Max W. MOSING

SPAMMING IN THE EU

Solutions for Unsolicited Electronic Mail Ahead ?

January

[1]

… OR …

[2]

1. Introduction

"Is that spam?".[3] Few Internet users will be unaware of the background to this question: Unsolicited or Junk Electronic Mail – "[…] spam […] THAT evil"[4] of the Internet. Wherever there is evil there are media, politicians and lawyers trying to ban it – so there are intentions to ban spam. In particular, online-newspapers have been crowded with articles about spamming[5] but also several lawyers across the globe have published their legal thoughts about unsolicited e-mails in law journals and on the Internet and even actions have been raised. Several states have passed laws against spamming and the

[1] Graphic: http://www.spam.com (12/10/2002).
[2] Graphic: http://www.matterform.com/about/welcome/anti-spam.gif (12/10/2002).
[3] These questions were raised several times in the itllm@lists.law.strath.ac.uk -mailing list in the last months.
[4] Commentator on slashdot.org, cited in Michael Jacobs / David Naylor / Megan Auchincloss / David Melaugh, "Spam Wars", IT Law Today (ITLT) 2002, 10.4(19).
[5] The search for "spamming" at www.google.co.uk leads to about 859,000 results (done at 18th Dec 2002).

European Union (EU) is trying to address the "spam problem".[6] However, most research and articles focus on national laws or political views rather than on a global approach to the issues of spam and the technical background to communication networks. Furthermore the Directive 2002/58/EC on privacy and electronic communications (E-Communications Directive)[7] will lead to new regulations on spamming in the EU-Member-States but will also raise new issues.

The aim of this work is to give a brief overview of the history of spamming and the damages it causes; questions about the technical background and the need for regulation will be raised and possible solutions of the EU with brief excurses on existing laws in the Member-States will be presented. Finally, one question is inescapable: Are these regulations effective enough to ban spamming? Can these regulations handle new (annoying and costly for the recipient) measures of direct marketing?

Because of the wide definition of spamming, as it is used in this work, the evaluation of illegal content of spamming (scam, fraud, racism, and other illegal matters) is not a part of this paper.

[6] Details will be described in following parts.
[7] 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 (Directive on privacy and electronic communications), Official Journal L 2002/201, 37.

2. "Spamming"

2.1. History and Definition

In the Internet a lot of rumours are afloat[8] - one concerns the history of the notion "spamming": "SPAM" is a trade mark for a canned meat product from Hormel Foods.[9] In a sketch of *Monty Python's Flying Circus*, a British comedy TV-show, the word "SPAM" is repeated to the point of absurdity in a restaurant menu.[10] It is said that this sketch inspired a user from the MUD/MUSH[11] community to assign a keyboard macro to the line, "SPAM SPAM SPAM …" and to send it to the MUD once every couple of seconds – and "spamming" was born.[12] A less moving interpretation is that spam could stand for "send phenomenal amounts of mail". However, the first economic spam was sent – funny enough – by a US attorney couple, Lawrence Canter and Martha Siegel, in April 1994:[13] They posted identical "green card" advertisements to every newsgroup they could locate. The Internet community fought back: Hackers tried to knock down their server and angry newsgroup-members attacked their e-mail-server with hundreds of senseless e-mails,[14] a measure called "flaming".[15] Although there was no rule or law against spamming the community found a way to punish the spammers – but meanwhile the "face of the Internet-community" has changed and these measures against spammers are not effective anymore.

Though spamming was originally not an issue of e-mail it has become the terminus technicus for "[…] the bulk-mailing, sometimes repeatedly, of unsolicited e-mail messages, usually of a commercial nature, to individuals with whom the mailer has had no previous contact […]".[16] The term is not used in a consistent way; some point out, that spamming is "[…] the sending of unsolicited e-mail for the purpose of commercial

[8] There is still the rumour that John Postel, the "father" of the Domain-Name-System (DNS) did not die a natural death; that the management of the company "Pretty Good Privacy (PGP)" are (Ex-)CIA-Agents: with http://groups.google.com/ (12/20/2002) a lot of rumours can be found.
[9] Http://www.spam.com (12/19/2002).
[10] Listen to the sketch: http://www.montypython.net/cgi-bin/dl2/sketches.cgi?spamenu.wav (12/19/2002).
[11] See for further information: http://www.idyllmtn.com/mush/what.html (12/19/2002).
[12] W.K. Khong, "Spam Law for the Internet", http://warwick.ac.uk/jilt/01-3/khong.html (12/15/2002).
[13] Serge Gauthronet / Etienne Drauard, "Unsolicited Commercial Communications and Data Protection", ETD/99/B5-3000/E/96, http://europa.eu.int/comm/internal_market/en/dataprot/studies/spamstudyen.pdf (12/20/2002).
[14] Khong, http://warwick.ac.uk/jilt/01-3/khong.html.
[15] Lilian Edwards, "Canning the Spam: Is There a Case for Legal Control of Junk Electronic Mail?", http://www.law.ed.ac.uk/script/spam.htm (12/19/2002).
[16] Rowan Middleton, "A Taste of European Spam Regulation", Privacy and Data Protection (PDP) 2.4(3).

advertising either to newsgroups or individuals."[17] In the case of focusing on e-mails "spam" is the umbrella term for

- unsolicited commercial e-mails (UCE) and
- unsolicited bulk e-mails (UBE).

As the history of spamming shows the issue does not only concern e-mails but also other communication technologies (MUD, newsgroups and new technologies like short message service (SMS) for mobile-phones and so on). So the LINX, the London Internet Exchange, suggested a better description would be

- unsolicited bulk material (UBM).[18]

This term does not distinguish the content of the sent material; a missing detail which makes no big difference in the annoyance of the recipient but could have effect on the legal evaluation. Therefore following terms should be used under the umbrella term "spam":

- unsolicited commercial material (UCM) by electronic mail and
- unsolicited non-commercial bulk material (UNBM) by electronic mail.

This wide term and the need for the named difference is indicated by the e-Communications Directive, which forces the EU-Member-States to prohibit "unsolicited communications" after the 31st October 2003: "The use of automated calling systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing [highlighting added] may only be allowed in respect of subscribers who have given their prior consent" (Art 13 E-Communications Directive). "Electronic mail" is defined extremely widely in Art 2 lit h of the Directive as "any text, voice, sound or image message sent over a public communications network which can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient".

Thus, spamming, as it is understood in this work, refers to the method of sending unsolicited material with the help of communication networks and does not refer to the content of the material (although the legal aspects concerning spam-material can differ because of its content: scam, fraud, racism, and other illegal matters). This distinction

[17] Communications and Information Industries Directorate, "UK E-Commerce Strategy: Building Confidence in Electronic Commerce – A Consultation Document", http://www.dti.gov.uk/cii/ecommerce/ukecommercestrategy/archiveconsultationdocs/summary.shtml (12/20/2002).
[18] Edwards, http://www.law.ed.ac.uk/script/spam.htm.

between method and content follows the communication theory dividing a communication system into three distinct layers:[19] At the bottom the "physical layer" (wires and hardware); in the middle the "logical/code layer" which makes the hardware run (here named as "method"); and on the top the "content layer", the actual content that is transmitted. Spamming is an issue of the "logical/code layer" and only secondarily an issue of the "content layer".

2.2. Spamming-Technology and Harm of Spamming

As mentioned above, spamming is not only an issue of e-mails; nevertheless, at the moment spam-e-mails cause the biggest costs and annoyance. The reason for these issues has its origin in the technology used for e-mails: The Simple Mail Transfer Protocol (SMTP), the standard protocol on the Internet for sending e-mails, enables that one e-mail can be sent to an infinite number of recipients and the protocol does not require a valid address to authenticate the sender. If a spammer does not worry about being identified, e.g. he is domiciled in a country without any possibility of legal enforcement, he just uses the e-mail-server of his provider.[20] In the absence of authentication by using SMTP the spammer can also send his spam over a third party e-mail-server (an open SMTP-Relay) even without knowledge of the provider of the e-mail-server.[21] Some Internet Service Providers (ISPs) who want to protect their servers from the misuse by spammers use a new protocol called "SMTP-Auth". With SMTP-Auth the sender has to authenticate himself with a password on the Mail Transfer Agent (MTA), a software running on the e-mail-server. This protocol does not prevent from spamming but makes it easier to identify the spammer (but only with the help of the ISP). However, it is very easy for senders to send spam anonymously to an infinite number of recipients.

For effective (commercial) spamming a big number of valid recipient addresses (e.g. of e-mail-accounts, of newsgroups, of mobile-phones (numbers), and so on) are needed. There are three ways to get through to an enormous number of recipients:

---

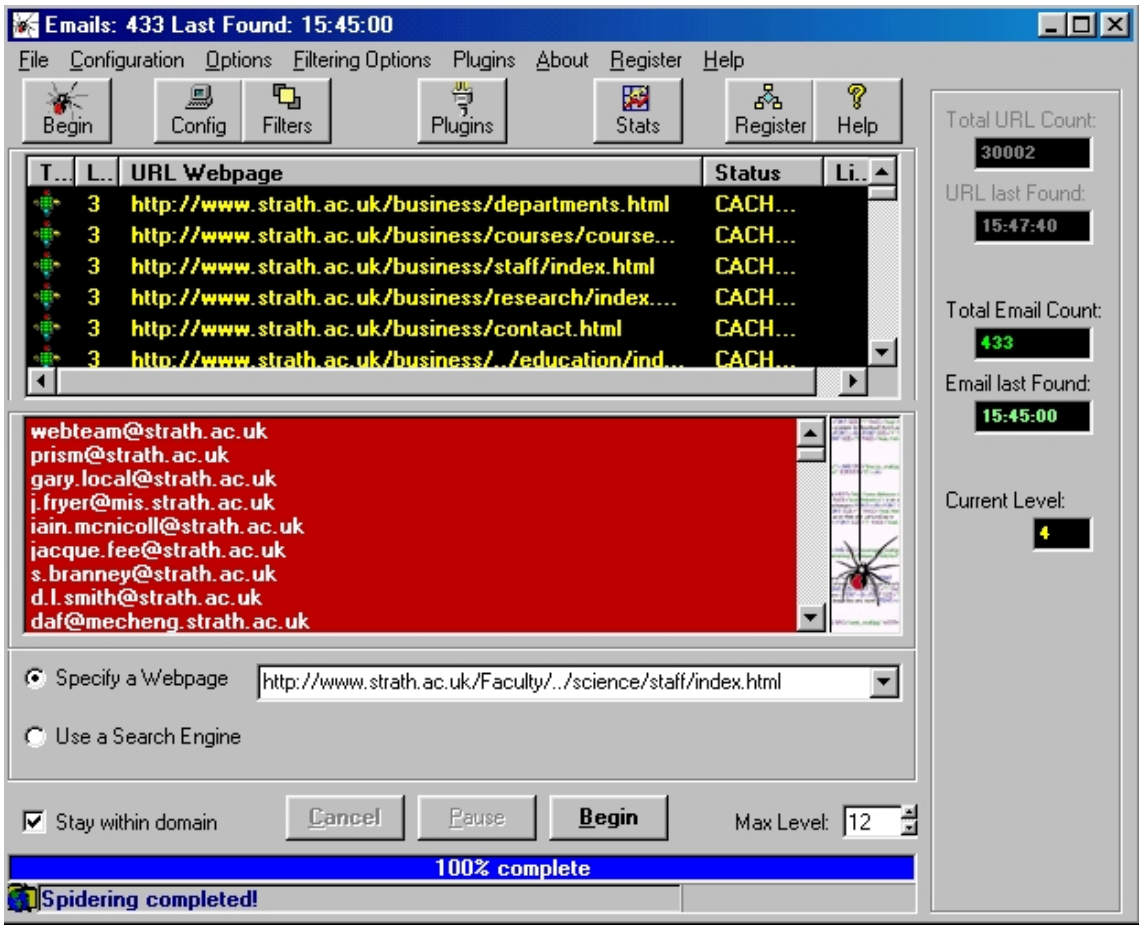
[19] Cp Lessig Lawrence, The Future of Ideas (2002) 23 et sqq.

[20] Although the address of the sender as it appears at the computer of the recipient can be chosen completely free the Internet Protocol address (IP-address) leads to the e-mail-server of the sender. With the IP-address of the e-mail-server the ISP of the spammer can be identified.

[21] There are several lists of open SMTP-servers on the Internet available, eg: "fyi: current list of open smtp relays (fwd)", http://www.health.ufl.edu/mail-archives/hnforum/2000/02/msg00004.html (1/5/2003).

- a professional spammer is paid for sending the spam;
- addresses are bought from a professional spammer; or
- do it yourself: search for addresses.

For the third possibility the world wide web (www) offers a nearly infinite source of addresses, from mobile-phone-numbers over newsgroup-addresses to e-mail-addresses. Special software (so called crawlers) can search the www for addresses automatically; e.g. a software called "email spyder" needed about 20 minutes to find 433 e-mail-addresses only under the domain www.stratch.ac.uk by checking 30.002 sites.[22]



Another possibility is to determine addresses by trial and error: E.g. a lot of e-mail-addresses are predictable because they are made up of the name of the recipient and the domain e.g. john.smith@domain.com.[23] Some well-known ISPs with a large client base whose e-mail-addresses can be easily "harvested" by acquiring a temporary guest

[22] The search was done on the 12/1/2002 with the free trial version available under www.emailspyder.com.
[23] Cp Rowan Middleton, PDP 2002, 2.4(3).

account, tend to be heavily spammed and this leads to the loss of customers who are annoyed.[24]

But not only the tools for finding addresses are available on the Internet but even the tools for sending (anonymous) messages to e.g. mobile-phones are provided[25] and it is predictable that these features will be provided for UMTS-mobile-phones and following generations too.

Recapitulating there are several tools to find addresses for spamming (even if not all of the addresses will be valid) and it is very easy for spammers to send their messages (anonymously) over the Internet or in the future over UMTS-networks (and other (tele-)communication networks). So the technology facilitates spamming and unfortunately it is used by spammers and furthermore often with dubious content: According to the Internet Fraud Complaint Center (IFCC)[26], a program by the Federal Bureau of Investigation and the National White Collar Crime Center, the total dollar loss from all referred (ecce!) cases of fraud per e-mail was $ 17.8 million in the year 2001, with a median dollar loss of $ 435 per complaint. This loss is not caused by spamming (the method) but the content of the sent messages, which is not topic of this paper. But as it will be shown beneath, regulations against spamming do not (only) focus on the content but mainly on the fact that spamming on its own causes enormous loss: The high speed of changes on the Internet leads thereto that every statistic about the Internet is out of date by the time that the figures are published. Being aware of this fact, the following figures show how important e-mail-traffic has become: The average daily traffic reached 25 billion e-mails[27] and up to 44 percent of this is spam (the average 11 percent).[28] So a high percentage of the daily e-mail-traffic is caused by e-mail-spammers and the consequences are costs and annoyance on different levels:

[24] Edwards, http://www.law.ed.ac.uk/script/spam.htm.
[25] E.g. for GSM in the UK: http://www.contactmusic.com/new/home.nsf/Lookup/Send-free-SMS-@-contactmusic/$file/Send-free-SMS-@-contactmusic.html (1/5/2003).
[26] IFCC 2001 Internet Fraud Report, http://www1.ifccfbi.gov/strategy/IFCC_2001_AnnualReport.pdf (1/5/2003).
[27] Jo Bager / Holger Bleich / Joerg Heidrich, “Die Internet-Massenplage”, c’t 2002/22, 150.
[28] Tobias Oetiker / Dave Rand, Email Service: Spam Entering, http://dune.coam.net/mailstats/spam/spam.html (1/5/2003).

- The recipient has to face download-costs, storage-costs and the risk of being unreachable because of full storage-space on his account, and the loss of time because of reading and deleting the spam-message;
- The ISP of the recipient has to bear the costs of storage (till the message is deleted on the server) and traffic of the message and has to spend time to handle customer's complaints and as mentioned before could even lose annoyed subscribers;
- ISPs who have to transport the messages through the network(s) have to bear these costs; and
- the community of users is annoyed or even has to face damages, because the efficiency and speed of the Internet could be threatened.

Because of the wide notion of spam, not all the mentioned harm is caused by every spamming-technology. E.g. there are normally no costs for receiving a text-message by a mobile-phone; therefore mobile-phones have less memory-space than computers for storing messages. In many aspects spam is not even dissimilar to non electronic direct marketing, although it is significant that the costs of marketing by spam are shifted almost wholly from the spammer to the recipient and the community of the network providers and users. But even this significance is not substantial for every spamming-technology; e.g. is a message to a mobile-phones and its transport normally paid by the sender. The crash of servers is mainly an issue of e-mail-spam; servers from which spam is sent or through which it is transmitted may crash not only because of the initial volume of mail sent out but also as a result of "mail undeliverable" or "mail delivered" messages returned from (non existing) recipients.

Apart from the spamming-technology and the taking over of the costs one main argument is brought forward by the recipients: Annoyance. And this cannot only be seen as a local annoyance to users but as a real hazard for the consumer and business confidence in the Internet as a commercial medium.[29]

Because of the enormous data-traffic that spam causes, many ISPs waste money buying excess bandwith, 24 hours support and storage-space as preventive strategy. This is still

[29] Edwards, http://www.law.ed.ac.uk/script/spam.htm.

cheaper than risking a crash: E.g. estimated a US court in the American Online vs Prime Data Systems that AOL has to spend 0.0078 cents per spam-message (in sum was that in this concrete case $ 400,000.-).[30] In another US case the spam effected the server so much that e-mails that should have been delivered in minutes were taking three days to arrive – therefore the loss of reputation was enormous.[31]

The listed losses, the annoyance coupled with the damages caused, show that spamming is much more than an innovative measure for direct marketing. But still there are different approaches to spamming: Is there a need for new regulation or can the spam-issue be handled with existing technology or/and existing laws? Is there a need for regulation at all?

2.3. Need for Regulation?

As it is already mentioned above the EU and states across the globe[32] are discussing or even passing regulations against spamming (cp. 22 US-states have passed bills).[33] On the other hand spamming is a new and innovative measure of direct marketing with a huge potential of creating new jobs. It could also be argued that there are few differences between mail direct marketing and some methods of spamming as long as there is no concrete damage.

2.3.1. "No Damage = No Regulation Approach"

Spammers could argue that spamming causes no damage: They just use an infrastructure which technically enables their behaviour; there are technologies (filter-systems) that prevent annoyance and even damage of ISPs as they could use it to avoid traffic; electronic direct marketing causes no pollution – in contrast to direct marketing by mail or leaflet; and it offers the possibility for new companies to enter the market with less market forces and costs, so that the benefit of the (national) economy prevails the damages that are caused. Finally, spammers could bring forward that regulations

[30] American Online v. Prime Data Worldnet Systems, Inc. - Report and Recommendation, Civil Action No. 97-1652-A (12/20/1998), http://legal.web.aol.com/decisions/dljunk/primereport.html (1/6/2003).
[31] Compuserver Inc v. Cyber Promotions, Inc. – Final Consent, Civil Action No. C2-96-1070, http://www.jmls.edu/cyber/cases/cs-cp3.html (1/6/2003).
[32] Cp Electronic Privacy Information Center / Privacy International, Privacy and Human Rights 2002, http://www.privacyinternational.org/survey/phr2002/phr2002-part1.pdf (1/8/2003).
[33] Michael Jacobs / David Naylor / Megan Auchincloss / David Melaugh, "Spam Wars", ITLT 10.4(19).

against spamming would be a senseless measure because there is no possibility for a global enforcement and they would just change their place of business and carry on.

2.3.1.1. Technology vs. Spam

A lot of companies deal with filter-systems against spam – and most of them sell it for a bit amount of money. So the "no damage"-argument is from the very beginning wrong and although there are sophisticated systems (text-filter in header, subject or whole text; "black lists"[34] for sender-addresses or even sender-servers),[35] they are still imperfect. Filters cannot block all spam and filtering always comes with the worry that e-mails will be mistakenly blocked.[36] As e- and m-commerce is growing (and this is a political aim of most governments) the "white-lists-system", where only messages from senders who are on the list can be received, becomes impossible for businesses and for ISPs and other network providers who (have to) provide "open message services" for their customers. Furthermore, the 'Directive on electronic commerce' (E-Commerce Directive)[37] could lead to major difficulty by using filter systems: Art 11 para 1 second indent E-Commerce Directive determines that "the order [… is] deemed to be received when the parties to whom they are addressed are able to access [it]." Although para 3 restricts the appliance of Art 11 the second indent is applicable to all cases within the "coordinated field" (Art 2 lit h E-Commerce Directive). So offers/orders (and arguably other declarations of intention) can be sent by electronic mail and it is the obligation of the recipient to be able to access them. From this follows that filter systems are no solution against spamming.

2.3.1.2. Spamming vs. (National) Economy

Many spamming-methods (especially by e-mail) are the cheapest way for the sender to reach (potential) customers with his advertisement. On the other hand, the costs of most spamming-methods are borne by the network providers and consequently by the customers of the providers and by the recipients. This shift of costs combined with the

[34] Cp critics on so called Realtime Blackhole List (RBLs): Sharon Gaudin / Suzanne Gaspar, "The Spam police", www.nwfusion.com/research/2001/0910feat.html (1/7/2003).
[35] Cp Paul Graham, "A Plan for Spam", www.paulgraham.com/spam.html (1/7/2003).
[36] Cp Jacobs / Naylor / Auchincloss / Melaugh, ITLT 10.4(19).
[37] 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') Official Journal L 2000/178, 1.

annoyance and the invasion of privacy and additionally the political aim to strengthen the confidence in the e-commerce lead to the evaluation that the benefit of the single spammer does not prevail the loss and damage caused by spamming.

2.3.2. "Self-Regulatory Approach"

Especially the history of the Internet is stamped by self-regulation.[38] So it could be argued that (at least) the Internet-community could regulate spamming with technological measures (e.g. no anonymous e-mail; not more than 5 recipients per e-mail and so on). But these measures would limit the usability of the whole e-mail-system because of "some spammers": "A belief that, to date, technology, self-regulatory efforts and case-by-case legal action have had a limited impact on unsolicited commercial email."[39] Furthermore, one argument convinces why spamming cannot be a case of self-regulation: It is a political decision if spamming should be forbidden but nearly all self-regulatory-systems handle (only) technological issues[40] and the competent organisation for such a decision would be unclear.[41]

2.3.3. "Legal Regulatory Approach"

It is/was mainly a political decision if spamming is/should be explicit forbidden; this decision raises a question which can only be mentioned in this paper: "Sending e-mails and Freedom of Speech/Expression." For this question the content of spam is very important: Although even advertisement is protected by the freedom of expression,[42] in the case of spamming the freedom of expression (Art 10 European Convention on Human Rights' (ECHR))[43] is concurring with the Right to respect for private and family life (Art 8 ECHR) and the property of the recipient. Although this issue can be

[38] Cp Request for Comments. The document series, begun in 1969, which describes the Internet suite of protocols and related experiments. Not all (in fact very few) RFCs describe Internet standards, but all Internet standards are written up as RFCs.
[39] Report to the Federal Trade Commission of the Ad-Hoc Working Group on Unsolicited Commercial Email, www.cdt.org/spam (1/7/2003).
[40] Cp Report on the Conference on "Political Change for the Information Society" (Rome, 19 & 20 March 1999) http://europa.eu.int/comm/consumers/policy/developments/e_comm/e_comm02_en.html (1/7/2003); cp Chet Dembeck, "Internet Self-Regulation Dead on Arrival", http://www.ecommercetimes.com/perl/story/2869.html (1/7/2003).
[41] Cp the competence of the ICANN: www.icann.org (1/7/2003).
[42] Cp Europ Court of Human Rights, Markt Intern and Beermann v. Germany (1989), http://www.echr.coe.int/ (1/24/2003).
[43] European Convention on Human Rights', http://www.echr.coe.int/Convention/webConvenENG.pdf.

problematically in connection with eg political, religious messages, in the case of pure economically spam, the author sees no big issue in banning them.

Nevertheless, spamming could violate existing general regulations.

2.3.3.1. Tort or Delict

If spamming is an issue of tort or delict cannot be answered by looking at the EU-regulations but by examining the national laws: As mentioned above the US courts have several times allowed claims in tort by ISPs against spammers (usually tort of trespass). The successful US cases cannot be applied directly to the European legal systems: E.g. in Scotland the delict of trespass relates almost exclusively to the use without permission of heritage (land and buildings).[44] On the other hand, actions by ISPs against spammers on the base of economic torts or delicts could be successful in many states of the EU (e.g. Scotland and England,[45] Germany[46]). It would go beyond the scope of this work looking at all national possible civil and criminal actions, but at least one criminal act should be highlighted: The Computer Misuse Act 1990. Although the Act was introduced primarily to deal with computer hacking in Sec 3 of the Act, which provides that an offence is committed if anyone with deliberate intent causes an unauthorised modification of the contents of any computer, could be a fertile ground of prosecution against a spammer. Sec 17 of the Act defines the unauthorised modification (amongst other) as any data that is added. But the modification must then be intended to impair the operation of the computer or to prevent or hinder access to any program or data held on any computer or to impair the operation of any such program or the reliability of any such data. Obviously it needs an extremely wide interpretation to subsume spamming under this regulation – but it is not totally absurd that this Act is applicable.

Another possible base for a prosecution against a spammer could be found in the national Telecommunications Acts (misuse of telecommunication equipment).[47]

[44] Edwards, http://www.law.ed.ac.uk/script/spam.htm.
[45] Cp Edwards, http://www.law.ed.ac.uk/script/spam.htm.
[46] Cp Geraint G Howells., "The privatisation of justice", New Law Journal 2000 / 150, 972.
[47] Cp Section 43 of the UK Telecommunications Act 1984.

Furthermore, an action against a spammer could be raised on the ground of violation of the right to privacy: "[… The] main impact on the public of spam is that of annoyance [and] invasion of privacy […]."[48] The ECHR provides in its' Art 8 the "right to respect for private and family life"; the ECHR only imposes an obligation on the state/government but not between citizens. The EU-law "only" provides a data protection law but not the right to privacy between citizens. Some legal systems of the Member-States of the EU provide a general right to privacy or personal rights which could be used as a base for an action against spammers (cp § 823 BGB (tort) in connection with the general personal right (cp Art 2 GG) in Germany;[49] § 1295 ABGB (tort) in connection with § 16 ABGB in Austria[50]). But on the other hand "[…] neither English nor Scots law currently recognises any general right to privacy […]."[51] Recapitulating, there is no EU-wide general right to privacy and at the moment no intention to uniform the regulations about privacy as long as the issue does not concern data protection.

2.3.3.2. General Regulation: Data Protection (in the EU) and E-Mail-Addresses

One of the major problems of nearly all data protection laws in the EU is that they are less than crystal clear in their wording. Most of them are more or less based on the EU Data Protection Directive.[52] The first issue raises with the question as to whether spammers are "controllers" in terms of Art 2 lit d of the Directive which premises that e-mail-addresses are personal data (Art 2 lit a). Because of this definition spamming resp collecting e-mail-addresses of legal persons is not an issue of data protection. If the e-mail-address is not relating to an identified or identifiable natural person (an example seems to be, a9605583@unet.univie.ac.at) the data protection law is not applicable either. How difficult the distinction can be, is shown by the above-named address: According to Art 2 lit a Data Protection Directive an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification

[48] Edwards, http://www.law.ed.ac.uk/script/spam.htm.
[49] Http://www.akademie.de/business/tipps_tricks/marketingpr/spam_gesetzeslage.html (1/5/2003).
[50] Elmar Liese, "Spam-Urteile: Zur rechtlichen Zulässigkeit von E-Mail-Werbung", http://www.akademie.de/business/tipps_tricks/marketingpr/spam_gesetzeslage.html (1/9/2003).
[51] Ian J. Lloyd, Information Technology Law (2000) 205.
[52] 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, Official Journal 1995 L 281, 31.

number; in this case "9605583" is the matriculation number of a student of the University of Vienna in Austria (easy to recognize by the domain univie.ac.at). But the student is still not identifiable for every spammer; therefore he needs to combine it with other information. This fact does not affect the evaluation in the terms of the Directive but in many national Data Protection Laws: Section 1 of the UK Data Protection Act 1998 defines "personal data" as data "[…] which relate to a living (ecce!) individual who can be identified […] from those data […] which is in the possession of, or is likely to come into the possession of, the data controller." Normally lists of matriculation numbers are not free available, but on the other hand the e-mail-address could be written on a website and be found via a search engine.[53] It is not necessary that the spammer really searches for the additional information ("likely to come into the possession"). Another example is Sec 4 of the Data Protection Act 2000 in Austria: Data is not "personal data" if the necessary additional information cannot be procured by legal means.

Recapitulating it is not possible to generalise if e-mail-addresses are or are not personal data which are protected by the Data Protections Laws of the EU-Member-States. Obviously a lot of Data Protection Acts differ from the guidelines of the EU-Directive. However, in terms of the Data Protection Directive most e-mail-addresses can be subsumed under the term "personal data". So the spammer has to fulfil the obligations of the Directive: Processing fairly and lawfully and mind the data quality (Art 6); the data subject's right to access the data (Art 12) and to object (Art 14); the security of processing (Art 17); and the obligation to notify the supervisory authority (Art 18).[54] For spammers the biggest hurdle is the fair processing: According to Art 7 of the Directive the processing of personal data is prohibited as long as there is no listed exception (a quasi "opt-in-System").[55] In connection with spamming

- the given consent of the data subject; or
- that the e-mail-address is necessary for the performance of a contract; or
- that the e-mail-address is necessary for compliance with a legal obligation;

[53] Cp Edwards, http://www.law.ed.ac.uk/script/spam.htm.

[54] Cp to the obligations under the UK Data Protection Act: Edwards, http://www.law.ed.ac.uk/script/spam.htm; for Austria: Thomas Fraiss, Die rechtlichen Rahmenbedingungen von Spam in der EU und in Österreich (2002), http://www.it-law.at/papers/Fraiss_Thomas_Spam_EU_Oesterreich.pdf (1/8/2003).

[55] Seems to be of another opinion: Lloyd, Information Technology Law, 112; more to the opt-in-System is stated below.

are the most important possible exceptions.

That the given consent[56] justifies "spamming" (cp the conflict with the definition) follows from the idea of "informational self-determination":[57] Cp the first principle in schedule 1 in connection with Schedule 2 of the UK Data Protection Act 1998.

The e-mail-address can be used for "spamming" (cp the conflict with the definition) if it is necessary for the performance of a contract (e.g. newsletter). But according to the "economy of data principle" (Art 6 para 1 lit e of the Data Protection Directive) the service provider (e.g. newsletter provider) cannot use this data for "other spamming" (or disclosure to a third party). The named principle can be found in most national laws in the EU: cp the first principle in Schedule 1 in connection with Schedule 2 para 6 (1) of the UK Data Protection Act 1998 which requires to mind the rights and freedoms or legitimate interests of the data subject; cp Sec 6 of the Austrian Data Protection Act 2000, which requires to delete data which are no longer necessary for the legitimate purpose.

As mentioned above, according to Art 11 of the e-Commerce-Directive, the service provider has to acknowledge the receipt by electronic means; therefore, he needs the address of the electronic mail account. Again the above-named principle prohibits the use of the data for spamming.

So it can be said that most spammers in the EU have to mind the Data Protection Acts and in most cases they need the consent of the data subject to process the addresses. And even if the spammers are allowed to send the messages, there are several aspects they have to be aware: E.g. the principle of non-disclosure by using e.g. the "cc:"-feature by sending the messages to several recipients (Art 7 in connection with the definition of "processing" in Art 2 of the Data Protection Directive; the third principle of the UK Data Protection Act 1998; Sec 7 of the Austrian Data Protection Act); or in the UK the obligation to register with the Data Commissioner.[58]

[56] How this consent comes into existence will be investigated below.
[57] Cp Lloyd, Information Technology Law, 83.
[58] Cp Edwards, http://www.law.ed.ac.uk/script/spam.htm.

2.4. Special Regulation for Spamming

Before the special regulations for spamming are investigated, it is necessary to reflect on what kind of rules and prohibitions are possible:

- Total prohibition: Spamming is illegal (as long as there is no ground of justification).
- "Explicit opt-in-system": Spamming is prohibited as long as there is no explicit (ecce!) consent of the recipient before the first spam is sent (the spammer has even to check if the consent is really given from the recipient; called "double-opt-in").
- "Opt-in-system": Spamming is illegal as long as there is no (implicit) consent.
- "first-free-system": The spammer can ask for the consent by sending the recipient a message and only if the consent is given spamming is allowed.
- "Implicit - first-free-system": The spammer can ask for the consent by sending the recipient a message and if the recipient does not object spamming is allowed.
- "register opt-out-system": Spamming is allowed as long as the recipient has not put his name on an (official) opt-out-register.
- "opt-out-system": Spamming is allowed as long as the recipient has not objected to the individually sender.
- Spamming is totally legal.

The EU has dealt in several Directives with the issue of direct marketing by the use of (tele)communication infrastructure (cp the above-named layer-model). Unfortunately, not all of these regulations are applicable to spamming (cp the definition of electronic mail). Because the notion "consent" is so important in the above-listed possibilities of regulation, it is necessary to determine it: Art 2 lit h Data Protection Directive defines: "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."

2.4.1. ISDN-Directive 97/66/EC and National Laws

The ISDN[59]-Directive (or Telecommunications Privacy Directive)[60] provides in its Art 12 that

> "1. The use of automated calling systems without human intervention (automatic calling machine) or facsimile machines (fax) for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent. […]"

Although the definition of spamming and electronic mail is quite wide, only the spamming-method with facsimile machines (fax) for the purpose of direct marketing can be subsumed under Art 12 ISDN-Directive. Thus, the Directive regulates a method of the first case of the umbrella term spamming: using the fax for the purpose of sending unsolicited commercial material (UCM). E-mail-spamming cannot be subsumed under this Article as the aim is to regulate "standard telecommunication" by voice or fax.[61]

So the Directive determines an "opt-in-system" for fax-spamming. For the interpretation of the consent the definition of the (older) Data Protection Directive must be consulted; an explicit consent is not necessary (an implicit is enough) but it has to be an informed consent.

The Directive determines only a minimum standard for the protection of the subscriber (not the user (ecce!)). Some states have thus enacted national laws which have a wider protection than the Directive (and the following Directives). Here some examples:[62]

- Austria (opt-in-system):

  § 101 Telecommunications Law: [...] Sending of email in bulk or for advertising purposes requires the prior - revocable at any time - consent of the recipient.

[59] ISDN = Integrated Services Digital Network.
[60] 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 Official Journal 1998 L 24, 1.
[61] Of another opinion: Khong, http://warwick.ac.uk/jilt/01-3/khong.html, who subsumes spamming undert "automatic calling machines".
[62] Source: http://www.euro.cauce.org (1/5/2003) and http://europa.eu.int/comm/internal_market/en/dataprot/studies/spamstudyen.pdf (1/9/2003).

- Denmark (register opt-out-system and first free system):

  6 a. Danish Marketing Practices Act: (1) Where a supplier sells goods, immovable or movable property or work or services to customers, he shall not be allowed to make calls to anybody using electronic mail, automated calling systems (automatic calling machines) or facsimile machines (fax) for the purposes of such selling unless the particular customer has made a prior request for such calls.

  (2) A supplier may not call a specific natural person using other means of distance communication for the purposes of selling goods or services as referred to in subsection (1) above, if that person has asked the supplier not to make such calls, if a list made on a quarterly basis by the Civil Registration System (CPR) includes an indication that the person concerned has objected to receiving calls made for such marketing purposes, or if the supplier has become aware by a search of the Civil Registration System that the person concerned has objected to receiving such calls. Moreover, telephone calls to consumers are subject to the rules on unsolicited calls set out in the Act on Certain Consumer Agreements.

  […]

  (4) The first time a supplier makes a call as described in subsection (2) above to a specific natural person whose name is not included in the CPR list, the supplier shall inform that person in a clear and comprehensible manner of the right of consumers to object to calls from suppliers as described in subsection (2) above. At the same time the person concerned shall be given easy access to object to such calls.

  [...]

- Finland (Fax-spamming: opt-in for natural persons; opt-out for legal persons. Other electronic mail-spamming: register opt-out-system):

  Section 21 of Act n° 1999/565 of April 1999: Telecommunications in direct marketing: 1. Telecommunications may not be used for direct marketing without the prior consent of the subscriber if the calls to the called subscriber are made by means of automated calling systems or facsimile machine unless otherwise decided by the ministry under paragraph 4.

2. Without prejudice to the provisions of paragraph 1, telecommunications may be used for direct marketing by means of automatic systems if a subscriber who is not a natural person has not forbidden it unless otherwise decided by the ministry under paragraph 4. However, a telefax may be used for direct marketing to a subscriber who is not a natural person.

3. Telecommunications used for the purposes of direct marketing to a natural person by other means than those referred in paragraph 1 shall be allowed unless expressly forbidden by him. The subscriber must have a way of forbidding the direct marketing referred to in this subparagraph free of charge.

4. The ministry shall, where necessary, taking into account the functionality and security of the telecommunications network and telecommunications services as well as the reasonableness obligations ensuing on the providers of direct marketing, decide in more detail on the means of telecommunications which :

- would be allowed in telecommunications referred to in paragraph 1 without the consent of the subscriber provided, however, that the subscriber is able to forbid or prevent the telecommunications referred to in this subparagraph; as well as which
- in telecommunications referred to in paragraph 2 require prior consent of the subscriber.

Direct marketing directed at consumers shall further be governed by the provisions of the Consumer Protection Act (1978/38).

Section 22: Availability of refusals to accept regarding direct marketing: The ministry shall, where necessary, decide in more detail on ways in which the refusals referred to in section 20, paragraph 2, subparagraph 2 (direct marketing towards subscriber directories) and section 21 shall be held available to those providing direct marketing.

- Italy (explicit opt-in-system for fax; opt-out-system for addresses that are personal data):

  Article 10 Implementing Decree n°171 of 13 May 1998: Unsolicited calls: […]

  5. The use of automated calling systems without human intervention or facsimile machines for the purposes of direct marketing or sending advertising materials,

or else for carrying out market surveys or interactive business communication shall only be allowed with the subscriber's express consent.[…]

Article 13 of the Act n° 675 of 31 December 1996: Data subject's consent: […]

1. In respect of the processing of personal data, any data subject shall have the right to: […] e) object, in whole or in part, to the processing of personal data relating to him which is carried out for purposes of commercial information or advertising or direct marketing, or else for the performance of market or interactive commercial communication surveys, and be informed by the controller, no later than at the time when the data are communicated or disseminated, of the possibility to exercise such right free of charge. […]

- Norway (opt-in-system for electronic mail):
  Section 2b Marketing Control Act: Restrictions regarding certain methods of communication: It is prohibited in the conduct of business to direct marketing at consumers using methods of telecommunication which permit individual communication, such as electronic mail, text messaging services to mobile telephones, facsimile or automatic calling machine, without the prior consent of the recipient.
  The prior consent required in accordance with paragraph one is, however, not applicable to marketing where the consumer is contacted orally by telephone.

2.4.2. Distance Selling Directive

Art 10 of the Distance Selling Directive[63] nearly repeats the wording of the ISDN-Directive:

"Restrictions on the use of certain means of distance communication:

1. Use by a supplier of the following means requires the prior consent of the consumer:

- automated calling system without human intervention (automatic calling machine),

[63] 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, Official Journal 1997 L 144, 19.

- facsimile machine (fax).

2. Member States shall ensure that means of distance communication, other than those referred to in paragraph 1, which allow individual communications may be used only where there is no clear objection from the consumer."

The Directive affirms the opt-in-system for fax-spamming – for other spamming-methods the Directive determines at least an opt-out-system ("clear objection"). Although only consumers are in the scope of protection of the Directive, it is again a minimum standard; so Member-States can pass acts with wider protection (Art 14 of the Directive).

2.4.3. E-Commerce Directive

Article 7 of the E-Commerce Directive brought great confusion in connection with spamming:

"Unsolicited commercial communication

1. In addition to other requirements established by Community law, Member States which permit unsolicited commercial communication by electronic mail shall ensure that such commercial communication by a service provider established in their territory shall be identifiable clearly and unambiguously as such as soon as it is received by the recipient.

2. Without prejudice to Directive 97/7/EC and Directive 97/66/EC, Member States shall take measures to ensure that service providers undertaking unsolicited commercial communications by electronic mail consult regularly and respect the opt-out registers in which natural persons not wishing to receive such commercial communications can register themselves."

One of the most important parts is "Member States which permit unsolicited commercial communication by electronic mail", because of this wording the Member States are still free to choose their own system handling spamming as long as the fulfil the minimum standard, namely a "register opt-out-system" for natural persons. From the notion "unsolicited commercial communication" follows that only spamming (cp the

definition) has to be labelled but not electronic mails that are sent with the consent of the recipient.

Again the Directive determines a minimum standard but prima facie the "country of origin principle" (Art 3, 2 of the Directive) seems to start a race to the bottom for regulations, because spammers could go to an EU-Member-State with no spam-laws and send the electronic mails from there. But as the Annex of the Directive determines, Art 3 does not apply to "the permissibility of unsolicited commercial communications by electronic mail". Consequently, every spammer has to mind – depending on the wording of the individual national law[64] - the laws of the state where he sends his mails to and (maybe) of the state of his domicile.

The "register opt-out-system" has been subject to a lot of criticisms:[65] It is especially unclear who has to bear the costs and when and how often spammers have to check the register. Furthermore, it has been argued that the register with the e-mail-addresses could be used by spammers who do not care about any laws to collect new e-mail-addresses.

Although an obligatory labelling could help filter-system to handle spam, the imprecise terms of the Directive lead to no solution: How does the label have to look like? Has it to be in the subject line of e-mails (what about text messages to mobile phones?)? A more functional wording has e.g. the California Business & Professions Code §17538.4[66] which determines that "[…] the subject line of each and every message shall include "ADV:" as the first four characters […]". In some national law systems the obligation to label follows already from the unfair competition law and its' principle of transparency (e.g. Sec 1 of the German and Sec 1 of the Austrian Unfair Competition Act).

[64] Depends if it is forbidden to send spam or to reach sb with spam.
[65] Cp Khong, http://warwick.ac.uk/jilt/01-3/khong.html.
[66] Http://www.spambrigade.com/word/California1.doc (1/10/2003).

2.4.4. E-Communication Directive

The E-Communication Directive[67] has to be transposed until 31st of October 2003 and determines in its' Art 13 with the title "Unsolicited communications" for the first time an opt-in-system (with exceptions) for all spam for the purpose of direct marketing:

> "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. 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.
>
> 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.
>
> 4. In any event, 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, shall be prohibited.
>
> 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

[67] 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 (Directive on privacy and electronic communications), Official Journal L 2002/201, 37.

other than natural persons with regard to unsolicited communications are sufficiently protected."

This Directive seems to be the EU-wide solution for spamming; but it raises some (new) issues and some of them will be discussed beneath:

2.4.4.1. E-Communication Directive: Achievement and (New) Issues

The biggest achievement of the Directive is without any question the EU-wide uniformity of spamming-regulation and the technical neutral wording (cp the above-named definitions) which make the regulation applicable to many upcoming spamming-methods (e.g. UMTS[68]). Nevertheless, some issues are not solved and even new are raised with the Directive:

2.4.4.1.1. Unsolicited Non-Commercial Bulk Material (UNBM)

All the above-mentioned Directives apply only to "commercial communication"[69] or "electronic mail for the purposes of direct marketing" and not to unsolicited non-commercial bulk material (UNBM). Although the practical relevance of this kind of spamming is not immense, some states prohibit it (e.g. Austria). So there is no uniform regulation for UNBM across the EU-Member-States ahead.

2.4.4.1.2. Contract Instead of Consent

Article 13 para 2 determines that in the context of the sale of a product or a service spamming is allowed for own similar products or services if the customer has been given clearly and distinctly the opportunity to object when the (address-)data are collected and on the occasion of each message. It seems that this leads to an opt-out-system if there is a contract between the spammer and the recipient. But in the author's point of view it is just an "unfortunate wording": As herein before mentioned the use of address-data for spamming needs in most cases the consent of the recipient (according to the Data Protection Directive). The definition of "consent" in the same Directive

[68] Universal Mobile Telecommunications System: The third generation (3G) of mobile phones.
[69] Because Unsolicited Non-Commercial Bulk Material (UNBM) is not a "information society service" the E-Commerce-Directive is not applicable.

needs no explicit declaration of intention, but the freely given specific and informed indication of the wishes. Recital 41 of the E-Communication Directive says that "[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." So the customer has to be informed and has the free possibility to object (as a freely given indication of his wishes): So he gives his (implicit) consent by ignoring the opportunity to refuse – para 1 can be applied. In the author's point of view para 2 is only needed if there are Member-States where an implicit declaration of intention is not possible.

Even if there are cases where para 2 can be applied, it is unclear what similar "products or services" are: Is a book from amazon about IT-law similar to a tourist guide? A mobile phone similar to a computer?

2.4.4.1.3. Opt-In or Opt-Out for Other Communications

Spamming (with electronic mail) is not the most sophisticated method; spammers are looking at new technology: Alan Ralsky, the "Spam King", is developing a new "stealth spam". "It is intricate computer software, said Ralsky, that can detect computers that are online and then be programmed to flash them a pop-up ad, much like the kind that display whenever a particular Web site is opened. 'This is even better,' he said. 'You don't have to be on a Web site at all. You can just have your computer on, connected to the Internet, reading e-mail or just idling and, bam, this program detects your presence and up pops the message on your screen, past firewalls, past anti-spam programs, past anything.' 'Isn't technology great?'."[70] For these kind of methods it is up to the Member-States to pass opt-in or opt-out-systems – again no uniformity and the question of whether the annoyance and the costs of the named pop-ups make more regulations necessary.

[70] Mike Wendland, "Spam king lives large off others' e-mail troubles", http://www.freep.com/money/tech/mwend22_20021122.htm (1/10/2003).

2.4.5. Distance Selling Directive for Financial Services

The latest Directive dealing with spamming is the Distance Selling Directive for Financial Services:[71]

> Article 10: Unsolicited communications
>
> 1. The use by a supplier of the following distance communication techniques shall require the consumer's prior consent:
>
> (a) automated calling systems without human intervention (automatic calling machines);
>
> (b) fax machines.
>
> 2. Member States shall ensure that means of distance communication other than those referred to in paragraph 1, when they allow individual communications:
>
> (a) shall not be authorised unless the consent of the consumers concerned has been obtained, or
>
> (b) may only be used if the consumer has not expressed his manifest objection.
>
> 3. The measures referred to in paragraphs 1 and 2 shall not entail costs for consumers.

It seems that the lobby of the financial service providers was strong enough to change the E-Communication Directive in the sector of financial services: According to the Directive it is now[72] up to the Member-States to determine an opt-in or an opt-out-system for spamming (UCM) with the exception of fax-spamming where an opt-in-system is obligatory. This raises some (new) issues: Can this Directive change the general regulation of the E-Communication Directive which is also applicable on financial services? The scope of the Directive is consumer-protection; what about businesses – can they be spammed by suppliers? In the author's point of view they cannot be - cp Recital 26: "Member States should take appropriate measures to protect effectively consumers who do not wish to be contacted through certain means of communication or at certain times. This Directive should be without prejudice to the

[71] Directive 2002/65/EC of the European Parliament and of the Council of 23 September 2002 concerning the distance marketing of consumer financial services and amending Council Directive 90/619/EEC and Directives 97/7/EC and 98/27/EC, Official Journal L 2002/271, 16.

[72] According to Art 21 of the Directive not later than 9th of October 2004.

particular safeguards available to consumers under Community legislation concerning the protection of personal data and privacy" – the Distance Selling Directive for Financial Services does not change the guidelines of the E-Communication Directive and therefore, there has to be an opt-in-system in the sector of financial services as well.

3. Evaluation of the EU-Regulations

The political decision if spamming should be regulated was made by several states across the globe, some EU-Member-States and in the last months even by the EU. This political decision must now be implemented in a way that bears in mind that there has to be a global approach on the issue: Spam is inherently a global problem not just (or even mainly) an EU one.[73] But in the author's point of view, regulations – even if there would be a world-wide one on spamming - will never ban spamming totally – as laws against murder have not banned this crime. For the first time seem to be uniform regulations for unsolicited commercial material (UCM) by electronic mail in all EU-Member-States ahead, because of the E-Communication Directive: An opt-in-system for the use of facsimile machines (fax) or electronic mail (any text, voice, sound or image message sent over a public communications network which can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient) for the purposes of direct marketing. Although the wording raises some (new) issues and the regulation cannot be applied on unsolicited non-commercial bulk material (UNBM) by electronic mail, it is (the beginning of) a solution for spamming across the EU. Unfortunately, the Directive does not give crystal clear guidelines. There is the danger that Member-States will pass regulations that differ from each other in details. Especially the exception for customer-relationships could lead to confusion and even the "traditional legal background" of the Member-States when the consent comes into existence could lead to inconsistency. And one question is inescapable: What will the regulations of the Member-States (following the Directive) change in our daily "spam life" where most of the spam comes from Non-EU-Member-States? In the author's point of view, there are several approaches to that question:

- The approach of world-wide regulation: As more and more states across the globe pass regulations against spamming, it will get harder for spammers to find "spam-friendly" domiciles.
- The technical approach: For filter-systems it will become much easier to filter spam from states where no regulations against spamming are passed.
- The approach of obviousness: Because it does not make sense to advertise goods without having any selling offices in Europe, only services (e.g. porn, software)

[73] Cp Edwards, http://www.law.ed.ac.uk/script/spam.htm.

will be topic of spam; this spam can be recognised pretty easily and is therefore less of a danger.

- The "bad faith contract" approach: Even if the spammer is domiciled in a state without regulations against spamming, most producers of goods or service providers are domiciled in Europe or the US – in many states the contractual lien of the spammer will (also) be liable for the spam (at least according to the unfair competition laws).

Recapitulating the (uniform) regulations in the EU-Member-States will not ban spamming in Europe but in connection with (geographical) filter-systems the spam-free e-mail-, text messaging-accounts seem a little bit closer. How big the effects will be in the every-day-life is unpredictable.

4. Bibliography

Ad-Hoc Working Group on Unsolicited Commercial Email, www.cdt.org/spam (1/7/2003).

Jo Bager / Holger Bleich / Joerg Heidrich, “Die Internet-Massenplage”, c’t 2002/22, 150.

BBC, “US workers spared junk e-mails”, http://news.bbc.co.uk/1/hi/technology/2558113.htm (12/9/2002).

BBC, “Spam on the rise again”, http://news.bbc.co.uk/1/hi/technology/2409855.stm (12/9/2002).

Julia Lapsis Blakeslee, “Spam Wars Part II”, ITLT 2002, 10.5(28).

Communications and Information Industries Directorate, "UK E-Commerce Strategy: Building Confidence in Electronic Commerce – A Consultation Document”, http://www.dti.gov.uk/cii/ecommerce/ukecommercestrategy/archiveconsultationdocs/summary.shtml (12/20/2002).

Peter Carey, “Editorial”, PDP 2002, 2.4(2).

Chet Dembeck, "Internet Self-Regulation Dead on Arrival", http://www.ecommercetimes.com/perl/story/2869.html (1/7/2003).

Lilian Edwards, “Canning the Spam: Is There a Case for Legal Control of Junk Electronic Mail?”, http://www.law.ed.ac.uk/script/spam.htm (12/19/2002).

Electronic Privacy Information Center / Privacy International, Privacy and Human Rights 2002, http://www.privacyinternational.org/survey/phr2002/phr2002-part1.pdf (1/8/2003).

Thomas Fraiss, Die rechtlichen Rahmenbedingungen von Spam in der EU und in Österreich (2002), http://www.it-law.at/papers/Fraiss_Thomas_Spam_EU_Oesterreich.pdf (1/8/2003).

Deborah Fallows, “Email at Work”, http://www.pewinternet.org/reports/pdfs/PIP_Work_Email_Report.pdf (12/15/2002).

Serge Gauthronet / Etienne Drauard, “Unsolicited Commercial Communications and Data Protection”, ETD/99/B5-3000/E/96, http://europa.eu.int/comm/internal_market/en/dataprot/studies/spamstudyen.pdf (12/20/2002)

Sharon Gaudin / Suzanne Gaspar, “The Spam police”, www.nwfusion.com/research/2001/0910feat.html (1/7/2003).

Paul Graham, “A Plan for Spam”, www.paulgraham.com/spam.html (1/7/2003).

Geraint G Howells., “The privatisation of justice”, New Law Journal 2000 / 150, 972.

IFCC 2001 Internet Fraud Report, http://www1.ifccfbi.gov/strategy/IFCC_2001_AnnualReport.pdf (1/5/2003).

ITLT, “Consumer Law – Distance Selling And Financial Services”, ITLT 2002, 09.10.

ITLT, “Editor’s Comment”, ITLT 2002, 10.4(3).

Michael Jacobs / David Naylor / Megan Auchincloss / David Melaugh, “Spam Wars”,

IT Law Today (ITLT) 2002, 10.4(19).

W.K. Khong, “Spam Law for the Internet”, http://warwick.ac.uk/jilt/01-3/khong.html (12/15/2002).

Lessig Lawrence, The Future of Ideas (2002)

Elmar Liese, "Spam-Urteile: Zur rechtlichen Zulässigkeit von E-Mail-Werbung", http://www.akademie.de/business/tipps_tricks/marketingpr/spam_gesetzeslage.html (1/9/2003).

Ian J. Lloyd, Information Technology Law (2000)

Bruce Lloyd, “Australia: Securities Law”, Internationla Company and Commercial Law Review 2000, 11(10).

Rowan Middleton, “A Taste of European Spam Regulation”, Privacy and Data Protection (PDP) 2.4(3).

Tobias Oetiker / Dave Rand, Email Service: Spam Entering, http://dune.coam.net/mailstats/spam/spam.html (1/5/2003).

Bill Onwusah, “A Spammer in the works”, New Law Journal 1998, 1718.

Karl H. Pilny, “Germany: Electronic Commerce – Spam”, Computer and Telecommunications Law Review 2002, 8(5).

PDP, “News & Views – More On Spam”, PDP 2001, 2.2(1).

PDP, “News & Views – Sainsbury’s In Email Fiasco”, PDP 2002, 2.3(1).

PDP, “News & Views – Cookies And Spam”, PDP 2002, 2.3(1).

Heather Rowe, “Data Protection”, TLT 2001, 1.7(4).

Susan Singleton, “E-Commerce-Directive – The Responses Are In”, ITLT 2002, 10.3(7).

Susan Singleton, “A Legal Guide To Advertising On The Web”, ITLT 2002, 10.6(9).

TIF, “Return to Sender”, http://www.tif.co.uk/news/PR20021204.html (12/13/2002).

Mike Wendland, "Spam king lives large off others' e-mail troubles", http://www.freep.com/money/tech/mwend22_20021122.htm (1/10/2003).

Graeme Wearden, “Ofcom won’t ban spam”, http://uk.news.yahoo.com/021205/152/dg4qk.html (12/9/2002).

Jane Wakefield, “Fighting the spammers head on”, http://news.bbc.co.uk (12/13/2002).

Mark Ward, “How to keep your life junk free”, http://news.bbc.co.uk (12/13/2002).

Websites:

http://www.akademie.de/business/tipps_tricks/marketingpr/spam_gesetzeslage.html (1/5/2003)

http://www.contactmusic.com/new/home.nsf/Lookup/Send-free-SMS-@-contactmusic/$file/Send-free-SMS-@-contactmusic.html (1/5/2003).

www.emailspyder.com (1/5/2003)

http://www.euro.cauce.org (1/5/2003)

http://europa.eu.int/comm/internal_market/en/dataprot/studies/spamstudyen.pdf (1/9/2003)

http://groups.google.com/ (12/20/2002)

http://www.health.ufl.edu/mail-archives/hnforum/2000/02/msg00004.html (1/5/2003)

http://www.idyllmtn.com/mush/what.html (12/19/2002).

http://www.icann.org (1/7/2003).

http://www.matterform.com/about/welcome/anti-spam.gif (12/10/2002).

http://www.montypython.net/cgi-bin/dl2/sketches.cgi?spamenu.wav (12/19/2002).

Http://www.spam.com (12/10/2002).

Http://www.spambrigade.com/word/California1.doc (1/10/2003).

Cases:

American Online v. Prime Data Worldnet Systems, Inc. - Report and Recommendation, Civil Action No. 97-1652-A (12/20/1998), http://legal.web.aol.com/decisions/dljunk/primereport.html (1/6/2003).

Compuserver Inc v. Cyber Promotions, Inc. – Final Consent, Civil Action No. C2-96-1070, http://www.jmls.edu/cyber/cases/cs-cp3.html (1/6/2003).

Europ Court of Human Rights, Markt Intern and Beermann v. Germany (1989), http://www.echr.coe.int/ (1/24/2003).