provides for legal examination of the clarity and the accessibility of the relevant limitation; the legitimacy of its aims and the important question of whether the limitation or prohibition is necessary in a democratic society, i.e., an examination of whether the national rule is appropriate and proportionate to its aim. However, the European Court of Human Rights applies a broad margin of appreciation when assessing the admissibility of national content-restrictions on commercial advertising.[29] This means that national authorities have a rather great freedom in their policy with regard to restrictions on the content of advertising.[30] The right to freedom of expression can therefore be restricted with regard to content, e.g. to protect the public in moral and health issues. Spam containing pornographic images can be perceived as offensive.[31] Spam promoting Viagra without warning of the possible consequences for heart patients can for example be seen as a health hazard.[32] The right to freedom of expression can also be restricted to protect the rights of others, such as the right to privacy.

The right to privacy, as protected by Article 8 ECHR, can conceptually be divided in informational privacy, privacy of communications and relational privacy. [33] In short, informational privacy is the individual's right to decide which personal data can be communicated to others. In Chapter 6, we will discuss whether electronic mail addresses can be considered personal data. Processing of such data, which includes the collection, storage or use of electronic addresses could intrude on this informational privacy right. Privacy of communications or confidentiality of communications can be relevant with regard to filtering of e-mail.

Relational privacy includes the right to determine which communications one wishes to receive or not.[34] Freedom of expression and the right to be left alone can obviously conflict. The spam issue therefore reflects a conflict between freedom of expression and the right to privacy. The State has to balance both interests in the process of drawing up national legislation.

The clash between the freedom of expression of the spammer and the right to privacy of the person who does not want to receive spam is evident. Service providers who have to service both groups of users are caught in the middle. They themselves suffer from an overload of spam which requires expansion of capacity of both technical assets and human resources. To target outbound spam, service providers include anti-spam provisions in their standard license agreements and close down accounts if their anti-spam policy is ignored. These procedures should be applied carefully because they could themselves encroach upon freedom of expression.

[28] *X and Church of Scientology v. Sweden*, Appn. No. 7805/77, Decision on admissibility by the European Commission of Human Rights of 5 May 1979, DR 16, p. 68; *Jacubowski v. Germany*, Judgment of the European Court of Human Rights of 23 June 1994, Series A, No. 219; *Casado Coca v. Spain*, Judgment of the European Court of Human Rights of 24 February 1994, Series A, No. 285; *Markt Intern Verlag GmbH & Klaus Beermann v. Germany*, Judgment of the European Court of Human Rights of 20 November 1989, Series A, No. 165; *Hempfing v. Germany*, Appn. No. 14622/89, Decision on admissibility by the European Commission of Human Rights of 7 March 1991, DR 69, p. 272; *Barthold v. Germany*, Judgment of the European Court of Human Rights of 25 March 1985, Series A, No. 90; *Stambuk v. Germany*, 24) Judgment of the European Court of Human Rights of 17 October 2002.
[29] Compare on the 'right to antenna', (*Verein gegen Tiergabriken v Switzerland)*, Judgment of the European Court of Human Rights of 28 June 2001, *Reports of judgments* 2001-VI.
[30] Kabel 2003b, p. 4-5.
[31] Sorkin 2001, p. 336.
[32] See Kabel 2000, p. 9 on prescription of drugs and medical advice on the internet.
[33] Kabel 2003a, p.6.
[34] Kabel 2003a, p.6.

To prevent spam from entering their mail servers (and sometimes even from leaving them) service providers use filtering. Filtering can also infringe on fundamental rights such as freedom of expression and privacy. Use of filters and blocking of servers can restrict people's ability to communicate and therefore be an impairment of freedom of speech. This applies to spammers as well as to people who would actually like to receive spam, be it for pleasure or business. Blocking all spam by technical means without the e-mail user's consent could therefore intrude on the right to receive (and send) information, including spam messages. Filtering can also result in the blocking of legitimate information, the so-called false positive. This can be an infringement on the right to freedom of expression, even of persons who do not spam at all.

The E-Privacy Directive strikes a balance between freedom of speech and the right to privacy and property rights. This point of view is reflected by Recital 40 of the E-Privacy Directive which mentions both the invasion of privacy and the cost-shifting argument, in relation to receiving and transmitting parties, as a ground to impose an opt-in regime.

Recital 40 E-Privacy Directive

Safeguards should be provided for subscribers against intrusion of their privacy by unsolicited communications for direct marketing purposes in particular by means of automated calling machines, faxes, and e-mails, including SMS messages. These forms of unsolicited commercial communications may on the one hand be relatively easy and cheap to send and on the other may impose a burden and/or cost on the recipient. Moreover, in some cases their volume may also cause difficulties for electronic communications networks and terminal equipment. For such forms of unsolicited communications for direct marketing, it is justified to require that prior explicit consent of the recipients is obtained before such communications are addressed to them. The single market requires a harmonized approach to ensure simple, Community-wide rules for businesses and users.

1.6 Old legal framework

Now that we have discussed how spam is defined, we will take a look at the regulation of spam before the E-Privacy Directive. In this section, European Directives which address(ed) unsolicited communications are presented in chronological order. They show the enigmatic history of European regulation of unsolicited communications. The new framework for electronic communications and the E-Privacy Directive will be discussed later on.

1.6.1 Data Protection Directive

The 1995 Data Protection Directive[35] provides general rules for the processing of personal data. Personal data are data which allow for identification of an individual. The Data Protection Directive does not target spam in particular. However, e-mail addresses can be personal data.[36]

[35] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data *OJ* 1995 L 281/31-50.
[36] Schaub 2002, p.4.

The Article 29 Working Party, the advisory committee of European Data Protection Authorities, declared in 2000 the harvesting of e-mail addresses on the internet as amounting to unlawful processing of personal data according to the rules of the Data Protection Directive.[37] According to Recital 10 and Article 1(2) of the E-Privacy Directive, the general regime on data processing of the Data Protection Directive applies alongside the special regime on electronic communications of the E-Privacy Directive. In Chapter 4 we will explain which electronic addresses can be classified as personal data and which rules of both Directives therefore apply.

1.6.2 Distance Selling Directive

The 1997 Distance Selling Directive[38] is the first Directive to protect consumers from unsolicited communications. The Directive requires prior consent of the consumer for the use of automated calling systems without human intervention (automatic calling machine) and fax as a means of distance communication for the conclusion of a contract between consumer and supplier (Article 10 (1)). According to Article 10(2), other means of distance communication which allow individual communications, may be used only where there is no clear objection from the consumer. The first provision refers to an opt-in regime for automatic calling machines and faxes. The technology neutral formula of the second provision seems to imply an opt-out regime for other unsolicited communications, including unsolicited e-mail.[39]

1.6.3 Telecommunications Privacy Directive (ISDN Directive)

The 1997 ISDN Directive[40] contained provisions on unsolicited calls. Article 12 prescribed an opt-in regime for the use for purposes of direct marketing of automated calling machines without human intervention, including fax machines (provision 1). Unsolicited calls for purposes of direct marketing by other means could be governed by either an opt-in or an opt-out regime, depending on the choice of individual Member States (provision 2). Some countries interpreted e-mail as falling into the category of 'calls by other means'.[41] The Article 29 Working Party is of the opinion that:

"the telecommunication legal framework should apply to Internet services in the same way as it applies to other forms of communication…processing of personal data on the Internet has to respect data protection principles just as in the off-line world. Personal data processing on the Internet therefore has to be considered in the light of both data protection directives."[42]

The European Commission subsequently issued a proposal for a new Directive. The Telecommunications Privacy Directive has now been replaced by the E-Privacy Directive.

[37] Art. 29 Working Party: Privacy on the Internet - An integrated EU Approach to On-line Data Protection- Working Document, Adopted on 21st November 2000, 5063/00/EN/FINAL WP 37.
[38] 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.
[39] Schaub 2002, p.5.
[40] Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector (incl. Annex) *OJ* 1998 L 24/1-8.
[41] Magee 2003, p.20.
[42] Article 29 Working Party: Opinion 2/2000 concerning the general review of the telecommunications legal framework, Adopted on 3rd February 2000, 5009/00/EN/FINAL, p. 3. Documents of the working party can be found on <http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/index.htm

1.6.4 E-Commerce Directive

The 2000 Directive on electronic commerce (E-Commerce Directive)[43] is the first Directive to explicitly mention electronic mail as an example of unsolicited communication:

"The sending of unsolicited commercial communications by electronic mail may be undesirable for consumers and information society service providers and may disrupt the smooth functioning of interactive networks; the question of consent by recipient of certain forms of unsolicited commercial communications is not addressed by this Directive, but has already been addressed, in particular, by Directive 97/7/EC and by Directive 97/66/EC; in Member States which authorise unsolicited commercial communications by electronic mail, the setting up of appropriate industry filtering initiatives should be encouraged and facilitated; in addition it is necessary that in any event unsolicited commercial communities are clearly identifiable as such in order to improve transparency and to facilitate the functioning of such industry initiatives; unsolicited commercial communications by electronic mail should not result in additional communication costs for the recipient."

The Directive also contains specific provisions to protect users from unsolicited commercial communications by electronic mail. Article 7(1) states that when commercial communications are permitted by Member States, these communications shall be identifiable clearly and unambiguously upon receipt of the message. This means that the header of the message must contain a label like 'ADV' (advertisement) so the receiving party does not have to open the mail to be aware of its commercial content. Article 7(2) imposes an obligation to consult and respect opt-out registers regarding unsolicited commercial communications by electronic mail.
This has been interpreted as the Directive leaving Member States the choice between opt-in and opt-out regimes, although Recital 30 of the E-Commerce Directive specifically states that the question of consent is not addressed by this Directive.[44]

During the preparation of the E-Privacy Directive opinions were put forward against regulating spam in a separate Directive with an opt-in regime because Article 7 of the E-Commerce Directive and the General Data Protection Directive would already make regulation of electronic mail by Member States possible. Arguments were: regulatory inefficiency, penalizing responsible marketers and hindering the development of e-commerce within the EU, reducing the impetus for business to develop effective software solutions.[45] However, with regard to the single market approach the existence of different regimes within the EU was considered as counterproductive and therefore the harmonization of spam regulation was aimed for, although not throughout the whole spam spectrum, as we will see in Chapter 4.

The labeling requirements of Article 7(1) of the E-Commerce Directive will apply next to the requirements of the E-Privacy Directive. For non-harmonized situations

[43] Directive 2000/31/EC of the European Parliament and of the Council COUNCIL of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') *OJ* L 178/1.
[44] Schaub 2002, p.6.
[45] Committee on Citizens' Freedoms and Rights, Justice and Home Affairs, Rapporteur: Marco Cappato.
Report on the proposal for a European Parliament and Council directive concerning the processing of personal data and the protection of privacy in the electronic communications sector, 13 July 2001, FINAL A5-0270/2001
(COM(2000) 385), p.18, 30-31.

in which Member States will choose the opt-out regime, Article 7(2) on opt-out registers applies as well.

The E-Commerce Directive uses the notion 'commercial communications' as defined in Article 2(f) of the E-Commerce Directive. That notion does not have the same meaning as the notion 'direct marketing' which is used in the E-Privacy Directive. This is rather confusing since the two Directives are both applicable to different kinds of unsolicited electronic mail.

1.7 Conclusions

In this Chapter we have introduced our main research questions and the main objectives of this study. We have seen that it is hard to come to a universal agreement on what is spam. We have established that spam must be seen from both an economic point of view and from a human rights point of view. We have noted the cross-over between spam and viruses. If spam is so hard to define, it will be also difficult to regulate it on a detailed level. Recital 40 of the E-Privacy Directive points to an approach to spam based on quality and the principle of permission, and not on quantity, which would use the notion of 'bulk' as a defining factor.

We have also described the complex relation between some fundamental rights and spam. We have introduced the spam triangle in order to describe the different roles and perspectives of the Internet Service Providers, the spammers and the end users. Different reasons to object to spam have a distinct legal translation. The regulation of spam is itself a multi-layered multi-focus project.

Since the E-Privacy Directive does not give a closed definition of spam it is up to the Member States, and eventually to the courts, to decide what exactly is spam in the spirit of the E-Privacy Directive and what is not. There have been a number of Directives that addressed the problem of unsolicited communications. The most explicit is the E-Commerce Directive. This is the first Directive to explicitly mention electronic mail, and to contain provisions on unsolicited commercial communications by electronic mail. The labeling requirements stated in Article 7(1) will operate in complement to the requirements of the E-Privacy Directive. In non-harmonized situations Article 7(2) might also apply. Since not all Member States have already implemented the Directives described in this Chapter, the implementation of the E-Privacy Directive will provide them with a chance to catch up with the regulation of unsolicited communications. However, already before the E-Commerce Directive, the ISDN Privacy Directive introduced an opt-in regime for some forms of unsolicited communications.

2 Article 13

2.1 The new framework

In this Chapter, we will assess the meaning of Article 13 of the E-Privacy Directive. We will be answering sub-questions 2 and 3 as presented in the first Chapter, i.e. What is the scope of Article 13 in terms of object, subject and addressee and what are the weak spots or gray areas that this article creates.

First, we must describe the background to the E-Privacy Directive in order to present the context of the present regulatory regime. After the European IT summit in Lisbon, the Commission proposed a package of measures for a new regulatory framework for electronic communications. This package followed partly from the 1999 Review of the electronic communications sector. The new regulatory framework altered the discourse from classical telecommunications to electronic communications. The e-communications framework is comprised of a general framework directive and four specific directives.[46] In its proposal for a common regulatory framework for electronic communications networks and services, the European Commission stated:

> "The existing [now former] legislative framework was primarily designed to manage the transition from monopoly to competition and was therefore focused on the creation of a competitive market and the rights of new entrants. It has been successful in achieving those aims. But in part because of the success of liberalization at European level, the market is now changing with ever-increasing speed. This was foreseen by the current legislative framework, which required the Commission to review the operation of the Directives making up the regulatory framework in the light of developments in the market, the evolution in technology and the changes in user demand. The new policy framework needs to take account of these developments, in particular the convergence between telecommunications, broadcasting and IT sectors. It seeks to reinforce competition in all market segments, while ensuring that the basic rights of consumers continue to be protected. It is therefore designed to cater for new, dynamic and largely unpredictable markets with many more players than today." 47

According to the Communication, the proposed Directive aims to establish a harmonised regulatory framework for electronic communications networks and services across the EU.

With regard to privacy and data protection in the communications sector, the Commission noted in its Communication following the 1999 Communications Review and Orientations for the new Regulatory Framework: 'the support in the consultation for updating the telecom data protection directive, will introduce proposals to ensure that data protection rules in the communications sector are technologically neutral and robust. In this context, it will examine in particular

[46] Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive), *OJ* L 108/33 (24.04.2002).Besides the E-Privacy Directive, the other three specific directives are: Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorisation of electronic communications networks and services (Authorisation Directive), Directive 2002/19/EC of the European Parliament and of the Council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive), Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive).

[47] Proposal for a common regulatory framework for electronic communications networks and services, COM(2000) 393 final 2000/0184 (COD) (presented by the Commission) p.3-4.

existing terms and definitions of the Directive and the consistency of coverage of old and new telecommunications services with new functionalities embedded in networks or software"[48]

A proposal for a Directive concerning the processing of personal data and the protection of privacy in the electronic communications sector was subsequently issued.

The e-communications framework was due for implementation on July 25th 2003. The E-Privacy Directive was adopted a few months later and did not have to be implemented until October 31st 2003. The Framework Directive is *inter alia* relevant for this study as it defines a number of important concepts that are used in the E-Privacy Directive. Article 2 of the E-Privacy Directive refers to the Framework Directive as a general set of definitions. A monitoring report of the E-Privacy Directive by the Commission is due before 2006.

2.2 E-Privacy Directive

Article 1 Scope and aim

1. This Directive harmonizes the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community.
2. The provisions of this Directive particularize and complement Directive 95/46/EC for the purposes mentioned in paragraph 1. Moreover, they provide for protection of the legitimate interests of subscribers who are legal persons.
3. This Directive shall not apply to activities which fall outside the scope of the Treaty establishing the European Community, such as those covered by Titles V and VI of the Treaty on European Union, and in any case to activities concerning public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law.

The E-Privacy Directive replaced the Telecommunications Privacy Directive with regard to regulation of privacy within the telecommunication sector. The European Commission stated in its initial proposal: 'The Directive is one element in a new regulatory framework which seeks to ensure that the electronic communications sector continues to develop as a competitive market delivering benefits to all companies and individuals in the Community that use electronic communications services. The aim is to cover all electronic communications services in a technology neutral fashion. A harmonised level of data protection in the electronic communications sector is an essential element for the functioning of the internal market in electronic communications services and networks.'[49]

The basis for the E-Privacy Directive was provided by Article 95 of the Treaty establishing the European Community: measures relating to the establishment and

[48] Communication of the European Commision, The results of the public consultation on the 1999 Communications Review and Orientations for the new Regulatory Framework, COM(2000)239 final,p. 26. Available at: http://europa.eu.int/ISPO/infosoc/telecompolicy/en/com2000-239en.pdf.

[49] Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector /* COM/2000/0385 final - COD 2000/0189 */ *Official Journal C 365 E , 19/12/2000 P. 0223 – 022* (under: Impact Assessment).

functioning of the internal market. In order to improve the functioning of the internal market, the Member States of the European Union decided to harmonize privacy law on a European level and therefore to give up part of their autonomy. However, since privacy is a very sensitive topic among the Member States, the E-Privacy Directive, as the outcome of difficult negotiations among Member States, is a complex political compromise. Apart from that, a minimum level of harmonization was aimed for. Member States are indeed allowed to impose a stronger regime of protection, leaving Member States a lot of room to maintain their own national standards while implementing the Directive. In the process of that implementation, Member States interpret the Directive and transpose that interpretation into national legislation. To facilitate this interpretation the European Commission can put forward guidelines for implementation (as this kind of regulation is largely non-binding it is also called soft-law). The Communication on unsolicited communications or 'spam' of January 2004 is an example of the latter.[50] Ultimately, the European Court of Justice has the final say regarding the meaning of the Directive.

The E-Privacy Directive contains provisions on a number of issues such as security of networks and services, confidentiality of communications, cookies, data retention, calling line identification, public subscriber directories and unsolicited communications. We must focus on Article 13 which regulates unsolicited communications but we will also discuss some other provisions related to the spam problem.

2.3 Article 13

The general rule on unsolicited e-mail has been laid down in Article 13 of the E-Privacy Directive. Article 13 is the result of a fierce battle of interests within and between the European Parliament and the Commission.

> Article 13(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.

2.4 Scope I: Electronic communications

Unsolicited communication as a term reflects more than just e-mail. Unsolicited voicemail messages, faxes, sms, unexpected pop-ups on computers and television commercials can also be perceived as spam. Article 13(1) mentions the following types of electronic communication: automatic calling machines, faxes and electronic mail. Article 13(2) and Article 13(4) refer to electronic mail. Article 13(3) and 13(5) refer to the notion of 'communications'. In order to be able to assess what rules apply to what type of communication we need to assess which types of electronic communications fall within the scope of Article 13 of the E-Privacy Directive.

[50] Communication from the commission to the European parliament, the council, the European economic and social committee and the committee of the regions on unsolicited commercial communications or 'spam', 22 january 2004, COM (2004) 28.

Article 13(1) of the E-Privacy Directive lists automatic calling machines, fax machines and electronic mail as types of electronic communication to which the opt-in regime of the E-Privacy Directive applies. As a result of the Directives that preceded the E-Privacy Directive (see 2. 1) automatic voicemail messages and junk faxes no longer pose huge problems. This Section will therefore focus on the question of which other types of electronic communication fall within the scope of the E-Privacy Directive. We will therefore look at the meaning of the notions of 'communication' and 'electronic mail' for the purposes of the E-Privacy Directive. We will start with the more general notion 'communication' of which electronic mail is a specific category.

Article 13 does not refer to the general notion 'electronic communication', but uses the notion 'communication'. Article 2(d) of the E-Privacy Directive defines 'communication' for the purpose of the E-Privacy Directive as

"Any information exchanged or conveyed between a finite numbers of parties by means of a publicly available electronic communications service. This does not include any "Any information exchanged or conveyed between a finite numbers of parties by means of a publicly available electronic communications service. This does not include any information conveyed as part of a broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the identifiable subscriber or user receiving the information".

Recital 16 of the E-Privacy Directive adds to this:

"Information that is part of a broadcasting service provided over a public communications network is intended for a potentially unlimited audience and does not constitute a communication in the sense of this Directive. However, in cases where the individual subscriber or user receiving such information can be identified, for example with video-on-demand services, the information conveyed is covered within the meaning of a communication for the purposes of this Directive".

The exclusion of information which is part of a broadcasting service and aimed at a potentially unlimited audience, unless the recipient can be identified, makes the difference between the notion of 'communication' in the E-Privacy Directive and the meaning of the general notion of 'electronic communications', which can be derived from the definitions within the Framework Directive of 'electronic communications network'[51] and 'electronic communications service',[52] which both include broadcasting. The phrase 'a finite number of parties' in the definition of 'communication' in the E-Privacy Directive seems to aim at point-to-point

[51] Article 2 (a) Framework Directive " electronic communications network " means transmission systems and, where applicable, switching or routing equipment and other resources which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed.

[52] Article 2 (c) Framework Directive "electronic communications service" means a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services; it does not include information society services, as defined in Article 1 of Directive 98/34/EC, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks

communication. For this kind of communication an address is required, both to send and receive the communication.

A specific category of communication is electronic mail. According to Article 2(h) of the E-Privacy Directive 'electronic mail' means:

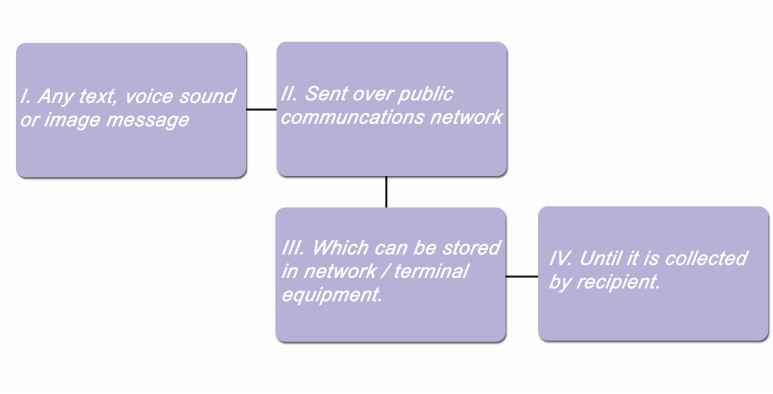
> "Any text, voice sound or image message sent over a public communications network which can be stored in the network or on the recipient's terminal equipment until it is collected by the recipient."

To find out what types of electronic communication are included within the notion 'electronic mail' we turn to the preparation of the E-Privacy Directive.

The original version of Article 2(h) contained the phrase "which is addressed directly or indirectly to one or more natural or legal persons" [53], instead of "until it is collected by the recipient". By contrast, an earlier version of Article 13(1) stated:

> "The use of automated calling systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail and other personally addressed electronic communications for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent."

The justification for the addition of the phrase "other personally addressed electronic communications" is the following: "With the huge expansion of mobile Internet products, services such as SMS are already being abused by direct marketers. Europe has been the world leader in mobile telephony. To allow direct marketers to abuse the service would be to reduce its attractiveness to European consumers. For the interests of the protection of personal data and the growth of electronic and mobile commerce, there is an overwhelming case in favor of a ban on unsolicited e-mail and other personally addressed messages in the EU."[54] Nonetheless, the addition "and other personally addressed electronic communications" has been removed.



Discussing the exclusion of electronic mail from the opt-in regime of Article 13(1), and the inclusion of SMS, the Council stated: "with protection of the subscriber

[53] Committee on Citizens' Freedoms and Rights, Justice and Home Affairs, Rapporteur: Marco Cappato. Report on the proposal for a European Parliament and Council directive concerning the processing of personal data and the protection of privacy in the electronic communications sector, 13 July 2001, FINAL A5-0270/2001 (COM(2000) 385), p.58.
[54] Committee on Citizens' Freedoms and Rights, Justice and Home Affairs, Rapporteur: Marco Cappato. Report on the proposal for a European Parliament and Council directive concerning the processing of personal data and the protection of privacy in the electronic communications sector, 13 July 2001, FINAL A5-0270/2001 (COM(2000) 385), p.71.

and of technological neutrality in mind, the Council thought that the subscriber consent arrangements should embrace *every use of electronic mail* for the purposes of direct marketing purposes, and not just SMS." The Commission commented on this by stating: "EP amendment 35 proposed to only single out SMS messages and include them in paragraph 1 of this article requiring prior consent of recipients while leaving the approach to *other forms of e-mail* for the Member States to decide. The Council preferred a harmonised approach on the basis of prior consent for *all forms of electronic mail*."[55]

The preparation of the E-Privacy Directive showed two other interesting points. First, electronic mail seems to have been characterized as a personally addressed message. Second, the use of the notion 'electronic mail' has been rather inconsistent throughout the preparation of the Directive.

Another possible point of critique is that Article 13 on unsolicited communications, and the concepts related thereto, such as 'direct marketing' and 'communication', are connected to content. This is in itself inconsistent with the Framework which is supposed to regulate transmission, not the transmitted message, in a technology neutral fashion, as the Commission stated in its proposal for the Framework Directive:

> "The proposed Directive is part of a package of five Directives and one Decision intended to reform the existing regulatory framework for electronic communications services and networks in the Community. One of the aims of this overall reform is to create rules which are technology neutral. The legal framework must try to ensure that services are regulated in an equivalent manner, irrespective of the technological means by which they are delivered. This also implies that consumers and users should get the same level of protection regardless of the technology used by particular service. Maintaining a high level of data protection and privacy for citizens is one of the declared aims of the current review".56

According to Article 2(h) of the E-Privacy Directive electronic mail means "any text, voice sound or image message sent over a public communications network which can be stored in the network or on the recipient's terminal equipment until it is collected by the recipient."

Since Article 13 of the E-Privacy Directive specifically refers to electronic mail, there is no doubt that the Directive applies to e-mail. E-mail can contain different kinds of information, "any text, voice sound or image message" . Also, e-mail is sent over the internet which is a public communications network as defined in Article 2(d) of the Framework Directive.[57] Finally, "which can be stored in the

[55] Communication from the Commission to the European Parliament pursuant to the second subparagraph of Article 251 (2) of the EC Treaty concerning the common position of the Council on the adoption of a Directive of the European Parliament and of the Council on processing of personal data and the protection of privacy in the electronic communications sector /* SEC/2002/0124 final - COD 2000/0189 */, p. 1-2; p. 17.

[56] Communication from the Commission to the European Parliament pursuant to the second subparagraph of Article 251 (2) of the EC Treaty concerning the common position of the Council on the adoption of a Directive of the European Parliament and of the Council on processing of personal data and the protection of privacy in the electronic communications sector /* SEC/2002/0124 final - COD 2000/0189 */, p. 1-2.

[57] Article 2(d) of the Framework Directive "public communications network" means an electronic communications network used wholly or mainly for the provision of publicly available electronic communications services". The definition of Article 2 (a) on "electronic communications network"
specifically mentions internet as a network: "electronic communications network" means transmission systems and, where applicable, switching or routing equipment and other resources which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed;

network or on the recipient's terminal equipment": anything can in principle be stored on terminal equipment, provided it has the appropriate functionality. "Until it is collected by the recipient": before an e-mail user pulls e-mail messages into the inbox of an e-mail program on his computer, the e-mail is stored on the mail-server. It is possible to leave e-mail on the server to be able to use it as an archive when working with web mail or to retrieve e-mail from the server at different locations, e.g. at home and at work.

Short Message Service ('SMS'), addressed to a mobile phone number, is a specific type of electronic communication. Recital 15 states that "a communication may include any naming, numbering or addressing information provided by the sender of a communication or the user of a connection to carry out the communication'. Recital 40 explicitly mentions SMS as a subcategory of e-mail. SMS fits the criteria as well and falls within the definition of 'electronic mail'.

SMS is delivered directly to the telephone of individual users, which are identified by their unique numbers. SMS qualifies as an instrument of direct-marketing. Therefore, unsolicited SMS messages of a commercial nature are covered by the opt-in regime of Article 13(1). The analysis in this subparagraph applies *mutatis mutandis* to similar technologies with different specifications, such as Multi Media Messaging (MMS).

2.5 Scope II: direct marketing

There is no definition of direct marketing in either the specific or general data protection Directives. There is however a description of marketing purposes in Recital 30 of Directive 95/46/EC, which states : *"(…) whereas Member States may similarly specify the conditions under which personal data may be disclosed to a third party for the purposes of marketing whether carried out commercially or by a charitable organisation or by any other association or foundation, of a political nature for example, subject to the provisions allowing a data subject to object to the processing of data regarding him, at no cost and without having to state his reasons*".

The Article 29 Working Party has stated that Article 13 of Directive 2002/58/EC consequently covers any form of sales promotion, including direct marketing by charities and political organisations (e.g. fund raising, etc.).[58] In this section we will try to establish the meaning of the notion 'direct marketing' within the E-Privacy Directive.

Recital 44 of the E-Privacy Directive states:

> "Direct marketing activities carried out by political, charity or other organizations, for instance 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."

This Recital explains to what extent the provisions on unsolicited e-mail for direct marketing purposes would affect messages sent by political parties and charities.

[58] Article 29 Working Party 2004, p. 7.

According to some Members of the European Parliament, who initially voted against Recital 44, the distinction introduced between direct marketing activities ("aimed at recruiting new members, fund raising or lobbying for votes") and other activities ("expression of views, thoughts and ideas") is artificial because these activities, that are at the basis of and a reason for the existence of associations, charities and parties are intermingled and linked to each other. [59] According to the European Commission, Recital 44 only clarifies an existing interpretation under the General Data Protection Directive 95/46/EC on this issue.[60]

Recital 44 reflects that (political) ideas are more strongly protected under the flag of freedom of expression than speech of a more obvious commercial nature. Political parties, charities or other organizations, which send out messages solely expressing views, thoughts and ideas without a direct commercial aim would therefore fall outside the scope of Article 13 of the E-Privacy Directive. However, according to Recital 10 and Article 1(2) of the E-Privacy Directive, these communications would still be covered by the general regime on data-processing of the Data Protection Directive.

The distinction in Recital 44 between non-commercial and commercial messages does not define the meaning of the notion 'direct marketing'.

If we compare this to the current definitions of advertising, we find that, according to Article 2 of the Directive on Misleading Advertising, the notion 'advertising' means:

> "the making of a representation in any form in connection with a trade, business, craft or profession in order to promote the supply of goods or services, including immovable property, rights and obligations".61

The key element of advertising is the promotion of the supply of goods and services.

Article 2(f) of the E-Commerce Directive defines commercial communication as:

> "Any form of communication designed to promote, directly or indirectly, the goods, services or image of a company, organization or person pursuing a commercial, industrial, or craft activity or exercising a regulated profession."

The phrase "directly or indirectly" can be interpreted either to include direct marketing in the category of commercial communications or to include communications with an indirect commercial aim such as communications by political parties or charities.

[59] Committee on Citizens' Freedoms and Rights, Justice and Home Affairs, Rapporteur: Marco Cappato. Recommendation for second reading on the Council common position for adopting a European Parliament and Council directive concerning the processing of personal data and the protection of privacy in the electronic communications sector (15396/2/2001 . C5-0035/2002 . 2000/0189(COD)) FINAL A5-0130/2002. 22 April 2002, p. 11-12.

[60] Opinion of the Commission pursuant to Article 251 (2), third subparagraph, point (c) of the EC Treaty, on the European Parliament's amendments to the Council's common position regarding the proposal for a Directive of the European Parliament and of the Council on the processing of personal data and the protection of privacy in the electronic communications sector amending the proposal of the Commission pursuant to Article 250 (2) of the EC Treaty COM/2002/0338 final, p.2.

[61] Council Directive 84/450/EEC of 10 September 1984 relating to the approximation of the laws, regulations and administrative provisions of the Member States concerning misleading advertising, *OJ L 250 , 19/09/1984 P. 0017 – 0020.*

The 1985 Recommendation of the Council of Europe on the protection of personal data used for the purposes of direct marketing defines 'direct marketing' as:

> "All activities which make it possible to offer goods or services or to transmit any other messages to a segment of the population by post, telephone or other direct means aimed at informing or soliciting a response from the data subject as well as any service ancillary thereto."62

In this definition of direct marketing the phrases 'segment of the population' and 'direct means' are the distinctive elements.

The European Code of Practice for the use of Personal Data in Direct Marketing of the Federation of European Direct Marketing (FEDMA), [63] which has been approved by the Article 29 Working Party,[64] 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 is technology neutral and applies to e-mail, SMS or other means of communication. The phrase 'which is carried out by the Direct Marketer itself or on its behalf', within the definition of direct marketing of the FEDMA Code, does justice to the fact that most spam runs are handled by agents instead of by vendors themselves. The FEDMA Code further defines the notion 'direct marketer' as:

> "any natural or legal person (including charities and political parties) who communicates by whatever means (including but not limited to mail, fax, telephone, on-line services etc…) any advertising or marketing material which is directed to particular individuals".

The key phrase in the definition of direct marketing in the FEDMA Code is therefore 'directed to particular individuals'.

Once we look at the distinguishing elements of the various definitions addressed here, it is relevant to assess what distinguishes direct marketing from commercial communications in general. 'Marketing' seems to refer to the promotion of goods or services. The promotion of image seems not to be included since we have seen earlier in this section that messages reflecting ideas, without a direct commercial aim, seem to be exempted from Article 13 by Recital 44 of the E-Privacy Directive.

Crucial in distinguishing direct marketing from commercial communications in general is the manner in which the promotion reaches its target. In direct marketing the promotional message is delivered to a limited group of potential customers, as opposed to a potentially unlimited audience that can be reached through a mass medium, e.g. broadcasting or a newspaper.

---

[62] Council of Europe, Recommendation No.R (85) 20 of the Committee of Ministers to Member States on the protection of personal data used for the purposes of direct marketing. Appendix with Guidelines. Recommendation No. R (95) 4 of the Committee of Ministers to Member States on the protection of personal data in the area of telecommunication services, with particular reference to telephone services, refers to this 1985 Recommendation.

[63] Available at: http://www.fedma.org/img/db/FEDMACodeEN.pdf

[64] Article 29 Working Party, opinion 3/2003 on the European code of conduct of FEDMA for the use of personal data in direct marketing, adopted on 13 June 2003, 10066/03/EN final WP 77
Available at: http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2003/wp77_en.pdf
The Article 29 Working Party was set up pursuant to Article 29 of Directive 95/46/EC. It is an independent European advisory body on the protection of data and privacy. Its missions are laid down in Article 30 of Directive 95/46/EC and in Article 14 of Directive 97/66/EC, http://europa.eu.int/comm/privacy

To reach a limited group of potential customers, the message has to be addressed in order to be delivered on an individual basis. For the message to be addressed it is not necessary that the addressees name is stated, or that the message is individualized. The prerequisite of an address distinguishes direct marketing from advertising in general. In short, within the E-Privacy Directive, the notion 'direct marketing' seems to point to the promotion of goods and services by means of addressed messages.

2.6 Opt-in

Like its predecessor, the ISDN Directive, Article 13 of the E-Privacy Directive requires prior consent for the use of *automatic calling machines and faxes* for the purposes of direct marketing. Now, also electronic mail has been placed under an opt-in regime. Opt-in requires prior consent, meaning that the recipient has to give his permission to send him communications, beforehand. This is the mirror image of the opt-out option, when the recipient can only refuse permission to send him any further communications after receipt of an unsolicited communication.

The disadvantages of an opt-out regime are many (or: great). First, it can take a lot of effort to opt-out on every unsolicited communication a person may receive. Secondly, opting-out offers the spammer evidence that the used contact details are correct, making them even more valuable. Even if the organization which keeps the opt-out register is legitimate and does not use or sell the registered contact details, there is still the danger that the register will be hacked. A database with confirmed contact details is even more valuable to spammers than e-mail addresses which are harvested on the internet and which sometimes are out of date.

Opt-in can be made stronger by applying a so-called double opt-in standard. Double opt-in requires the following procedure: after a user has given his consent, a message is sent to this user (by e-mail or SMS). The user then has to reply to this message, for instance by following a link to a website and entering a code which has been included in the message. The user then receives a message which contains the final confirmation of the opt-in. This way it is harder to sign up with someone else's address.

The term "soft opt-in" has been used to describe the main exception to Article 13 (1), namely Article 13(2). It has been called soft opt-in because it presupposes a prior relationship between the sender and the recipient of the message. In that case a 'softer' regime applies than the one in Article 13 (1). The recipient has already provided the sender with his contact details in the context of a previous relationship and has at that time agreed to receive unsolicited messages, so no further action is required.

2.6.1 13(1) Prior consent

What are the requirements for prior consent? Article 2(f) of the E-Privacy Directive states
that consent by a user or subscriber corresponds to the data subject's consent in the Data Protection Directive. According to Article 2(h) of the Data Protection Directive 'the data subject's consent' shall mean 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.

There may be various ways by which consent may be provided in accordance with Community law. The actual method to collect that consent has not been specifically provided for in Directive 2002/58/EC. Recital 17 re-affirms this: *"(…) Consent may be given by any appropriate method enabling a freely given specific and informed indication of the user's wishes, including by ticking a box when visiting an Internet website."* Without prejudice to other applicable requirements on e.g. information, methods whereby a subscriber gives prior consent by registering on a website and is later asked to confirm that he was the person who registered and to confirm his consent seem to be compatible with the Directive. Other methods may also be compatible with legal requirements.

Recital 17 of the E-Privacy Directive adds: 'Consent may be given by any appropriate method enabling a freely given specific and informed indication of the user's wishes, including by ticking a box when visiting an Internet website'. In our opinion however, this does not include 'unticking a box'. Furthermore, since the consent has to be given by the data subject itself, 'tell a friend' is not a valid method to inform potential customers. Interpretation of the notion 'consent' is a matter of civil law, and therefore the meaning of consent can differ among Member States.

According to the Article 29 Working Party, it would not be compatible with Article 13 of Directive 2002/58/EC simply to ask, by a general e-mail sent to recipients, their consent to receive marketing e-mails, because of the requirement that the purpose for which the consent is sought be legitimate, explicit and specific. Moreover, consent given on the occasion of the general acceptance of the terms and conditions governing the possible main contract (e.g., a subscription contract, in which consent is also sought to send communications for direct marketing purposes) must respect the requirements in Directive 95/46/EC, that is, be informed, specific and freely given. Provided that these latter conditions are met, consent might be given by the data subject for instance, through the ticking of a box. Ultimately, this is a matter of national law to be solved by national legislators.

The purpose(s) should also be clearly indicated. This implies that the goods and services, or the categories of goods and services, for which marketing e-mails may be sent should be clearly indicated to the subscriber. Consent to pass on the personal data to third parties should also be asked where applicable. The information provided to the data subject should therefore indicate the purpose(s), and the goods and services (or categories of goods and services) for which those third parties would send e-mails.

According to the Article 29 Working Party, lists of e-mail addresses which have not been established according to the prior consent requirement may not be used anymore under the opt-in regime, at least until they have been adapted to the new requirements. Selling such incompatible lists to third parties is not legal either. Companies wishing to buy lists of e-mail addresses should be cautious that those lists are in accordance with applicable requirements, and in particular that prior consent was given in accordance with those requirements. However, it is a matter for national law to decide the exact rules on e-mail lists within the Directive's framework. Article 13 also provides for the obligation to offer an opt-out possibility in each message sent. Such an opt-out should at least be possible using the same communications service (e.g., by sending an SMS to opt-out of an SMS-based marketing list).[65]

[65] Article 29 Working Party 2004, p. 6-7.

2.6.2 13(2): Soft opt-in

Article 13(2)

Notwithstanding paragraph 1, where a natural or legal person obtains from its customers their electronic contact details for electronic mail, in the context of the sale of a product or a service, in accordance with Directive 95/46/EC, the same natural or legal person may use these electronic contact details for direct marketing of its own similar products or services provided that customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details when they are collected and on the occasion of each message in case the customer has not initially refused such use.

As mentioned above, Article 13 (2) presents an exception to the opt-in regime of Article 13(1), with regard to existing customer relations. When a company has acquired the electronic contact details of a customer in the context of a sale, the company can send this person unsolicited messages for purposes of direct marketing of its own products or services, unless this person objected to this at the time the contact details were acquired. The recipient of the unsolicited message can then opt-out if he no longer wants to receive such messages. Recital 41 explains Article 13(2) as follows:

Recital 41

Within the context of an existing customer relationship, it is reasonable to allow the use of electronic contact details for the offering of similar products or services, but only by the same company that has obtained the electronic contact details in accordance with Directive 95/46/EC. When electronic contact details are obtained, the customer should be informed about their further use for direct marketing in a clear and distinct manner, and be given the opportunity to refuse such usage. This opportunity should continue to be offered with each subsequent direct marketing message, free of charge, except for any costs for the transmission of this refusal.

As both Article 13 and Recital 41 state, electronic contact details must be processed in accordance with the principles of Directive 95/46 EC, the Data Protection Directive. Electronic contact details are personal data since the name of the customer will be registered as well. This renders it possible to identify the person behind even the most non-descriptive e-mail address. This means that, in order for the processing to be fair, the user of the electronic contact details must be provided with certain information before he discloses his or her data, and must consent to the use to which it is to be put. The information to be provided to him must include the identity of the data controller, the purpose for which the data is to be processed and "any further information which is necessary, having regard to the specific circumstances in which the data is or are to be processed, to enable processing in respect of the data subject to be fair".[66]

In practice, this means that when the electronic contact details are collected, information has to be provided about the natural or legal person that collects the data (the data controller). This includes information on whether the data is collected for the company itself, or for e.g. a holding to which the company belongs. Also, it must be clear to the data subject that his contact details may be

[66] Owen & Kiernan Earl 2003, p.3.

used for direct marketing purposes, so that customers have the opportunity to object to such use of their electronic contact details.

The phrase relating to the provision of further information "having regard to the specific circumstances in which the data is or are to be processed", might refer to the obligation to also provide information on the natural or legal person who processes the data on behalf of the data controller (the data processor). This could pose difficulties to a company, which wishes to hire another company to perform a direct marketing campaign on its behalf, after the data have been obtained. In some instances a company is required to have a privacy protocol, according to national law.

The text of paragraph 13(2) is unclear as regards the addresses obtained from customers before the entering into force of the E-Privacy Directive. Because the text of provision 13(2) is phrased in the present ("where a natural or legal person obtains from its customers their electronic contact details for electronic mail"), it seems unlikely that electronic contact details of previous customers can be used to send unsolicited commercial communications. Also, Article 13(2) demands that "customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details when they are collected". As Recital 41 explains, use of electronic contact details is only allowed when the data controller, to comply with the prerequisites for fair processing of the Data Protection Directive as described in the previous section, has already informed his customers at the time their electronic contact details were collected, of the possible use of those data for the purposes of direct marketing. A company is not allowed to send unsolicited communications to customers who did not consent to this beforehand.[67] In the process of transposing the Directive, national laws should clarify this ambiguity. To provide for a transitional system in which previous customers can be asked for permission to send further unsolicited communications may be a violation of the rules laid down in Article 13 of the Directive, because the communication which is used to ask for permission to send further communications, would be an unsolicited communication in itself.

Paragraph 13(2) relates to contact details obtained in the *context of a sale* of a product or a service. What is considered a sale? In an earlier draft the text stated 'purchase' instead of 'sale'. The text was amended because it was feared that marketers could argue that although no sale had taken place, a consumer could be approached under the soft opt-in regime, as they had expressed an interest in purchasing a product.[68] This indicates that there has to be a finalized sales contract, not just an order or a down-payment on a future sale.

If the sales contract is broken and the contract is subsequently nullified, it is a matter for national law to decide whether that means that there was never a relationship between consumer and supplier and that therefore the soft opt-in rule does not apply.

It is unclear for what period of time addresses of previous customers may be used for direct marketing purposes. Article 6 (e) of the Data Protection Directive states that Member States shall provide that personal data must be "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed."

[67] However, electronic addresses could be used to send unsolicited messages of an obvious non-commercial nature, such as safety warnings, which fall outside the scope of Article 13.
[68] Magee 2003, p. 22.

The term 'the context of the sale' suggests that contact details obtained from potential customers would fall in the soft opt-in exception. However, since the term "purchase" was replaced by the term "sale", details given *before* the sale can only be used if a sale eventually did take place. Therefore, addresses of potential buyers can only be used according to the opt-in rules of paragraph 13(1). Addresses of potential customers can be gathered through cookies that register people who are 'just browsing' on the web, and can register even the articles they are interested in.[69] Even if permission is obtained for the use of that kind of technology as is required under Article 5(3) of the E-Privacy Directive, this does not imply consent to send unsolicited communications. Another way of collecting contact details from potential customers is when interested consumers request information about a certain product or service. Unless of course these future customers already gave their consent for further related marketing on the request form, it seems logical that the opt-in rule of paragraph 13(1) would apply here as well.[70]

Paragraph 13(2) states that contact details may be used for direct marketing of a company's (or: the relevant natural or legal person's) own similar products or services. This immediately creates a number of questions of interpretation. It has to be established what this means for companies that sell thousands of different articles, whether a (web) store with different articles has the right to market every other item they sell, and whether the interpretation of 'similar' should be wide or narrow.

Another problem is the phrase 'its own products or services'. This prompts the question whether different parts of a holding can be considered as one company.

Article 13(2) states 'where a natural or legal person **obtains** from **its** customers'. A previous version of the Directive stated that the electronic contact details had to be obtained directly from the customer in question. The removal of that explicit condition could indicate that a manufacturer or wholesaler, who has obtained an e-mail address from the retailer who made the sale, may regard the e-mail address as being that of one of its own customers.[71] However, Recital 41 states clearly that the use of electronic contact details is allowed "only by the same company that has obtained the electronic contact details". Depending on whether the name of the holding or the company is used on the consent form, this could mean that the concept of 'company' might not stretch beyond that particular company, or the holding the company belongs to. In case of transfer to third parties, the data subject should be notified according to Article 11 of the Data Protection Directive. Again, however, this would be an unsolicited communication in itself.

Article 13(2) could become an area that could provoke a lot of case law. Whether products are similar, come from the same store or if the customer gave his address to this particular store are all questions to which the answers are different from case to case.
The addressee has to be able to opt out of future marketing, in an easy way and free of charge. However, it should be noted that the user of the address still has to pay to send that e-mail and spend time and effort on opting out. Recital 41 acknowledges this, but does not give the option of reimbursement.

[69] Magee 2003, p.22.
[70] For a broader interpretation of the notion context of a sale', see Butler 2003, on the British implementation of the E-Privacy Directive.
[71] Magee 2003, p. 22.

It seems reasonable that the requirements for soft opt-in, namely 'the opportunity to object, free of charge and in an easy manner' also apply to customers who have opted in before and now want to opt-out. This should be provided for in a clear and distinct manner on the occasion of each message that is sent.

The soft opt-in provision exchanges the prerequisite of prior consent of Article 13(1) for a more general consent to the use of electronic contact details, which includes the use of such data for the purpose of direct marketing. The range of products a customer agrees to receive promotional messages on, may not be clear at the time the customer gives his consent, since Article 13(2) can be interpreted in a very broad sense, including all kinds of products from all kinds of companies that are related to the original collector of the data, which had a direct relationship with this customer. However, in its later Communication, the Commission has made it very clear that Article 13 (2) is to be interpreted and implemented restrictedly.[72] The Article 29 Working Party also stresses that the exception of Article 13 (2) must be interpreted narrowly.[73]

2.6.3 13(3): Other unsolicited communications

Article 13(3)

Member States shall take appropriate measures to ensure that, free of charge, unsolicited communications for purposes of direct marketing, in cases other than those referred to in paragraphs 1 and 2, are not allowed either without the consent of the subscribers concerned or in respect of subscribers who do not wish to receive these communications, the choice between these options to be determined by national legislation.

Member States must take appropriate measures regarding other unsolicited communications. The choice between the options set out in Article 13(3) seems to refer to the choice between an opt-in and an opt-out regime. Non-automatic calls by direct marketers are an example of "other unsolicited communications".

2.6.4 13(4): Identification

Article 13(3)

Member States shall take appropriate measures to ensure that, free of charge, unsolicited communications for purposes of direct marketing, in cases other than those referred to in paragraphs 1 and 2, are not allowed either without the consent of the subscribers concerned or in respect of subscribers who do not wish to receive these communications, the choice between these options to be determined by national legislation.

This paragraph aims to ban the practice of falsifying the point of origin and transmission path of electronic mail to conceal the sender's identity. The requirement of a valid return address poses some questions. What is to be understood by "valid"? Spam spread through hacked machines and their e-mail programs (and possibly their address book) and which therefore can contain an existing address may very well be using a valid address. Perhaps the validity of an address should be connected with its opt-out effectiveness.

[72] Communication 2004
[73] Article 29 Working Party 2004.

The E-Commerce Directive also contains a requirement for the natural or legal person on whose behalf the commercial communication is made, to be clearly identifiable (Article 6, under b). Concerning the recognizability of the direct marketing message, the labeling requirements of Article 7 (1) of the E-Commerce Directive will apply next to the requirements of the E-Privacy Directive.

2.7 Users, subscribers, corporations

Article 13(5)

Paragraphs 1 and 3 shall apply to subscribers who are natural persons. Member States shall also ensure, in the framework of Community law and applicable national legislation, that the legitimate interests of subscribers other than natural persons with regard to unsolicited communications are sufficiently protected.

Article 13(5) states that only subscribers that are natural persons are protected by paragraphs 1 and 3 of Article 13. This poses some questions.

Article 13(5) excludes subscribers which are legal persons from the protection of Article 13(1) and 13(3). Consider, for instance, the head of a family who has a contract with an internet service provider to access the internet and to have an e-mail account. Such an account often has several addresses which are distributed to members of that family. The mother and children are users but not subscribers. This means that only the father would be directly protected by Article 13.

According to paragraph 1, in order to opt-in, the subscriber has to give his consent. Theoretically this would mean that the mother and children would have to ask the father to opt-in for them.

According to Article 13(5) Member States have to ensure that the legitimate interests of subscribers other than natural persons are sufficiently protected. This points towards protection of corporations. Users, like the other family members in our example who are natural persons but not subscribers, are therefore only protected under Article 13(2). Article 7(2) of the E-Commerce Directive applies in concurrence with the E-Privacy Directive. The obligation to respect and consult opt-out registers might therefore also be relevant to customers opting-out of unsolicited electronic communications based on existing customer relationships. This includes users.

Recital 12

Subscribers to a publicly available electronic communications service may be natural or legal persons. By supplementing Directive 95/46/EC, this Directive is aimed at protecting the fundamental rights of natural persons and particularly their right to privacy, as well as the legitimate interests of legal persons. This Directive does not entail an obligation for Member States to extend the application of Directive 95/46/EC to the protection of the legitimate interests of legal persons, which is ensured within the framework of the applicable Community and national legislation.

Legal persons are not protected by the general regime of the Data Protection Directive. According to Article 13(5), subscribers other than natural persons are exempt from the protection of paragraphs 1 and 3 of Article 13.

Corporations and government institutions are therefore outside the scope of the protection provided by Article 13(1) and 13(3). However, Recital 45 of the E-Privacy Directive states:

Recital 45

This Directive is without prejudice to the arrangements which Member States make to protect the legitimate interests of legal persons with regard to unsolicited communications for direct marketing purposes. Where Member States establish an opt-out register for such communications to legal persons, mostly business users, the provisions of Article 7 of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market (Directive on electronic commerce) are fully applicable.

In our opinion this means that Member States are obliged to protect corporations from unsolicited communications, either by means of an opt-in or an opt-out system. If Member States choose the opt-out system, the provisions of the E-Commerce Directive apply.

The need for protection of corporations was expressed in the initial proposal for the E-Privacy Directive: "Articles 12 and 13 on directories and unsolicited communications require Member States to take account of the legitimate interests of subscribers to electronic communications services who are legal persons, with regard to the publication of their data in public directories and with regard to possibilities to protect themselves against unsolicited communications for direct marketing purposes. Those provisions recognize that small and medium sized firms may have similar problems as individuals in these two areas."[74]

Article 13(5) states that the protection of Article 13(1) and Article 13(3) only applies to subscribers who are natural persons, which seems to exclude all corporations, including their personnel. However, when a corporation consists of only one person, in that case the subscriber might in fact be a natural person. Freelancers for example, are often not legal persons. Freelancers often use the same address for work and personal mail. Furthermore, employees can also use their work address for non-work related communications, at home as well as at work.

They are left outside the scope of Article 13. The employer is the subscriber and as the employer in most cases will be a legal person, paragraphs 13(1) and 13(3) do not apply. Consequently, the employee is left unprotected by Article 13. Unlike the members of the family in our example the employee cannot turn to the employer to ask him to complain on his behalf, or even opt-in. However, paragraph 5 only relates to paragraphs 1 and 3 of Article 13. Paragraph 2 on existing customer relations refers to customers who may opt-out of their e-mailings. The notion 'customers' comprises both individuals as well as organisations. Companies and their employees can therefore opt-out of business to business e-marketing.

The interests of subscribers other than natural persons have to be sufficiently protected by national law. Member States are free to arrange for a stronger protection for corporations.

[74] Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector /* COM/2000/0385 final - COD 2000/0189 */ *Official Journal C 365 E, 19/12/2000 P. 0223 – 022* (under impact assessment).

This has caused a lot of discussion in various Member States. Corporations obviously suffer from spam too. The argument that business to business marketing should stay possible could be met by giving employees the protection as offered by the opt-in requirements of paragraph 13(1). This would meet the needs of companies, while leaving strict business addresses like info@ susceptible to unsolicited communications. It is very important how the burden of proof is divided in situations like this. If, for instance, the spammer had the burden to prove that the spam receiver is in fact not a natural person and the subscriber, it would mean that spammers could not risk to keep sending spam to most corporate e-mail addresses. That would *de facto* broaden the opt-in rule to corporate e-mail accounts. However, the division of the burden of proof is a matter of national law.

2.8 Conclusions

In this Chapter, we have discussed the specific regulation of unsolicited communications in the E-Privacy Directive. We have seen how that directive fits within the framework on electronic communications that has been introduced in the EC. An important goal of the framework is to adapt former telecommunications law to the internet era and to provide for effective consumer protection. In that perspective, the Commission has more than once stressed the importance it attaches to protection against spam.

The E-Privacy Directive itself is the successor to the 1997 ISDN Privacy Directive and contains provisions on a number of issues related to privacy and communications. Article 13 provides for a harmonized protection against unsolicited communications or spam. The article has been the subject of a lot of debate between the European Parliament and the European Commission and the final text presents in some ways the results of that fierce struggle. The scope of Article 13 is defined by a number of key definitions. First of all, electronic communications are the subject of the Directive and therefore of Article 13. Secondly, Article 13 only relates to unsolicited communications with direct marketing purposes. It is therefore important to find out the meaning and correct interpretation of "direct marketing."

Article 13(1) has introduced a pan European opt-in rule for unsolicited communications. It is a very important step in order to harmonize anti-spam laws throughout the Union. The opt-in rule means that spammers are only allowed to send their messages if they have received the prior consent of their addressees. The meaning of the concept of 'consent' is influenced by the meaning attached to consent in the Data Protection Directive. Article 13(2) introduces an exception to the main opt-in rule for sending information in the context of existing customer relations (or: to existing customers) concerning similar products or services. It is because of that exception that Article 13 was named 'soft opt-in" by some.

Article 13(3) introduces an obligation for Member States to ensure an adequate protection against other forms of unsolicited communications. Article 13(4) prohibits the use of false or disguised identity when sending direct marketing e-mails, while Article 13(5) requires Member States to take measures in order to protect the interests of corporations. It is very important how the burden of proof is divided in situations where the opt-in rule does not apply to legal persons. If, for instance, the spammer had the burden to prove that the spam receiver is in fact not a natural person and the subscriber, it would mean that spammers could not risk to keep sending spam to most corporate e-mail addresses.

The scope of Article 13 is limited to natural persons being subscribers to the relevant electronic communications services. It is left up to Member States to decide whether legal persons and users which are not subscribers can also enjoy the protection of the opt-in rule of Article 13(1). This limited scope renders the article much less effective in providing adequate protection against spam as a lot of people receive most unsolicited communications while at work or at their work address.

3 Spam and security

3.1 Introduction

Spam can slow down computer networks and can seriously damage personal computers when used to spread computer viruses or worms. Large volumes of spam can even interfere with critical computer infrastructures and endanger public safety. Some spam also contains destructive viruses and worms. Virus writers sometimes write programs that download users' address books and propagate viruses by sending them to all users in an address book. That way, virus writers avoid anti-spam filters.[75] Spammers also exploit security weaknesses inherent in e-mail transfer technology such as open relays and open proxies. In recent years, internet users have been plagued by combinations of spam and viruses. Spammers seem to be using virus-writing techniques to get their messages through filters. Virus writers also have made use of spammers' mass-mailing techniques for the purpose of attacking computer systems. Therefore, we need to assess the possible convergence in the regulation of viruses and spam via the rules on security. In this paragraph we look at the meaning of "security" in the context of the E-Privacy Directive and at the possible impact thereof on the regulation of spam. We pose the question whether the obligation to secure networks could be of relevance in the context of the fight against spam. Article 4 of the E-Privacy Directive is relevant to the spam problem in two ways. First of all, we have to consider whether spam spread by a virus is spam in the context of Article 13 of the E-Privacy Directive. It is safe to assume that sometimes virus e-mails fit the definition of Article 13. Secondly, if spam threatens the security of a network, it seems reasonable to infer that Article 4 applies.

Also, Article 4 and recital 20 point to the General Data Protection Directive, suggesting that the safeguarding measures could possibly apply to the security of transmitted data.

Article 4 Security

(1) The provider of a publicly available electronic communications service must take appropriate technical and organizational measures to safeguard security of its services, if necessary in conjunction with the provider of the public communications network with respect to network security. Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented.

(2) In case of a particular risk of a breach of the security of the network, the provider of a publicly available electronic communications service must inform the subscribers concerning such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, of any possible remedies, including an indication of the likely costs involved.

Recital 20 states that security is appraised in the light of Article 17 of the Data Protection Directive.[76]

[75] OECD 2004.
[76] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *OJ* 1995 L 281/31-50.

Service providers should take appropriate measures to safeguard the security of their services, if necessary in conjunction with the provider of the network, and inform subscribers of any special risks of a breach of the security of the network. Such risks may especially occur for electronic communications services over an open network such as the Internet or analogue mobile telephony. It is particularly important for subscribers and users of such services to be fully informed by their service provider of the existing security risks which lie outside the scope of possible remedies by the service provider. Service providers who offer publicly available electronic communications services over the Internet should inform users and subscribers of measures they can take to protect the security of their communications for instance by using specific types of software or encryption technologies. The requirement to inform subscribers of particular security risks does not discharge a service provider from the obligation to take, at its own costs, appropriate and immediate measures to remedy any new, unforeseen security risks and restore the normal security level of the service. The provision of information about security risks to the subscriber should be free of charge except for any nominal costs which the subscriber may incur while receiving or collecting the information, for instance by downloading an electronic mail message. Security is appraised in the light of Article 17 of Directive 95/46/EC.

This prompts the question of what that means with regard to the notion of security as used in Article 4 of the E-Privacy Directive.

Article 17 DPD Security of processing
1. Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.
2. The Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures.
3. The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that:
- the processor shall act only on instructions from the controller,
- the obligations set out in paragraph 1, as defined by the law of the Member State in which the processor is established, shall also be incumbent on the processor.
4. For the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the measures referred to in paragraph 1 shall be in writing or in another equivalent form

According to Article 2(c) of the Data Protection Directive processing of personal data means:

"any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use,

disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction."

Service providers process data in multiple ways: use, storage etc. This means that providers are processors within the meaning of Article 2(e) of the Data Protection Directive:

(e) 'processor' shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;

Personal data must be processed in accordance with the principles of the Data Protection Directive. Principle 7 states: "Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing and against accidental loss or destruction of personal data." (see 4.3.2). This is a short version of the more extensive formula in Article 17 DPD. However, Article 17 puts the responsibility, and therefore the liability, in the hands of the controller. According to Article 2(d) of the Data Protection Directive 'controller' means:

"the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law."

However, Article 17(3) DPD can create a contractual obligation for the provider, with regard to the controller, to process the data according to the standards of Article 17 DPD. Furthermore, in the specific context of the E-Privacy Directive, the provider is the controller who is responsible for the security of the network or service and therefore for the data transport (including the data processing involved).

Apart from the question of who is responsible for security of the data, it is not clear what situations are covered by the reference in Recital 20 of the E-Privacy Directive to Article 17 DPD, which provides for "appropriate measures to protect personal data (…) against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access (…) and all other unlawful forms of processing." Several interpretations of Article 4 are possible in this light. A restrictive interpretation would lead to the conclusion that the duty to take measures only points to an obligation to protect those data the ISP processes himself. A broader interpretation would include the duty to protect against unsolicited or damaging information. The question is whether this includes hacking of servers which contain personal data databases (e.g. directories) and listening in on data-traffic in order to harvest e-mail addresses. We think it is reasonable to state that this is covered by the Directive.

Another interpretation of the notion of security could be significant with regard to anti-virus protection. The mass-mailing worm SOBIG.F marks a trend of spamming tools used in concert with computer worms.[77] SOBIG.F supposedly can also open up computer ports, making them vulnerable to hacking. Finally, the worm is said to spoof sender information and to use e-mail addresses that are harvested from the infected computer. The worm is believed to be used deliberately by spammers, to be able to use infected computers as open relays for more future spamming activities. The integration of spamming and virus communities is an enormous addition to the spam problem.

[77] TechNewsWorld August 21, 2003. Available at: http://www.technewsworld.com/perl/story/31393.html.

In this interpretation of security, providers do have certain obligations with respect to prevention, also through means of education and notification, as well as damage control after the fact. However, in other matters than privacy, these issues seem questions to be answered by general liability law, which includes the duty of care for providers with regard to the security of their networks or services.

The first sentence of Article 4(1) states:

'The provider of a publicly available electronic communications service must take appropriate technical and organizational measures to safeguard security of its services, if necessary in conjunction with the provider of the public communications network with respect to network security'.

"Technical measures" refers to protective devices such as firewalls, but also to blocking and filtering of e-mail containing viruses. Since viruses can also operate as spam distributors this obligation is relevant to the fight against spam. Article 4(1) also calls for organizational measures, for instance extra personnel for system analysis and helpdesk operations. This could also include education of subscribers.

According to Article 4(1) both technical and organizational measures have to be 'appropriate'. The second sentence of Article 4(1) states:

'Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented'.

What is appropriate therefore depends on the seriousness of the risk involved, what kinds of measures are technically possible and available, and what it would cost to implement them. Appropriate is a discretionary notion. It will depend on the circumstances of each individual case what measures have to be taken.

As technical measures are further developed all the time it is impossible to lay down a minimum required level of protection in legislation. As for organizational measures, it seems reasonable for these measures to have a certain level before they gain any effect. For instance, educational material should be brought to the attention of subscribers and should be easily accessible. It is unclear how far a provider should stretch to inform its subscribers of possible risks involved. Relevant requirements can be put into legislation more easily than requirements for technical measures.

Can a communications service provider hold the network service provider liable for not fully securing the network, as a result of which the communications service provider is facing a lawsuit from one his subscribers? The Directive does not answer that question but it cannot be excluded. In the end, it is a matter of national law whether liability of the ISP is inferred as a result of this part of the E-Privacy Directive.

Other security issues are raised by the use of spam to lure unsuspecting users to Web pages where spying software is secretly downloaded. Spyware monitors a user's activity on the Internet and transmits that information to someone else. It may also gather information about e-mail addresses, passwords, and credit-card numbers.[78]

[78] ÓECD Background paper 2004, p. 16-17.

Since spam can contain viruses, spam can under certain circumstances also be considered a 'breach of the security of the network'. This could mean that communications service providers have an obligation towards their users to warn them if there is such a spam attack and of what they can do about it themselves. Article 4 (2) of the E-Privacy Directive contains an obligation to inform customers about potential security breaches:

Article 4(2)

In case of a particular risk of a breach of the security of the network, the provider of a publicly available electronic communications service must inform the subscribers concerning such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, of any possible remedies, including an indication of the likely costs involved.

It is unclear whether the obligation to inform subscribers concerning such a risk includes an obligation of notification after the fact. However, we assume that under certain circumstances the obligation of a service provider to inform his subscribers in case of a particular risk of a breach of security, also includes the risk following a breach of security that has already occurred.

3.2 Conclusions

In this Chapter we described the specific section of the E-Privacy Directive dealing with network security. Article 4 introduces the obligation for providers to take appropriate measures in order to safeguard the security of their services. In case of a particular risk of a breach of security, the provider must also inform subscribers concerning such risk and of possible remedies available. A development with serious security implications is the convergence of spam and viruses.

The E-Privacy Directive addresses security issues and requires appropriate measures to be taken by providers. This does not introduce a strong right for users to object to their providers about letting through spam. Under certain circumstances, tort law or contract law could oblige providers to take measures against spam and viruses, such as filtering. A duty to act could be reasonable as soon as the access to either network or services is threatened due to spam and viruses. ISPs should inform their customers about their spam policy and possibly about available technological solutions.

4 Harvesting mail addresses

4.1 Introduction

In order to send unsolicited e-mail a spammer needs addresses, such as e-mail addresses or phone numbers. Those addresses can be collected by the marketer in several ways, not all of which are legitimate. Addresses can be obtained directly from persons by request, they can be retrieved from a database which is compiled by another party, or they can be harvested on the internet. Databases may contain addresses that are collected in a legal manner, for instance by a business that went bankrupt and now sells the client database to pay its debts. Databases can also contain stolen addresses or addresses which have been harvested on the internet by means of a so-called crawler. This is a computer program that roams the internet looking for electronic addresses, mostly e-mail addresses.

The Data Protection Directive contains rules on the processing of personal data. The Article 29 Working Party, the independent European advisory body on the protection of data and privacy, declared in 2000 the harvesting of e-mail addresses on the internet as amounting to unlawful processing of personal data according to the rules of the Data Protection Directive.[79] In this Chapter, we will try to determine if and how the Data Protection Directive offers additional protection to the E-Privacy Directive with regard to spam.

According to Recital 10 of the E-Privacy Directive, the Data Protection Directive applies in parallel to the E-Privacy Directive. Recital 10 states:

"In the electronic communications sector, Directive 95/46/EC applies in particular to all matters concerning protection of fundamental rights and freedoms, which are not specifically covered by the provisions of this Directive, including the obligations on the controller and the rights of individuals. Directive 95/46/EC applies to non-public communications services."

This means that forms of processing personal data which are not covered by the E-Privacy Directive fall within the scope of the Data Protection Directive. The Data Protection Directive also provides additional protection to situations which are covered by the various paragraphs of Article 13.

This is confirmed in Article 1 of the E-Privacy Directive, which states:

"(1)This Directive harmonises the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community.

[79] Art. 29 Working Party: Privacy on the Internet - An integrated EU Approach to On-line Data Protection- Working Document, Adopted on 21st November 2000, 5063/00/EN/FINAL WP 37.
Recital 48 of the E-Privacy Directive states: "it is useful, in the field of application of this Directive, to draw on the experience of the Working Party on the Protection of Individuals with regard to the Processing of Personal Data composed of representatives of the supervisory authorities of the Member States, set up by Article 29 of Directive 95/46/EC. Article 15(3) of the E-Privacy Directive adds to this:
"The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC shall also carry out the tasks laid down in Article 30 of that Directive with regard to matters covered by this Directive, namely the protection of fundamental rights and freedoms and of legitimate interests in the electronic communications sector."

(2)The provisions of this Directive particularise and complement Directive 95/46/EC for the purposes mentioned in paragraph 1. Moreover, they provide for protection of the legitimate interests of subscribers who are legal persons."

The phrase "particularise and complement" in Article 1(2) of the E-Privacy Directive means that the Data Protection Directive provides the general regime on data protection.
The E-Privacy Directive offers a sector specific regime with regard to privacy and electronic communications. This means that only situations regarding processing of personal data, which are not covered by the E-Privacy Directive, fall within the scope of the Data Protection Directive. It also means that the E-Privacy Directive has to be interpreted in a manner consistent with the Data Protection Directive. The second sentence of Article 1(2), on the protection of the legitimate interests of subscribers who are legal persons, is explained in Recital 12 of the E-Privacy Directive, which states:

"Subscribers to a publicly available electronic communications service may be natural or legal persons. By supplementing Directive 95/46/EC, this Directive is aimed at protecting the fundamental rights of natural persons and particularly their right to privacy, as well as the legitimate interests of legal persons. This Directive does not entail an obligation for Member States to extend the application of Directive 95/46/EC to the protection of the legitimate interests of legal persons, which is ensured within the framework of the applicable Community and national legislation."

This means that, although Member States have an obligation to protect the legitimate interests of legal persons, data related to legal persons are not personal data and the rules of the Data Protection Directive do not apply.[80]

Another special regime for electronic addresses is provided for by Article 12 of the E-Privacy Directive on directories, which is dedicated to prevention of harvesting. Article 12 obliges Member States to make sure a subscriber's permission is obtained before being listed. Article 16 of the E-Privacy Directive states that Article 12 does not apply to editions of directories, which have been already produced or placed on the market in printed or off-line form, before the national provisions which transpose the Directive enter into force. Note however that this provision deals with publicly accessible subscriber lists.

4.2 Personal Data

According to Article 2(a) of the general Data Protection Directive,

"'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."

[80] It is a matter of discussion in legal literature whether or not legal persons have a right to privacy. If the scope of a right to privacy is limited to an personal and intimate sphere, is seems hardly imaginable that a legal person should have a right to privacy. For other aspects of privacy, such as confidentiality of communications and spacial privacy, this is less obvious. The ECHR has issued jurisprudence in which legal persons are granted a right to respect for the home, one of the aspects of privacy mentioned in Article 8 of the European Convention of Human Rights (ECHR 30 March 1989, Series A no. 152-A (Chappell); ECHR 16 December 1992, Series A no. 251-B (Niemietz) and especially ECHR 16 April 2002 (Stes Colas Est), available at http://hudoc.echr.coe.int/).
The European Court of Justice had earlier declined the possibility that legal persons have a right to privacy (ECJ 21 September 1989, C-46/87 and 227/88 (Hoechst)), but recently seems to accept that legal persons have a certain right to privacy (ECJ 22 october 2002, C-94/00 (Roquette Frères SA)).

Direct identification means that an e-mail address contains one or more of the mentioned identifiable factors, such as a name, so that the person to which the data relate can be identified without the use of a third source.

In the 1985 Recommendation of the Council of Europe on the protection of personal data used for the purposes of direct marketing, 'personal data' is defined as follows:

"Personal data" means any information relating to an identified or identifiable individual (data subject). An individual shall not be regarded as "identifiable" if the identification requires an unreasonable amount of time, cost and manpower." [81]

The Article 29 Working Party is of the opinion that if an e-mail address is collected in a public space on the Internet¸ its use for unsolicited electronic mailing would be contrary to the relevant Community legislation - for three reasons. Firstly, it could be seen as "unfair" processing of personal data under the terms of Article 6(1)(a) of the general Data Protection Directive.
Secondly, it would be contrary to the "purpose principle" in Article 6(1)(b) of that Directive, in case the data subject made his/her e-mail address public for a quite different reason, for example participation in a newsgroup. Thirdly, given the cost imbalance and the nuisance to the recipient, such mailing could not be regarded as passing the balance of interest test in Article 7(f). This provision (one of several possible legitimate grounds for processing) requires data processing to be "necessary for the purposes of legitimate interests pursued by the controller . . . except where such interests are overridden by the interests of fundamental rights and freedoms of the data subject". [82]

Phone numbers allow indirect identification of the subscriber through reverse directories as well as through telecom providers. Since a phone number is a personal item, which is tied to a telephony service by means of a personal contract, identification of the subscriber will often mean identification of the user. According to Recital 13 of the E-Privacy Directive:

"The contractual relation between a subscriber and a service provider may entail a periodic or a one-off payment for the service provided or to be provided. Prepaid cards are also considered as a contract."

IP addresses allow indirect identification. IP addresses can be traced back to a computer, and through the internet service provider to a subscriber. Also dynamic IP addresses can be traced back to a computer. Although the link between subscriber and user is less strong compared to e-mail addresses and phone numbers, most IP addresses can be tied to a log-in and therefore may qualify as personal data.

Processing of personal data means, according to Article 2(c) of the Directive (specify which Directive),

"any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction."

[81] Appendix with Guidelines. Recommendation No.R (85) 20 of the Committee of Ministers to Member States on the protection of personal data used for the purposes of direct marketing.
[82] Art. 29 Working Party,: Privacy on the Internet - An integrated EU Approach to On-line Data Protection- Working Document, Adopted on 21st November 2000, 5063/00/EN/FINAL WP 37.

Processing of personal data has to conform to the principles set out in the Data Protection Directive. The most important principle of the Data Protection Directive is that the processing must be "fair" (principle 1). This means that the user of the electronic address (the data subject) must have been provided with certain information before he discloses his or her data and must have consented to the use to which it is to be put. The information to be provided to him includes the identity of the data controller, the purpose for which the data is to be processed and "any further information which is necessary, having regard to the specific circumstances in which the data is or are to be processed, to enable processing in respect of the data subject to be fair".[83]

According to Article 2(h) of the Data Protection Directive, 'the data subject's consent' shall mean 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. Article 2(f) of the E-Privacy Directive subsequently states that consent by a user or subscriber corresponds to the data subjects' consent in the Data Protection Directive.

The Data Protection Directive contains a number of definitions regarding various parties engaged in data processing, which are relevant to the situations covered by Article 13 of the E-Privacy Directive.

Article 2 of the Data Protection Directive *inter alia* states:

> "(d) 'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law;
> (e) 'processor' shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;
> (f) 'third party' shall mean any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data;
> (g) 'recipient' shall mean a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients;
> (h) 'the data subject's consent' shall mean 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."

4.3 DPD Enforcement

According to Article 28 of the Data Protection Directive, processing of personal data falls within the jurisdiction of the national data protection agency. According to Article 24, the Member States shall adopt suitable measures to ensure the full implementation of the provisions of this Directive and shall in particular lay down the sanctions to be imposed in case of infringement of the provisions adopted pursuant to this Directive. Often this will result in an administrative fine.

[83] Owen & Kiernan Earl 2003, p.3.

Article 15(2) of the E-Privacy Directive, on the application of certain provisions of Directive 95/46/EC states:

"The provisions of Chapter III on judicial remedies, liability and sanctions of Directive 95/46/EC shall apply with regard to national provisions adopted pursuant to this Directive and with regard to the individual rights derived from this Directive."

According to Chapter III of the Data Protection Directive on judicial remedies, liability and sanctions, without prejudice to any administrative remedy for which provision may be made, inter alia before the supervisory authority referred to in Article 28, prior to referral to the judicial authority, Member States shall provide for the right of every person to a judicial remedy for any breach of the rights guaranteed to that person by the national law applicable to the processing in question (Article 22 DPD). Member States shall provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered (Article 23(1) DPD). The controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage (Article 23(2) DPD).

4.4 Conclusions

Harvesting and scanning of old directories are forms of collecting and therefore processing of personal data, which can under certain circumstances be unlawful. To collect an electronic address in an electronic address book or to use this address to send a spam message also qualifies as processing of personal data. Processing of personal data has to be in accordance with the principles of the Data Protection Directive.

The European Court of Justice has decided in the Lindqvist case that the act of referring, on an internet page, to various persons and identifying them by name or by other means (giving their telephone number or information about their working conditions and hobbies) constitutes "the processing of personal data wholly or partly by automatic means".[84]

The Court also pointed out that the Directive lays down specific rules intended to allow the Member States to monitor the transfer of personal data to third countries. However, given the state of development of the internet at the time the Directive was drawn up and the absence of criteria applicable to use of the internet, the Court takes the view that the Community legislature did not intend the expression "transfer of data to a third country" to cover the loading of data onto an internet page even if such data are thereby made accessible to persons in third countries.[85] Principle 8 therefore does not apply to e-mail addresses on websites.

Finally, regarding electronic addresses as personal data, with the corresponding rules in respect of processing of these data, makes certain software applications which use electronic addresses, subject to data protection rules. These so-called social applications such as Plaxon (automatic address book updater), Friendster (extension of your social network), meetup.com etc. use snowball techniques to verify and gather electronic addresses.

[84] European Court of Jusitice, Case C-101/01, Bodil Lindqvist, 6 November 2003.
[85] Idem

These kinds of applications are based on the principle of exchanging electronic addresses with others, sometimes by means of a database which belongs to a third party. This kind of use is processing within the meaning of the Data Protection Directive and consequently, the principles on data processing apply.[86] This means that it is possible that those applications are not allowed under data protection law unless specific consent is acquired for those forms of processing. Those type of applications are a possible source for harvesters and must also be secured according to Principle 7 on security of processing (Article 17 DPD, see also Chapter 6 on security).

Moreover, the Article 29 Working Party also recalls that e-mail harvesting, i.e., the automatic collection of personal data on public Internet places, e.g. the web, chatrooms etc, is unlawful under the general 95/46/EC Directive.[87] Notably, it constitutes unfair processing of personal data and respects neither the purpose limitation principle (finality) nor the obligation of information mentioned above. This is also the case when automatic collection is performed by software.[88]

[86] Aoun & Rasie 2003

[87] Compare the Dutch case of *Netwise Publications BV vs NTS Computers Technology BV* District Court Rotterdam, 5 December 2002, *Computerrecht 2003/2*, p. 149 in which a company called NTS had 'harvested' the addresses from the website of Netwise. That website contains a publicly accessible directory of e-mail addresses. Visitors to the website can fill in their (e-mail) address on the site themselves. Anybody can search the directory by name and also, or alternatively, by place. At the same time Netwise had installed some technical security devices, providing a limit to the number of e-mail addresses that one can collect from the directory. Despite this, NTS had succeeded in collecting vast numbers of e-mail addresses from the directory, to which addresses they subsequently sent vast quantities of e-mail advertisements.
The Rotterdam District Court granted an injunction ordering NTS to stop collecting e-mail addresses from the Netwise directory. An important consideration was that all users of Netwise had been the guarantee that their data would not be used for spam. The general conditions of Netwise contain a full restriction on spam. In its defence NTS argued that that restriction was invalid because the general conditions had not been properly declared applicable, for nowhere on the website were visitors specifically asked to confirm acceptance of the general conditions. However, the Court decided that in the circumstances such (confirmation of) acceptance was not necessary. It held that a professional visitor of websites, like NTS, should be expected to understand that Netwise would attach such conditions - which the visitor can easily find and inspect - to the use of the directory. Furthermore, so the Court held, NTS should be expected to know that managers of e-mail files usually do not want 'harvesting' and spamming.

[88] Article 29 Working Party 2004.

5 Implementation and enforcement

5.1 Implementation

The implementation of the E-Privacy Directive by Member States will be reviewed by the European Commission in 2006, ex Article 18 of the Directive. This means that the Commission will be monitoring national transposition measures ever since the implementation deadline. In this Chapter, we will not provide an overview of implementation in all Member States but rather make a few general remarks on the implementation process.

A number of EU Member States already had an opt-in system in their national law before the Directive.[89] Others are now implementing an opt-in system. These include Austria, Denmark, Finland, Germany, Italy and Spain. Others are in varying stages of implementation. As the implementation deadline has passed on October 31st 2003, the European Commission has announced infringement procedures against nine Member States that are late in implementing the Directive. On April 1st 2004, the Commission issued a second warning against eight Member States for still not having implemented the E-Privacy Directive.

The E-Privacy Directive was required to be transposed by the Member States before 31 October 2003. It effectively replaced the ISDN Privacy Directive as from that date. The European Commission has stated in its 9th Implementation Report of the telecommunications package that the E-Privacy Directive constitutes a vital element in the new framework and that it therefore will carefully monitor whether its key concepts are properly transposed in national transposition measures.[90] The Commission also explicitly states that, even though the Directive introduced an exception to the general opt-in rule for spam in Article 13 (2) concerning direct marketing of a company's own similar products, if such an exception is transposed into national law it should be strictly drawn up so as not to undermine the general opt-in rule.[91]

Also, effective and timely enforcement will be essential to ensure a real protection of subscribers. Therefore the Commission demands that real and serious sanctions are introduced in the event of breach of the relevant rules. Those sanctions must include financial penalties where necessary. That implies that the responsible authorities must have the proper powers of investigation and enforcement.[92]

Even though a number of Member States have been very slow to implement the Directive, we can already see a few trends in the choices they have made or are about to make. A very important area of divergence in implementing the Directive is the protection of corporate interests as provided for in Article 13 (5) of the Directive. The Netherlands, the UK and France have for example made the choice not to put in place an opt- in regime that protects corporate subscribers. In Italy and Sweden, however, opt-in is also required for sending e-mails to corporate accounts and therefore employees are also protected against receiving unsolicited communications at their workplace.

This section is based in part on the thorough report for the Computer Law Association by Elisabeth Thole, of Van Doorne Lawyers.

[90] 9th Implementation report, p. 39.

[91] 9th Implementation report, p. 40.

[92] 9th Implementation report, p. 40.

Germany also requires opt-in from corporate users but is quicker to accept implied consent in the case of corporate users, than when private individuals are concerned.

The use of e-mail opt-out registers also differs between Member States. As mentioned above, the Electronic Commerce Directive introduced the explicit possibility of opt-out registers. The UK and the Netherlands did not put e-mail registers in place. Sweden did not bother to do so either while Belgium and France have provided for e-mail opt-out registers.

The most important implementation differences however can be seen when judging the enforcement mechanisms put in place by the several Member States. Both in terms of choice of authority and in terms of choice of method of enforcement, serious differences appear between Member States. All Member States will put in place the possibility of fines as an enforcement tool. The maximum penalty for spammers differs between states. For example, in the Netherlands to break the anti-spam law is not a criminal offence in most cases while in Italy breach of the law may be punished by imprisonment. In Italy, it is also possible that the provider is ordered to implement technical measures to stop spamming.

Even where comparable ways of implementing have been chosen by Member States, the practical meaning of new laws can differ enormously because of differences in interpretation methods or differences in other national law aspects such as the division of the burden of proof.

5.2 Enforcement

In what way will the E-Privacy Directive be enforced? When considering new legislation on any topic, it is relevant to take a look at enforcement mechanisms in place. In this Chapter, we will make a few remarks on that difficult topic. Note that enforcement mechanisms are mainly a matter of national (Member State) law and that it is therefore not possible to make far-reaching statements on pan-European enforcement. Enforcement can be hindered *inter alia* by a lack of cost effectiveness, by difficulties in tracking spammers, difficulties in collecting evidence and by differences in regulation between Member States.[93] Sometimes existing privacy legislation can also cause obstacles to effective law enforcement.

Recital 47 (of the E-Privacy Directive) urges Member States to provide for judicial remedies where the rights of users and subscribers are not respected. Recital 47 further states that penalties should be imposed on any person, whether governed by private or by public law, who fails to comply with the national measures taken under the E-Privacy Directive.

According to Article 15(2) the provisions of the Data Protection Directive on judicial remedies, liability and sanctions shall apply with regard to national provisions adopted pursuant to the E-Privacy Directive and with regard to the individual rights derived from this Directive. Article 15(3) states that the Article 29 Working Party on the Protection of Individuals with regard to the Processing of Personal Data, shall also carry out the tasks laid down in Article 30 of the Data Protection Directive applicable with regard to matters covered by the E-Privacy Directive, namely the protection of fundamental rights and freedoms of legitimate interests in the electronic communications sector.

[93] OECD 2004.

Member States can choose to introduce penalties through civil, penal or administrative law. Because Recital 47 refers to 'judicial remedies', it will not be possible to rely solely on co-regulation or self-regulation. There has to be a final say by a court, be it a civil, penal or administrative court. Before turning to the different remedial options, we will first look at the problem of jurisdiction. Enforcing rules is not possible when the spammer hides away in a country that is not very engaged in the fight against spam.

5.3 Cross-border enforcement

A lot of spam originates from outside the EU. Much of the spam received in Europe originates from America, Africa or Asia. To enforce European anti-spam legislation outside the EU is problematic for a number of reasons. However, some of these difficulties also apply to enforcement of national legislation, in which the European rules are transposed. Member States have a lot of discretion regarding the implementation of the rules of the E-Privacy Directive. Therefore, the obligations of spammers, recipients and intermediaries, as well as the related penalties, will differ within the European Union. Because of the EEX Treaty on cross-border enforcement it is easier to trace, try and enforce penalties on European offenders, than to pursue offenders from outside the EU.[94] The level of difficulty of enforcing penalties on offenders from outside the EU depends inter alia on what treaties regarding cross-border enforcement exist, and on the cooperation of the other nation(s) involved.

The law on cross-border enforcement, i.e. private international law, consists of rules with respect to jurisdiction, applicable law and execution of the penalty. International private law is national law, even though it partly derives from international or European treaties.

In case of cross-border law enforcement, it first must be established in which country a case can be brought to court, before the applicable law or the way of executing the penalty can be assessed. Jurisdiction is derived from the applicable international or European treaties or from national rules of international private law. Both treaties and national legislation have exceptions on the general rules for certain kinds of cases, such as tort law or contract law cases.

In general, a case must be brought before a court of the country of residence of the defendant. In the case of tort law, European jurisprudence states that also the court of the place where the damaging fact has occurred can decide on the matter. The place where the damaging fact has occurred can be either the place where the action was initiated (i.e. where the spam run was sent from) or the place where the result of that action occurs.[95] In the case of international spam runs, this could be anywhere in the world. To ground jurisdiction on the country of origin of the spammer could prove problematic, since spammers can locate themselves in spam harbors with no execution or extradition treaties. And even when a country is a party to such treaties, spammers can still move to certain areas within this country where these treaties are more difficult to enforce.

In the United States, Boca Raton, Florida has become a spam center.[96] Jurisdiction which is based on the place of origin of the action is also problematic because it is very easy to put the server from which the spam run is sent in a spam harbor.

[94] 1968 Convention on Jurisdiction and the Enforcement of Judgements in Civil and Commercial Matters (EEX Convention).
[95], ECJ 30 November 1976, case 21/76.
[96] Graham 2003, p. 4.

This leaves the possibility to fix jurisdiction on the place where the result of the action occurs. This means that every country where a spam run has effect can designate a court before which a case against the spammer in question can be tried.

Jurisdiction based on the place where the results of the action occur would be very disadvantageous to E-marketers who wish to send legitimate mail. As long as they limit their marketing campaign to their own country they can probably figure out the relevant rules. However, if they operate internationally it will be hard to find out what is allowed where. Also, with some e-mail addresses like .com, .net or .org e-marketers cannot always establish for certain in which country the recipient is located. Permission marketers should then ask for more than just an e-mail address before they send out mail to potential customers. This will diminish the amount of addresses they will gather, because people do not bother, or do not want, to give out detailed information about themselves.

Once it has been established before which court a case can be tried, that court has to decide what law is applicable and therefore what kind of rules regarding spam apply. Some countries accept a choice of law by contract between civil parties . If an address is acquired in the context of a sale (as referred to in Article 13(2) of the E-Privacy Directive) and the customer opted out, but nevertheless receives e-mail from this company, the choice of law of the contract could also apply to unsolicited e-mail. If no choice of law has been made, the principle of *lex protectionis* may apply. This means that if a case is tried before a court of the country in which the results of the action have taken place, the court can apply the law of this same country. In the case of a spam run, this could mean that a spammer could be tried by a court of a foreign country, under foreign law. If the results of the action did not take place in the same country as that of the court trying the case, the court may use the 'contacts approach' to establish the applicable law. In that case, the law that is most closely connected to the matter has to be applied.[97] This connection can be established for instance by a previous customer relation. It would then depend on the circumstances of that relation which law would apply. The court can also apply the principle of the *lex loci delicti*, the law of the place where the action took place. In that case, it foreseeable that it will be hard to find out for an e-marketer what laws may apply to his actions. E-marketers should adjust marketing material to the national laws of the country of the recipient or to international guidelines on protection of consumers, such as those of the OECD.[98]

5.3.1 Execution

Once there is a court ruling, this ruling has to be executed. There are European and international treaties on execution. However, there are a number of countries that do not participate in execution treaties so even when the spammer is identified and tried before a court, it might be difficult to execute the ruling of that court. Therefore, cooperation with the countries from which a lot of spammers originate, e.g. the United States, is necessary. It might be more productive to have spammers tried in their country of origin than have a pointless verdict.

[97] Trzakowski 2003, p. 5.
[98] Trzakowski 2003, p. 8., see for the OECD Guidelines for Consumer Protection in the Context of Electronic Commerce www.oecd.org.

5.4 Authority

Enforcement is not the responsibility of the same authority in all Member States. In a majority of states, the data protection authority enforces the rules in the first place. In other countries, the national regulatory authority for electronic communications enforces the regulation of unsolicited communications. Also, sometimes more than one authority has to be involved in enforcing the provisions. In some instances, spamming also amounts to fraudulent or misleading practices. In this case the relevant rules would be enforced by consumer protection authorities.

Spamming activities are often linked to data protection infringements such as harvesting, if not cybercrime activities such as illegal intrusion into PCs or servers. The corresponding provisions may not be enforced by the same authorities, let alone across borders.
Except in a few Member States, complaints do not necessarily have to lead to investigations. Pre-complaint contacts are sometimes used, including directions and guidelines to companies, with some success. Sometimes this pre-complaint phase is left to the consumer who should contact the company before filing a complaint. Self-regulation is in place in a number of countries (e.g. the UK) to organize this first phase of action. In some Member States, industry has self-regulatory complaints mechanisms already in place. Authorities also often act on their own initiative. Specific entrustment to an administrative authority would normally not preclude direct access to the judicial system. Not all DPAs (Data Protection Authorities) have the power to act against legal persons. Nor do all DPAs have the possibility to impose sanctions (as yet). These authorities would have to initiate a legal process with the judicial authorities. In France, experience with the e-mailbox has led the DPA to select a few specific cases and refer them to judicial authorities, without much success.

5.5 Sanctions

5.5.1 Civil law

Article 13(1) prohibits direct marketers from sending unsolicited e-mail to natural persons who did not give their prior consent. This provision has direct effect, meaning that even when Member States have not implemented this provision into national law, subscribers can still bring a claim against the spammer under tort law as a breach of a legal requirement, asking for compensation.

If the requirements of Article 13 are transposed into civil legislation the same tort action can be brought. The downsides of civil law actions are the costs, compared to the compensation the complainant will receive for one or a few e-mails sent by one spammer. The costs could be shared with other complainants by means of a class-action or acting through means of an interest group.

5.5.2 Criminal law

Penal sanctions can consist of punitive fines, a prison sentence and alternative sentences such as community work. It will depend on the penal system within the Member States what penalties are available and to what extent.

This means that among those Member States that will choose penal law as a means to sanction spammers, big differences may arise in the severity of the sentences.

The cost-effectiveness argument is one of the reasons why criminal law is often regarded as the last resort in enforcing spam law. Member States can also choose to impose penal sanctions only in respect of certain provisions, e.g. Article 13(4) (of the Data Protection Directive) prohibiting the falsifying of headers and routing information. Hacking computers and/or domains to subsequently send spam runs from them is a criminal offence already in a number of Member States. The Treaty on Cybercrime and the pending Council Framework Decision on Cybercrime (insert references in footnote) also contain provisions regarding this kind of illegal activities.

Government resources might also be used to attack the side-effects of spam. Spamming is only profitable because of the transactions resulting from it. Transactions can be physical or virtual. Physical transactions such as parcel shipment can perhaps be traced and intercepted. Virtual transactions such as electronic money traffic handled by credit card companies, can also be intercepted. As the transactions are obstructed, the incentive to spam diminishes.

If it is not possible to sue the primary offender in the enforcing state, the state may be able to keep the enforcement national by applying joint responsibility for contribution or other kinds of support to the offence. Depending on the offence in question, it may be effective to forbid users to participate in certain acts such as illegal gambling or to impose sanctions on intermediaries who benefit from or support the illegal activity.[99]

5.5.3 Administrative law

In a number of Member States, the choice has been made to enforce the law of electronic communications through administrative law. The advantage of this is that the National Regulatory Authorities (NRAs) are used to enforcing telecommunications law via administrative procedures. Also, a variety of enforcement instruments is available in administrative law. An example is the use of administrative fines.

5.6 Conclusion

This Chapter deals with a number of practical issues surrounding the regulation of unsolicited communications. In order to have a serious impact on the actual proliferation of spam, a lot depends on how new regulations are implemented into national law and how new rules will be enforced throughout the European Union.

In the first place, we have established that Member States have used the full margin they are allowed to choose their own implementation of the E-Privacy Directive. Large differences exist between individual Member States in terms of the scope of protection they decided to offer users as well as in terms of the position of legal persons. A second notable fact is that more than half of all Member States has yet to fully implement the E-Privacy Directive while it should have been transposed into national law by October 31st 2003.

[99] Trzaskoswski

The Commission is displeased with this delay of over half a year and has issued warnings of upcoming infringement procedures against 8 Member States.

The choice of enforcement methods has been left largely up to individual Member States, which in effect means that very different systems have been put in place. Issues like complaints mechanisms, choice of public or administrative law and penalties are dealt with in altogether different ways in a lot of EU Countries. The Commission seems to have realized that this development could threaten the practical effect of the Directive and has stressed the importance of effective enforcement mechanisms in its 2004 Communication. The choice of sanctions to be used against violations of the anti-spam laws also presents significant differences.

Linked to the question of which enforcement mechanism is adopted is the question of who will be responsible for enforcement. The E-Privacy Directive does not specify which authority should be in charge of enforcing spam laws. This means that it is left up to the Member States to decide whether they leave it up to their NRAs or up to their Data Protection Commissioners to enforce the Directive. It is even possible to leave this responsibility with a general consumer protection authority, as is the case in Sweden.

6 Other aspects of the fight against spam

6.1 Introduction

In this Chapter we briefly describe a number of measures that are being taken against spam or that could be taken against spam and we assess their legal consequences. The question we try to answer in this chapter is: what are the alternatives to article 13 of the E-Privacy Directive both technically and legally?

6.1.1 Anti-spam technology

Anti-spam solutions protect and help business, ISPs and individual users to reduce the amount of time spent reading and managing unwanted e-mail by filtering out inappropriate and offensive content. One of the options is the use of filters using "blacklists", which consist of domain names or Internet protocol (IP) addresses of known spammers. Blacklists can be established in a collective way. Once enough recipients in a certain user community object to a particular message, the message is automatically transferred to future users' spam folders. Another technical option, consisting of "white list", or "approved sender lists", allows users to identify e-mail from approved and legitimate senders. While white lists can help refine spam filtering, they are currently prone to spoofing, or falsification of e-mail source data. Another technical tool which has been suggested as having good anti-spam potential is to set one's e-mail client to accept only messages signed with trusted digital certificates issued by a trusted certificate authority. Digital signature schemes such as public key infrastructure solutions can be used for this purpose.

6.1.2 Filtering

The majority of spam-blocking technologies currently use keyword or blacklist blocking, which results in a large number of false positives. False positives occur when a legitimate e-mail is mislabeled as spam and filtered. In addition, anti-spam blacklists sometimes block innocent Internet users connected through blocked ISPs. There have even been cases of entire country domains being blocked. While some users have felt empowered by these filters, many ISPs argue that they have had the effect of blaming the wrong people, including ISPs that host spammers unknowingly, Internet users who may have been spoofed by a spammer, and addresses adjacent to the alleged spammer.

Another approach to spam filtering is the consensus model, whereby people who receive messages that they consider to be spam report them as spam to a coordinating entity. A computer program is then used to co-ordinate all of the input. A properly compiled list of known spammers would also be a significant improvement on unregulated blacklists that currently operate. Nevertheless, perfect filter systems are nearly impossible to deliver.
Many spammers are technologically sophisticated enough to cover their tracks, adjust their systems to slip through filters and scale other technological barriers. They can electronically commandeer unprotected computers, turning them into a tool for their own spamming. As long as spam costs are so low, spammers have a vested interest in finding ways to defy technological limits.

There are numerous technical approaches to try and stop spam, such as filtering and blocking of e-mail, distributed denial of service attacks or tracing a spam outbreak to find and sue the spammer.

Filtering is used in this study as a generic term for all kinds of technical features that aim to keep inboxes free from spam. Those technical measures can operate at a gateway/mail server level or at inbox level. Blocking is a form of filtering at mail server level that does not allow the e-mail to go into the inbox of the individual user. Blocking e-mail is possible in several ways: through the use of black lists, white lists and key word/lexical/heuristic scanning. Black lists block all e-mail coming from specific IP-addresses. They can also block whole servers. Another way to block e-mail is through the use of a white list. A disadvantage of using a white list is that the person who uses such a list cannot be reached by a person whom he did not add to the list. This inconvenience can be tackled by using an additional challenge response filter. When such a filter is used people who are not on the white list but wish to send e-mail to this user anyway, fill out a request form on a web page or in a response email and then are added to the white list. This is convenient to the user, but inconvenient to the people who want to contact this user. [100] Also, some people use different (reply) addresses and have to make sure all those different addresses get white listed.

The downsides to blacklisting are clear as well. First of all, a lot of spam passes the filter that is supposed to block it. It is estimated that filters using blacklists only block 25 to 50% of spam.[101] A weak spot of blacklisting is that it requires human intervention. Unless a domain that is being used by a spammer, is placed on the list, the spam will not be blocked. And since spammers continuously use different domains a lot of spam makes it through the barricades. A second disadvantage of using blacklists is that a lot of legitimate mail is being bounced.

A famous black list is the Realtime Blackhole List (RBL) of the anti-spam group MAPS (Mail Abuse Prevention System). The RBL is a blacklist of servers that are not anti-spam. ISP's can use this list to block e-mail from the servers on the list. However, the question whether an ISP has an active anti-spam policy or not is prone to debate. Aside from that, the RBL of MAPS is based on a definition of spam that takes a double opt-in system as a criterion for legitimate mail. This leaves out e-mail sent by permission marketers which use single opt-in or opt-out schemes, sometimes according to the law of the country they originate from, or according to the law of the country they target. All e-mail from an ISP that is not anti-spam is blocked.[102]

Human intervention renders blacklists also susceptible to fraud. What is easier than having a competitor's domain put on a black list. It is an efficient way to rob people of their ability to communicate and therefore works as a means of obstruction of freedom of expression.[103] However, a responsible and actively kept up to date blacklist might be useful in combination with other ways to fight spam.[104]

Another problem with blocking mail at mail server level is that ISP's may under certain circumstances have an obligation to deliver e-mail sent through their services. This can be a contractual obligation towards their subscribers to send and deliver mail, or an obligation prescribed by law.

[100] Graham 2003, p. 3.
[101] Graham 2003, p.1, Graham 2002a, p.1.
[102] Magee 2003, p.25.
[103] Magee 2003, p.6.
[104] Graham 2003, p.1.

In case of a contractual obligation, spam which is sent through the network of the provider can be excluded from this obligation by contract. Subscribers who still want to send or receive spam can go to an ISP with a more tolerant policy regarding spam.

Aside from blocking, there are numerous other forms of filtering. Graham presents an elaborate description of different ways to fight spam in 'Stopping Spam'.[105] The most complex filtering techniques are rule-based (or heuristic) filtering and Bayesian (or statistical) filtering. While at first these were competing systems, nowadays they are used to complement each other.

Rule-based filters look for specific spam patterns in the text (header and body) of the e-mail, words such as cash, phrases like "try for free!" and malformed headers are give aways for the e-mail likely to be spam. Likely, because although a good heuristic filter can stop 90-95% of spam, it can also refuse up to 5% of legitimate mail. Also, since spammers use different patterns all the time, the programs of rule-based filters have to be rewritten constantly, resulting in expensive updates of anti-spam software. However, since rule-based filters can operate at mail server level, individual users do not necessarily have to switch to new version themselves all the time. However, the subscribers might still pay for the costs ISP's make on their behalf. The negative aspect of rule based/heuristic filtering technologies is that they are normally extremely ineffective against Spam that is not in English.

Bayesian filters also look at words used in e-mails. Bayesian filters compare two lists, a list of legitimate e-mail and a spam list, that are kept by the user, and, based on those lists, add a probability for words to be used in spam or legitimate e-mail. Bayesian filters learn through time and therefore work better the longer they are used, if both lists are being kept up to date. That is also one of the weak spots of Bayesian filtering, they require maintenance and are much harder, though not impossible, to operate at mail server level by an ISP.[106] The main negative aspects of Bayesian filters is the fact that they tend to lack in accuracy and that cannot filter text which has been included into a GIF type of photo format. The weighting of Bayesian filters is often times easily tricked when spammers include a listing of "non-spam" words in white text in their emails, to throw off the weighting system of the Bayesian filter.

Additional anti-spam technologies include Spam Outbreak technologies that are trying to be identify and protect users the moment a bulk spam message is launched to all of the recipients. These type of technologies offer real time service center communications and are focused not on the content of a spam message but on recurrent patterns that are found in a specific spam message. Not being content based means that detection rates are equally as good in English as in other languages. As spam has proven to become a cost and nuisance to many, there are many technology providers that are studying new technologies as to how best to deal with identifying a spam message and also to authenticate a sender is who they say they are.

Most anti-spam software use a combination of filtering techniques to combat spam.[107] This will keep out the average spammer, but will not be sufficient to

[105] Graham 2003.
[106] Graham 2003, p.2-3.
[107] The free open software program SpamAsassin uses a variety of techniques to filter spam: header analysis, text analysis, blacklists and signature-based filtering. See: http://au2.spamassassin.org/index.html

scare off the most technologically proficient spammers. Filtering will therefore in itself in all likelihood not eliminate the spam problem, but merely contain it.[108]

In our opinion, ISP's should let their subscribers decide whether they want their e-mail to be filtered or not, and in what way. Even, if it is necessary to filter e-mail (also) at mail server level, subscribers should be made aware of this and of the possible results of the kind of filtering that is used, such as the blocking of mail altogether or the filing of suspicious e-mails in a spam folder. In this manner e-mail users stay in control of their communications. Therefore users should have the option of using custom-made instead of ready made filters. ISP's should provide users with friendly software, or information on it, and help out with the settings of this software at user level since the ISP's benefit from a reduction of spam just as much. Ideally users can define what is spam to them, not someone on the server level only ISP's also filter e-mail for viruses. As the overlap between spam and virus mail grows, education and information on the uses of virus filters gets more important.

6.2 Legal alternatives: trespass

As spam poses substantial costs, especially to ISP's, some American providers have sought to protect their interest by suing spammers for trespass to chattels and they have sought injunctive relief to protect their property.

Trespass to chattels is a tort action based on the unauthorized use or interference with another's property. For the claim to be upheld, there must be some kind of damage, debilitation or removal of that property. But does this rule make sense in a virtual world with intangible property? In American case law, the foremost problem had been that trespass to chattel necessarily had to do with interference with or use of tangible property of another.

In a number of recent American cases the theory that bulk e-mail amounts to trespass to chattel has been upheld.[109] However, some authors warn that side effects of such a development could prove detrimental to commons on the web. The endpoint to such a theory may be that a rights of use theory could develop that would scare anybody away who tries to reach an audience through internet.[110]

In it's decision of 12 March, 2004, the Dutch Supreme Court accepted a trespassed based claim of a provider to refuse spam traffic on its network.[111] According to the Supreme Court, the ISP had an exclusive property right to its network and the fact that the spammer used that network for sending out unsolicited communications amounted to an unlawful act towards the provider. Of course tort law differs largely between Member States, but the case could be followed by similar cases in other Member States, based on the claim hat providers have an exclusive right to their networks and can therefore prevent unauthorized use of those systems.

The mirror image of the right of ISP's to refuse spam traffic is the possibility of a

[108] Magee 2003, p. 25.
[109] A well known case is Intel versus Hamidi in which lower courts decided that junkmailer Hamidi trespassed the property of Interl. The California Supreme Court eventually sided with Hamidi and decided there was no trespass in this case. California Supreme Court 30 June 2003, *Intel v Hamidi,* S103781.
[110] Burke 1998, p. 31.
[111] Supreme Court of the Netherlands 12 March, 2004 (*xs4all v Abfab*).

legal obligation for ISP's to filter out spam. In Chapter 2, we have discussed the obligation of network and service providers to take appropriate measures in order to safeguard the security of their network and services. Under certain circumstances, it is conceivable that an end user may hold his ISP liable for not taking appropriate measures to protect him from unsolicited communications.

Another, more pragmatic approach to the spam problem could be to go after the vendors that profit from spam. If for example legitimate businesses see an increase of sales as a result of unsolicited communications it seems fair that they should be required to prove that they were not aware of the illegal advertising campaign and otherwise should be held liable for the damage inflicted on both ISP's and end users.

6.3 Fraud and deception

Fraudulent or deceptive spam can be targeted by criminal law. Fraud of a more serious kind is also very common in spam. Nigerian spammers pose a notorious example as they have stolen millions ofdollars from people which believed their claims. According to the OECD Background Paper, "the US Secret Service has designated this type of spam scam as an "epidemic" and claims that losses amount to hundreds of millions of dollars annually".[112] Several kinds of pyramid schemes and "get rich fast" tricks are floating in mailboxes. But a number of phenomenal diet or body improvement advertisements seem as misleading as anything.

6.4 Unsolicited pornographic or racist email

A special category of spam content to be discussed here is Unsolicited Pornographic Email (UPE). Spam messages containing pornographic photographs, and promoting adult entertainment products and services are deemed inappropriate for children. Since many spammers do not target specific recipients, young children are likely to be inadvertently exposed to pornographic or offensive messages. But aside from children, employees could have a right to be protected against pornographic email in their workplace.[113]

Under US Law, it is clear that pornographic email leaves companies vulnerable to charges of creating a "hostile work environment,'' and all the associated liabilities that implies. Already, employers have been found directly and indirectly liable under these rules for failure to protect their employees from offensive imagery, and failing to monitor and prevent inappropriate use of email when notified by employees of the problem.[114]

Is it conceivable that European employers could also be held liable for not protecting their employees against unsolicited pornographic or racist spam? In Europe, employers have an obligation to protect their employees from discrimination in the workplace. One indication can be found in Directive 76/207/EC as amended on 23 September 2002. In April, 2002, the European parliament issued a binding resolution addressed at member states to develop their own national frameworks for interpreting and enforcing a new sexual harassment law. The concept of employment discrimination is expanding up to a level where the possibility of sexual harassment could also amount to employer liability for unsolicited pornographic email.[115] Employers may also be vicariously liable for email misuse by their employees, including spamming.

6.5 Self/Co-regulation

There are a variety of ongoing self-regulatory efforts in place to reduce spam. Even though a self-regulatory approach may contribute considerably to the fight against spam, a number of restrictions are clear. First of all, self-regulation will by definition mainly address organized or official direct marketeers.

[112] OECD 2004.
[113] OECD 2004.
[114] Compare for example Blakey v. Continental Airlines, Inc., Supreme Court Of New Jersey, 164 N.J. 38; 751 A.2d 538 (2000).
[115] Waddington & Hendriks 2002.

"Bad Spammers" will not follow rules of self-regulation and will therefore break through any protection against spam offered by self-regulation. It remains very easy for those bad spammers to use false identities, ever changing locations and new techniques to avert filtering software.[116]

6.6 Consumer awareness

The European commission explicitly pays attention to consumer education and awareness as an important step to decrease spam. Increasing awareness of users of the risk of leaving e-mail addresses on numerous websites is indeed a first step to prevent address harvesting. At the same time, that would make it harder and more costly for spammers to obtain those addresses. Plus, the effects of consumer awareness are not limited to spam coming from Member States of the European Union. If people are more careful about their email addresses that would also give them a certain protection against spammers from third countries.

The European Commission is planning to provide consumer information on its website, Member States' regulation, links to national sites, and figures and trends on spam in the EU in the near future.[117] Also, the Commission has developed the so called Safer Internet Action Plan to promote awareness-raising activities in Member States for the safe use of the Internet.

6.7 Conclusions

In this Chapter, we have discussed a number of other aspects that are relevant in the attempts to regulate spam. First of all we paid some attention to technological measures that can be taken against spam. Anti-spam technology offers practical protection against at least a large quantity of spam messages. However, we have also pointed out the inherent risks of trusting technology to solve this problem. Both false positives –unjustly blocked messages – and false negatives –spam messages slipping through - can cause serious problems. It is important that users of anti-spam technology are aware of those inherent risks in order to prevent the damage which can be caused by important messages being blocked without justification.

Once again it is interesting to look at the specific responsibility of the Internet Service Provider. Technical solutions can be implemented either at the user level or at higher levels in the network. Employers often offer spam filtering on their corporations' networks. For users which are natural persons the most likely provider of filtering services however would be their ISP. It is for a large part a matter of contract law between user and ISP whether any obligation could exist to filter spam (except for possible obligations under the security provision of the E-Privacy Directive as discussed in Chapter 5)

Besides technological solutions, we briefly discussed some legal alternatives outside the present spam regulation that is the core subject of our research. The property based claim of trespass to chattel, to be brought by network owners has proven successful in some anti-spam cases both in the US and in the EU. Also, some spam may be targeted by criminal law for being deceptive and fraudulent.

[116] OECD 2004.
[117] OECD 2004.

The infamous example of the Nigerian scammers proves that outside the electronic communications framework, classic criminal law still applies to this kind of offences committed through sending unsolicited communications.

A specific remark has been made about the position of employers when it comes to spam. We have argued that it is important that employers are aware of potential risks of liability arising out of their failure to protect employees from unsolicited pornographic e-mail. In the US, it has been argued that failing to protect employees against these kinds of messages could contribute to a hostile work environment. European law suggests that the same reasoning could apply in a European context. Apart from binding legal rules, some see a complementing role for self- or co regulation. We do not believe that self-regulation will be the panacea to all spam problems, mostly because self-regulation does not tend to bind 'bad spammers.' Finally, the importance of consumer awareness has been stressed by the European Commission. We think that this is indeed an important aspect because lack of consumer awareness makes it very easy for spammers to keep collecting fresh and working e-mail addresses.

7 Conclusions and recommendations

7.1 Main conclusions

We have seen that spam poses a very complex problem to internet users, regulators and businesses. Therefore the solution to spam is not likely to be a simple one. A one-size-fits-all approach is not going to solve it.

The complexity of the spam issue is governed by its international dimension, the various opposite (fundamental right) interests of the actors involved, the lack of a single clear definition of spam and the present inadequacy of technological solutions.

The fight against spam represents a collision of the fundamental rights of spammer, recipients of spam and providers. We have called this clash of fundamental rights the spam triangle, because the relationship between spammer, provider and user can be seen as a triangular one, with the provider in the middle. On the one hand, we have seen that, although commercial communication in principle is protected by freedom of speech, freedom of speech does not grant the spammer a very strong claim against either provider or recipient. On the other hand, however, the recipient can claim both infringements on his relational privacy and on his informational privacy. The provider can claim ownership rights.

Informational privacy is protected by data protection law. It has been argued that the collecting via harvesting on the Internet and use of e-mail addresses without the users' consent would amount to an infringement on the Data Protection Directive. Even though it is hard to make a general statement on the legality of the collecting and use of e-mail addresses for spam purposes, it seems clear that large scale harvesting does amount to an infringement of at least some rights of data protection of users.

The 2003 E-Privacy Directive tries to contribute to an effective solution to the spam problem by regulating unsolicited communications for direct marketing purposes. It can be seen as an important first step in the fight against spam. The EU has chosen a pan European opt-in rule as the norm throughout the EU. Although it remains to be seen how effective this opt-in regime will be in practice, it is clear that the pan European approach will have an important symbolic meaning in the international fight against spam. It is the first international norm with regard to spam. As such it will be the point of departure for spam initiatives on other forums. Next to that, the EU's initiative will be an important signal to all actors involved in the spam issue: the spammers, those who use spammers to advertise their goods or services, providers and Internet users.

In this report we have analyzed the object and scope of Article 13 of the E-Privacy Directive. We have seen that the opt-in rule in Article 13(1) could in theory have a broad applicability, because of the open definition of email. Article 13(1) applies to users being natural persons in their capacity of subscribers. We have seen that outside that scope there is a possibility to choose between opt-in and opt-out for Member States. Article 13(2) introduces the possibility for continued direct marketing to existing customers for similar products. We have established that the wording of that second section leaves room for a myriad of interpretations.

Article 13(3) of the E-Privacy Directive provides protection in respect of the rest category. Unsolicited communications for direct marketing purposes that are not covered by the first two sections are covered by this section. This means that some of the newer forms of unsolicited communications such as pop-ups and SPIM are covered by this section and that Member States are under the obligation to provide some sort of protection against those unsolicited communication by choosing either an opt-in or an opt-out regime. Section 13(5) obliges Member States to provide protection for the legitimate interests of subscribers which are not natural persons.

We have seen that the meaning of this discrepancy between Article 13(1) and Article 13(5) will in practice largely depend on the national law division of the burden of proof. If the spammer carries the burden of proof to provide evidence that the recipient is not a natural person that would render it very risky to keep sending spam to corporate users also.

The practice of sending emails with false return addresses or using disguised or false identities is explicitly targeted in Article 13(4). That section requires Member States to prohibit the practice of sending electronic mail for purposes of direct marketing disguising or concealing the identity of the sender on whose behalf the communication is made, or without a valid address to which the recipient may send a request that such communications cease.

An important limitation on the effectiveness of the E-Privacy Directive is the simple fact that most spam originates from outside the EU. We have seen how the opt-in regime is rendered meaningless when it comes to spam from so-called third countries. The OECD initiative to discuss the fight against spam with both the EU and the US, as well as with other countries is an important development.

Beyond that, the effectiveness of the E-Privacy Directive depends on its implementation in national legislation. So far, implementation of the E-Privacy Directive has been rather slow in a number of countries. Twice the Commission has issued a warning that infringement procedures are to be expected if Member States do not comply with the Directive soon. A direct consequence is that it is hard to get a complete picture of the choices Member States have made in the implementation process.

One thing is clear. Member States have used every discretionary competence they had to provide for their own arrangements under the Directive. This means for example that the protection of corporate users and of users which are not subscribers will largely differ within the EU. Other differences will arise, because the Directive leaves the interpretation of a number of relevant aspects to national law, national courts and national regulatory authorities. Finally, a number of questions that could arise from new anti-spam law belong to the domain of civil law which is left largely unharmonized within the EU.

In terms of the effectiveness of the new European regime, a lot depends on whether effective enforcement mechanisms are put in place. It is for that reason that the European Commission has stressed in its 2004 Communication on spam that Member States should work on effective enforcement and accessible complaint mechanisms. The general picture is that differences between Member States are large both with respect to the practical enforcement of new spam legislation and with respect to the choice of law. Also, the question of who is to enforce the Directive is answered differently in different countries.

In some Member States, the Data Protection Commissioner is in charge of enforcement, while in other countries this is a responsibility of the National Regulatory Authority. In Sweden, enforcement is left up to the Consumer Protection Authority. In practice, it is to be expected that cross border complaints will be a big obstacle to effective enforcement in the years to come.

We have seen that the legal approach to spam must be complemented with other measures, most notably technological measures and consumer awareness programs. The risks of false positives and false negatives should however not be underestimated and warrant further analysis. Consumer awareness is an important way to protect users but is not the panacea to spam either. Besides the new regulatory approach to spam, consumers and businesses can still use other parts of the law to fight spam. Trespass to chattel can be a ground for providers to refuse spammers access to their networks. Civil law tort could be relevant in some user-spammer cases. In some instances, it could also be viable to address the vendors which use spammers to sell their products.

Furthermore, employers must be made aware of the risk of new computer related liabilities. An important example of a potential new liability is the risk of being held accountable for not sufficiently protecting employees against unsolicited pornographic e-mail. American case law shows that these lawsuits can be a dangerous reality and it is something employers should be aware of. Besides that, liability could arise out of behavior of employees such as for example sending out unsolicited e-mail. Another risk is connected to the technological measures taken against spam. There is always a certain risk that due to false positives good e-mails are not delivered which of course can cause harm. However, an obvious risk posed by spam to companies is without a doubt the loss of productivity and the increased bandwidth cost involved.

A development with serious security implications is the convergence of spam and viruses. The E-Privacy Directive addresses security issues and requires appropriate measures to be taken by providers. This does not introduce a strong right for users to object to their providers about letting through spam. Under certain circumstances, tort law or contract law could oblige providers to take measures against spam and viruses, such as filtering. A duty to act could be reasonable as soon as the access to either network or services is threatened due to spam and viruses. ISP's should inform their customers about their spam policy and possibly about the technological solutions available

7.2 Recommendations

- The EU should consider additional actions in order to promote effective enforcement mechanisms.

As soon as the E-Privacy Directive has been implemented in all EU countries, the European Commission should start monitoring its effects and focus on the enforcement of Article 13. We expect that additional measures are necessary in order to achieve effective enforcement throughout the EU.

- Further guidelines should be given as to the correct interpretation of a number of key elements in Article 13.

The correct interpretation of a number of key elements of Article 13 is too important to the fight against spam that a further Communication is needed to give guidance.

Especially the continued confusion about Article 13 (2) shows the need for a harmonized interpretation

- Further cooperation between NRA's and Data Protection Commissioners is desirable.

In order to provide effective enforcement, accessible complaint mechanisms are needed. The probability of European cross border spam complaints requires the responsible authorities to cooperate. Transparent complaint mechanisms for consumers are needed.

- International cooperation should be intensified.

The success of the EU regulation depends in large part of its practical effect on consumers inboxes. Therefore, the proliferation of third country spam must also be stopped. International cooperation is very important to achieve this.

- Consumer awareness should be promoted at the national level.

It is very important that consumers are aware of the new European rules, of the risks with regard to spam and of the possibilities to stop it. Awareness also includes knowing where to file a complaint. Also, it is important that users know not to opt-out to certain illegitimate spam messages. This is typically a matter that should be directed at the national level.

- The responsibility of users with regard to the security of their computers should be defined at the national level.

Users must be aware of the fact that their computer too could turn into a spam machine if backdoors are left wide open. It is important to stress that everybody has a responsibility in stopping spam.

- Stopping email address harvesting should be an objective.

Making it harder to collect email addresses should be part of a concerted effort to fight spam.

- The development of technological solutions will be important and should be brought to the attention of market players and consumers.

The only solution to spam is a combined effort of legal, educational and technological measures. It is important that users and corporations are aware of the possibilities technology offers but also of the inherent risks of those technologies as false positives and false negatives are likely to happen.

- Businesses should be made aware of the risks spam poses not only in terms of costs and productivity loss but also in terms of possible liabilities.

The offensive nature of some spam messages renders it important to take measures to protect employees against those messages. Also, liability could exist for an employee sending out spam from a company machine.

- ISP's should adopt further measures to protect their customers against spam or at least inform them about the possibilities to fight spam.

The responsibility of ISP's with regard to providing security remain largely undefined. However, as spam and viruses sometimes converge into "V-spam" ISP's should inform their customers about the related risks and perhaps about the possibilities to protect oneself against spam. The role of the provider in the fight against spam and viruses should be debated at the EU level.

8 References

Aoun & Rasie 2003

Frederic Aoun & Bruno Rasie, 'Do social applications pose a threat?', available at: http://www.halte-au-spam.com.

Article 29 Working Party 2004

Article 29 Working Party, Opinion 5/2004 on unsolicited communications for marketing purposes under Article 13 of Directive 2002/58/EC, adopted 27 February, 2004

Butler 2003

Mike Butler, 'Spam, the meat of the problem', *Computer Law and Security Report Vol. 19 no.5 2003*, Elsevier Ltd.

Charlesworth 2003

Andrew Charlesworth, 'Information privacy law I the European Union: e pluribus unum or ex uno plures?, *Hastings Law Journal April 2003*.

Chavannes 2003

Remy Chavannes, 'Spam: abonnees, ontvangers en de kracht van de bestuurlijke boete' ('Spam: subscribers, recipients and administrative sanctions, unauthorized translation'), *Mediaforum 2003-11/12,* p. 357.

Cohen & Hiller 2003

Ronnie Cohen & Jamie S. Miller, 'Towards a theory of cyber place: a proposal for a new legal framework', *Richmond Journal of Law & Technology 2003-10/2.*

Communication 2004

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on unsolicited commercial communications or 'spam', Brussels 22 January 2004, COM (2004) 28 final.

Fisher 2000

Michael A. Fisher, 'The right to spam? Regulating electronic junk mail', *Columbia VLA Journal of Law & Arts 363 (2000)*.

Gauthronet & Drouard, 2001

Serge Gauthronet & Etienne Drouard, 'Unsolicited Commercial communications and Data Protection', January 2001, available at: http://europa.eu.int/comm/internal_market/privacy/docs/studies/spamstudy_en.pdf.

Geisler 2001

R.J. Geisler, 'Whether 'Anti-Spam' Laws Violate The First Amendment', *Journal of Online Law*, 2001, art. 8.

Graham 2002a

Paul Graham, '"Filters vs Blacklists', available at: http://www.paulgraham.com/falsepositives.html.

Graham 2002b

Paul Graham, 'Will filters kill spam?', available at: http://www.paulgraham.com/wfks.html.

Graham 2003

Paul Graham, 'Stopping spam', available at: http://www.paulgraham.com/stopspam.html.

Kabel 2003a

Jan Kabel, 'Spam: A Terminal Threat to ISPs? The legal position of ISPs concerning their Anti-Spam Policies in the EU after the Privacy & Telecom Directive', *Computer Law Review International,* 2003-1, pp. 6-10.

Kabel 2003b

Jan Kabel, 'Swings on the Horizontal. The search for Consistency in European Advertising law', *Iris Plus* 2003-8, p. 2-8. Available at: http://www.ivir.nl/publications/kabel/swings.pdf.

Kabel 2002

Jan Kabel, 'Reclamerecht online, problemen in theorie en praktijk', (advertisment law online, problems in theory and practice, unauthorized translation), available at: http://www.ivir.nl/publicaties/kabel/reclamerecht_online.pdf.

Kabel 2000a

Jan Kabel, Commercial communications', in: *Study on Consumer Law and the Information Society*, Amsterdam: PriceWaterHouseCoopers (2000), p. 22-38.

Kabel 2000b

Jan Kabel, 'Commerciële uitingen' (Commercial expression, unauthorized translation), in: F. Grosheide (red.), Hoofdstukken Communicatie & Mediarecht, Nijmegen: *Ars Aequi Libri 2000*, p. 269-270.

Kabel 2000c

Jan Kabel, 'Analysis of the existing European Law on the commercial communications in the light of the new conditions created by the Information Society', *chapter A of Final Report Study on Consumer Law and the Information Society*, p.1-15.

Kelin 2001

Sabra-Anne Kelin, 'State Regulation of unsolicited commercial e-mail', *Berkeley Technology Law Journal 2001,* p. 435.

Khong 2000

Wye-Keen Khong , Regulating spam on the internet, 15th BILETA Conference: "Electronic datasets and access to legal information", April 14, 2000. Available at: http://www.bileta.ac.uk/00papers/khong.html.

Kuilwijk 2000

Kees Jan Kuilwijk, 'Recent developments in E.U. privacy protection regulation', *international trade law and regulation 2000, 6(6), 200-206).*

Magee 2003

John Magee, 'The law regulating unsolicited commercial e-mail: An international perspective', *19 Santa Clara Computer & High Technology Law Journal 333, May 2003.*

OECD 2004

OECD, Directorate for science, technology and industry, Committee for information, computer and communications policy, "background paper for the OECD workshop on spam", 22 January 2004.

Owen & Kiernan Earl 2003

Mark Owen & Elizabeth Kiernan Earl, Data Protection the European Way: a discussion of the legislative framework adopted in the European Union, *Sedona Conference Journal Fall 2003.*

Schaub 2002

M.Y. Schaub, "Unsolicited email, 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, pp. 99-105.

Schiefelbine 2003

Erich D. Schiefelbine, 'Stopping a Trojan Horse: challenging pop-up advertisements and embedded software schemes on the internet through unfair competition laws', *Santa Clara Computer and High Technology Law Journal, May 2003*.

Siebecker 2003

Miacheal R. Siebecker, 'Cookies and the common law: are internet advertisers trespassing at our computers?', *Southern California Law Review, May 2003*, p. 893.

Sola Pool, de

I. de Sola Pool, *Technologies of Freedom*, Cambridge (MA): Harvard University Press, 1983.

Sorkin 2001

David E. Sorkin, 'Technical and Legal Approaches to Unsolicited Electronic Mail', *35 U.S.F. Law Review 325-2001,* pp. 325-384.

Thole 2003

E.P.M. Thole, *SPAM from the European Union Perspective*, Report to the CLA Munich Conference, 13-14 November, 2003.

Trzaskowski 2003

Jan Trzaskowski, 'Cross-Border Law Enforcement in the Information Society' available at: http://www.legalriskmanagement.artscape.dk/uploads/Artikler/Julebog2003.pdf