

UNIVERSITY OF OSLO
THE LAW FACULTY
Norwegian Research Center for Computers and Law

Som2005

ANTI-SPAM LEGISLATION
BETWEEN
PRIVACY AND COMMERCIAL INTEREST

(an overview of the European legislation regarding the e-mail
spam)
(19 800 words)

Supervisor:
prof.dr.juris LEE ANDREW BYGRAVE

Candidate no.2

- 1 september 2005-

INTRODUCTION

*“The ability of computers to remember so well for so long
undercuts the human frailty that assists privacy”¹*

In January 2001, a study² conducted at the initiative of the European Commission was pointing out that “Europe has not yet experienced an acute outbreak of unsolicited commercial communications or spam”. Only 3 years later, the Commission itself was calling attention to the fact that “spam has reached worrying proportions”³, arguably justifying the enactment of a special legal framework aimed at bringing this phenomenon to a halt.

Essentially, the purpose of most spamming is the commercial marketing activity, although the content of spam e-mails can vary, including sometimes malicious applications (like viruses) and different types of financial schemes. At the same time, this activity involves a personal data processing, as it needs, as an absolute prerequisite, the collection and use of e-mail addresses⁴. Thus, spamming is potentially directed indiscriminately towards each and every individual that owns one such address.

In my view, spam is to be viewed as an anomaly, both from the perspectives of commercial practice and data processing. As I will argue all throughout this thesis, the e-mail addresses can be considered in the overwhelming majority of cases (even when they

¹ James H.Moor “Towards a Theory of Privacy in the Information Age”, article in “Computer Ethics and Professional Responsibility” ed. Terrell Ward Bynum & Simon Rogerson, Blackwell Publishing 2004

² Commission of the European Communities: “*Unsolicited Commercial Communications and Data Protection*” (Internal Market DG – Contract n° ETD/99/B5-3000/E/96), January 2001, authors Serge Gauthronet and Etienne Drouard.

³ “Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee of the Regions on unsolicited commercial communications or ‘spam’”, Brussels, 22.01.2004, COM (2004) 28 final.

⁴ Although spam can be distributed also through sms messages, facsimile machines and automated calling machines, due to the limited size of this thesis I will limit my analysis to e-mail spam messages.

belong to legal persons) as personal data⁵. Therefore, the collection, use and third party disclosure of the e-mail addresses carried out as part of the spam activities represent not only commercial practices, but can be seen also as involving a processing⁶ of personal data. While as a rule, personal data has to be collected and processed “fairly and lawfully” and while e-mail marketing is a legitimate business with a series of unquestionable advantages both for the marketer and the prospect customer, as an exception, the spamming activity speculates on existing legal, technical or enforcement difficulties in order to reach the expected commercial benefits while short-circuiting the established rules⁷.

The scope of the analysis carried out in this thesis will be limited to the relevant material provisions in the European legislation, provisions that are supposed to represent the legislative tools available to the Member States in the fight against spam. I will not address therefore the procedural and enforcement challenges faced by the Member States in implementing and in making use of these tools. Such a broad analysis is presently conducted by international bodies such as ITU⁸, OECD⁹, or WGIG¹⁰. On the other hand, the research I carried out for the purpose of this thesis revealed the lack of a thorough legal analysis of the material provisions that the Member States are required to implement as a sign of their commitment to the fight against spam. While these legal provisions have been explained, dissected, reinterpreted at both European¹¹ and national level¹², few if any studies that I was able to access have questioned the balance of interests achieved by enacting them, the way in which they respond to existing business

⁵ in the interpretation given to the term “personal data” by the article 2(a) of the Directive 95/46/EC.

⁶ in the interpretation given to the term “processing” by the article 2(b) of the Directive 95/46/EC.

⁷ These rules pertaining both to the e-commerce framework and to the privacy and data protection

⁸ <http://www.itu.int/osg/spu/spam/> (last visited: 30 August 2005).

⁹ http://www.oecd.org/departement/0,2688,en_2649_22555297_1_1_1_1_1,00.html (last visited: 30 August 2005).

¹⁰ “Background Report of the Working Group on Internet Governance” (June 2005), available at: <http://www.wgig.org/docs/BackgroundReport.doc>.

¹¹ see for example: COM (2004) 28 final, COM (2003) 702 final, “Opinion 5/2004 on unsolicited communications for marketing purposes under article 13 of Directive 2002/58/EC”, 11601/EN WP90.

¹² see for example, UK Information Commissioner: “Guidance to the Privacy and Electronic Communications (EC Directive) Regulations 2003”, available at:

<http://www.informationcommissioner.gov.uk/cms/DocumentUploads/Electronic%20Communications%20Part%201%20Version%203.pdf>, and also “FPS Economy, SMEs, Self-Employed and Energy – Belgium « Spamming » 24 questions & answers” – January 2005 available at: http://mineco.fgov.be/information_society/spamming/spamming_note_en.pdf.

realities, their integration in the legal context to which they belong or their relative dynamics.

It is in these particular aspects that my present work aims at contributing to the existing doctrine examining the normative response to spam. It will focus mainly on the European Union framework, although references to non-European solutions will be also made, for comparison purposes.

The contextualisation of the spam anomaly will have as a basis the two facets of this phenomenon: the commercial one and the privacy and personal data processing one. Therefore, the thesis will consider three basic elements: the spam practices, the values and interests of the actors involved in spam (marketers and end-users) and the way in which these two elements are reflected and responded to in the current normative anti-spam framework.

One last preliminary comment needs to be made relating to the titles chosen for the first two sections of the third chapter. I am fully aware that the community law cannot be split into “e-commerce related legislation” and “privacy and data protection legislation”, as it is a whole body of legal norms aiming to establish rules applicable to all the facets of a complex reality (the Internal Market) and thus being intermingled and containing cross references. However, I chose to make this artificial distinction only to enhance the two facets of the topic I’m dealing with. Spam is most often an advertising tactic, that is a business related practice and at the same time an intrusion in the privacy of the natural person receiving it, involving often a processing of personal data (the e-mail address). Since the third section of Chapter 3 will evaluate the overall efficiency of the anti-spam provisions in the European legislation, the initial unity will hopefully be re-established.

Although most of the average computer users could recognise a spam message when they receive one in their e-mail box, very few of them might accept the challenge to define or to explain it. As for examples, lots of them could be provided. Their dilemma is perfectly excusable, as there is, up until this moment, no universally agreed definition of spam, although more and more international initiatives and action plans to combat it are

launched¹³. The various definitions provided are more functional and working definitions. Moreover, although the Community legislation refrains from using the term spam as it is, other official documents use it¹⁴.

It is important for the purpose of this thesis to identify clear definitions that would enable me to distinguish between the e-mail spam and the e-mail marketing (even the one involving some unsolicited commercial communications) on the one hand, and between the legal ways of collecting and processing personal data and the practices involved in spam. With this aspect in mind, I will use all throughout this thesis the interpretation given by the OECD to the term “spam”¹⁵, although references to other definitions will be provided also. The OECD identified a series of characteristics (primary and secondary traits) that can be associated with spam. Those characteristics pertain to:

- a) the way in which the e-mail addresses were collected (as spammers use addresses that were collected or sold without the user’s consent, either electronically harvested from public sources- web pages or newsgroups, or sold without the consent of the individual to third parties, or guessed with a specially designed software)
- b) the transmission practices (as these messages are sent electronically, in large quantities(bulk), by an anonymous or disguised sender, are repetitive, untargeted and indiscriminate as to the potential receiver)
- c) the content of the e-mail messages sent by the spammer (usually a commercial related content, although they could have political theme, contain viruses or illegal and harmful content.)

¹³ see for example http://www.oecd.org/departement/0,2688,en_2649_22555297_1_1_1_1_1,00.html for the OECD work on spam and also <http://www.itu.int/osg/spu/spam/> for the International Telecommunication Union activities in combating spam (last visited July 16th 2005)

¹⁴ see for example; the Presidency Paper, “*Unsolicited communications for direct marketing purposes or spam*”, Council of the European Union, Brussels, 24 November 2004, 15148/04, Article 29 Data Protection Working Party’s “*Working Document Privacy on the Internet - An integrated EU Approach to On-line Data Protection*” 21st November 2000, 5063/00/EN/FINAL WP 37

¹⁵ “*Background paper for the OECD workshop on spam*”, DSTI/ICCP(2003)10/FINAL, 2003, page 7 available at [http://www.oilis.oecd.org/olis/2003doc.nsf/43bb6130e5e86e5fc12569fa005d004c/edfc2255d6a8a51ac1256e240030f5b6/\\$FILE/JT00157096.PDF](http://www.oilis.oecd.org/olis/2003doc.nsf/43bb6130e5e86e5fc12569fa005d004c/edfc2255d6a8a51ac1256e240030f5b6/$FILE/JT00157096.PDF) (last visited July 16th 2005)

d) the position of the receiver with regard to the spam message (for the receiver, the e-mail spam message is unwanted, unsolicited, unstoppable, as the unsubscribe links do not work).

All the traits identified above will serve as comparison items in the first two chapters of the thesis.

I should also state that the characterisation provided above is more narrow than the one available in the official EU Documents, thus comprising a more limited range of behaviours. Take for example the following definitions: *Spam* is “the practice of sending unsolicited e-mails, usually of a commercial nature, in large numbers and repeatedly to individuals with whom the sender has had no previous contact”¹⁶. Other definitions point out apart from the unsolicited and the commercial character some other different features commonly associated with spam: the fact that the “e-mail address has been collected in a public space on the Internet”¹⁷ or that the sender disguises or forges his identity”¹⁸. Finally, a more recent view of the European Commission, after the opt-in regime for unsolicited commercial e-mail messages was introduced by the Directive on privacy and electronic communications¹⁹, states that “in short, [spam] is commonly used to describe unsolicited, often bulk e-mails. The new Directive does not define or use the term ‘spam’. It uses the concepts of ‘unsolicited communications’ by ‘electronic mail’, ‘for the purposes of direct marketing’ which taken together, will in effect cover most sorts of ‘spam’. Therefore, the concept of ‘spam’ is used in this Communication as a shortcut for unsolicited commercial electronic mail”²⁰

As it can be seen from these definitions, the most common traits of the practice that I aim at analyzing refer to the commercial character, to some circumstances involving the collection of the e-mail address and to the fake identity of the sender. While these are essential traits, they are only detailed in the national legislations implementing

¹⁶ DPWP: “*Privacy on the Internet* (2000), 5063/00/EN/FINAL.

¹⁷ DPWP “*Opinion 1/2000 on certain data protection aspects of electronic commerce*”(5007/00/EN/final), page 3 http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2000/wp28_en.pdf (last visited July 16th 2005)

¹⁸ Serge Gauthronet and Etienne Drouard (2001), op.cit

¹⁹ “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”, Official Journal L 201, 31/07/2002, P. 0037- 0047

²⁰ COM(2004) 28 final, op.cit.

the Directive with little guidance as to the distinction between spam and e-mail marketing.

The other term of the comparison, “direct marketing” is commonly agreed as designating “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”²¹. By examining this, as well as other very broad definitions for the same concept²², it can be noticed that no references to the “etiquette” of the advertising messages is being made, which in itself explains the fuzziness of the dividing line between the e-mail marketing involving also unsolicited commercial communications and spam. By using the comparative method described above, I will try to separate more clearly the two concepts.

The thesis is, for obvious reasons, limited as regards the technical and practical aspects of spam. Although I will make references to legal texts, codes of conducts and guidelines, I am conscious that there is a difference between stated principles and business practices, and that the marketer’s day to day practice will seldom be “black or white” in terms of the conformity to the stated rules.

²¹ FEDMA (2005), available at:



<http://www.fedma.org/img/db/PressPackJan2005.pdf> (last visited July 28, 2005).

²² see for example the definition in the ICC International Code of Direct Marketing, 1998: “**direct marketing** comprises all communication activities with the intention of offering goods or services or transmitting commercial messages presented in any medium aimed at informing and/or soliciting a response from the addressee, as well as any service directly related thereto.

CHAPTER 1

Spamming as an advertising practice

Sat, 02 Jul 2005 20:12:51 +0500

From:	"Clifton Baker" <sotebdwuyec@hotmail.com>  Add to Address Book
To:	 dancogs2@yahoo.com
Subject:	re [16]

A Genuine College Degree in 2 weeks !

Have you ever thought that the only thing stopping you from a great job and better pay was a few letters behind your name? Well now you can get them!

BA BSc MA MSc MBA PhD



**Within 2 weeks!
No Study Required!
100% Verifiable!**

These are real, genuine degrees that include Bachelors, Masters and Doctorate degrees. They are verifiable and student records and transcripts are also available. This little known secret has been kept quiet for years. The opportunity exists due to a legal loophole allowing some established colleges to award degrees at their discretion. With all of the attention that this news has been generating, I wouldn't be surprised to see this loophole closed very soon.

**Order yours today!
Just call the number below.
You'll thank me later...**

+1-206-984-0021

Section 1: The role of personal information in the advertising practice today

Once the technological advances are employed “in the interest” of the individuals, inevitably they will reshape the way in which people organise their daily lives, the way they perceive themselves and their needs and the way in which they do business with each other. “As the most disruptive technological change since electricity”²³, the digital revolution caused significant changes, especially in the market for individual goods, challenging the traditional dichotomy between goods and services and allowing the trade of a larger category of items through a variety of mediums .

One of these changes relates to the dual impact of the digital technologies on the individual’s ability to maintain control over the environment in which he lives: while expanding the choices available and bringing diversity in both products and lifestyles, through enabling at the same time the acquisition, retention and secondary dissemination of vast amounts of data, the digital technologies allow the individual to a lesser extent to exercise informational self-determination, making him no longer able to assert with certainty what information about him is available and who controls it, much less how it got out of the private sphere into the public domain.

From the marketers’ point of view, personal data²⁴ regarding both the off –line identity of a potential client(credit card number, name, physical address) and the on-line identity of the same customer(e-mail address, individual tastes and browsing patterns, purchasing history) represent both an asset²⁵ and a commodity²⁶ in itself.

²³ Paul H Rubin and Thomas M. Lenard, “*Privacy and the commercial use of personal information*” ,Kluwer Academic Publishing, 2001, page 18

²⁴ According to the *FEDMA European code of practice for the use of personal data in direct marketing*, the term “personal data” used by direct marketers has the same meaning as the one consecrated by article 2(a) of the Directive 95/46/EC: “Personal Data means any information relating to an identified or identifiable natural person. 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.” (see page 3 of the Code)

²⁵ <http://www.answers.com/asset&r=67> an “asset” represents a resource that an individual, corporation, or country owns or controls that has economic value and that is expected to provide future benefit

²⁶ <http://www.answers.com/commodity> a commodity (business meaning of the term) is an undifferentiated product whose market value arises from the owner's right to sell rather than the right to use. Example commodities from the financial world include oil (sold by the barrel), electricity, wheat, bulk chemicals.

Subsection 1: Personal data as an asset.

Data on individuals has been used by marketers long before the advent of Internet. The advertising campaigns had to take into account the characteristics of the targeted group, such as demographic structure, consumer group, trends in buying as well as manifested interests or hobbies, in order to increase their positive response rate. While the consumers have been accustomed with providing customer data, that can be used for these types of profiling, but that, at the same time cannot be traced back to their source enough to make the respondents identifiable, the increase in the personal data exchanges occurring through the Internet raised awareness among consumers worried that their privacy is being threatened. Whether this concern is justified or not, deserves a much larger analysis; what is important in this context, since I initially qualified spam as an anomaly, is to be able to draw the line between legitimate commercial activities involving the use of personal information for direct marketing purposes and the illegal and illegitimate use of personal information in the context of spam.

We can consider personal data is an ASSET for advertisers by examining the two features comprised in the definition of the term: economic value and the ability to provide future benefits:

1. **The economic value of the personal information.** While traditional media of dissemination of advertising messages is more rigid as regards the adaptability of the content to the profile of a certain group or individual, marketing techniques used by the advertisers today allow them to target the advertising campaigns to smaller groups of people, based on customers' interests, as identified or inferred previously by the marketer through examining on-line activities. On the Internet, targeted advertising is accomplished by developing an understanding about the possible customer's interests and then matching and delivering relevant advertisements. As Rubin and Lenard (2001)²⁷ have shown, advertisers compile individual's web-browsing activities and apply database technologies and statistical models that yield demographic and interest profiles. Advertisements relevant to consumers' profiles are then inserted in the web pages they visit and website operators receive advertising revenues based on pages viewed and

²⁷ Paul H Rubin and Thomas M. Lenard, op.cit, page 8

advertisements delivered. Targeted advertising is therefore made possible by the use of personal information. Marketers are interested in the efficient allocation of their resources, and this implies not spending on advertising products or services that either is not of interest to a particular consumer group, or the commercial communication is not suited to appeal their level of understanding and interest.

Two processes should be distinguished here:

a) on the one hand is the collection and use of personal data in order to compile aggregated profiles that permit the identification of a particular set of characteristics that make a group desirable to a marketer. In this case, what is of interest is not the identity of one particular person(What kind of car can I sell to John Smith ?) but the possibility to determine clusters of consumers “ more likely than average to want a new car”. Data is widely available, being compiled by credit reporting agencies (data pertaining to name, social security number, address, telephone numbers, date of birth, a detailed credit and payment history plus information available from public records), companies (data aggregators) engaged in the collection, processing and reselling of information from all possible registries, as well as data collected through cookies, pertaining to one’s on-line behaviour (sites visited, number of times, click –through, products bought on-line, e-shops visited)²⁸. Some companies distinguish between data collected through opt-in procedures, and data collected through opt-out, with the first category being more expensive. It is then stored on servers, and “not known” individually by any human that only get to perceive the end-result of this process, clusters with common features, more likely to be interested in a certain product or service(this does not exclude the possibility to trace back and match data from different sources in order to compile an individual profile).

Once the raw information is gathered, it can “be used multiple times at a low marginal cost without any decrease in its value”. As the authors quoted point out²⁹,

“Advertisers, credit institutions and insurance companies all use the same commercial information because all find it valuable. Since the

²⁸ this information is mainly linked to the browsing patterns of a certain computer, but it is assumed there is an individual (or more people using the same computer) that uses it.

²⁹ Paul H Rubin and Thomas M. Lenard, op.cit., page 9

various uses of information subsidise each other, more information is collected and the cost to each of the users is reduced”

b) on the other hand, personal data is being collected as to enable the direct marketing of the “custom made advertisements”; this personal data pertains to the address, the telephone number or the e-mail address of the targeted customers, depending on the medium chosen for the dissemination of the advertising communications. Although it has been argued this sort of data is publicly available in directories, so it can be used without any limitations³⁰, there are solid grounds³¹ to protect their owners by unsolicited intrusions.

2. The ability to provide future benefits. One of the benefits in gathering as much information as possible about prospective customers has been pointed out already: in the short run, targeted advertising made possible by the use of personal information increases the positive response rate of the customers (increases their willingness to buy the company’s products and services), hence the increase in the company’s revenues.

The costs of a direct marketing campaign through e-mail, automated calling machines, sms, facsimile are much smaller than those involved in indirect marketing techniques, through television, radio, brochures. The reduced costs come first of all from the fact that the companies do not actually pay to get the personal information from the customers (they still sell their products and services to the customers for the price they set), but consider somehow it’s their right to use it once it was made available. On the other hand, there are no intermediary costs involved in the printing, distribution, mailing of the commercial messages, which can reach the potential customers directly. At the same time, the marketers have the benefit of being provided instantly with the feedback of their activity, once the members of the target group chosen either decide to buy or to discard the commercial messages received.

³⁰ according to David Silver, a direct marketer who uses spam, “If I look up a phone number in the White Pages, I have the right to call that number because it’s public information. So is the E-mail address that’s posted anywhere on the ’net. If I had to break in with a password to get that address, that would be illegal. But what I do is the same as opening the phone book. If someone doesn’t want bulk E-mail, they shouldn’t place their address anywhere that’s publicly accessible” (the interview was published by L. Goff. “A Line in the SPAM”. *Computerworld*, 88–89, August, 1997 and quoted by R.A. Spinello in “Ethical reflections on the problem of spam” article in *Ethics and Information Technology* **1**: 185–191, 1999)

³¹ as it will be shown further in Chapters 2 and 3 of this thesis

In the longer term the company will be able to optimize its distribution or resources and achieve economic efficiency and a bigger market share.

Moreover, some businesses, such as Yahoo, Google, use funds resulted from advertising to support and finance services that are free for the customers (such as free e-mail), the company will get the possibility to advertise its products and services to a larger group of people and also to collect more personal information from them.

Subsection 2: Personal data as commodity

What defines personal data as commodity is the fact that its market value arises not only from the right to use it but even more from trading it. Companies engaged in the collection, processing and storage of data pertaining to individuals rent these lists and perform various kinds of analysis for customers, thus enabling them to develop both traditional and web based direct marketing campaigns. Due to the multiplicity of uses that personal information has, it has become profitable to engage in the collection, storage, and reselling of personal information. Still, while it is clearly in the advantage of business, the reselling and re-aggregation of personal information from different sources has not been backed up by allowing the individual to control and to rectify the information about him that can be found somewhere on a Internet server, as it is the case with other processing of personal data. Ann Cavoukian suggested³² that:

“While personal information has been commodified or commercialized, there has not been a corresponding empowerment of individuals that would give them the ability to control how their personal information will be used, or for which they will be compensated. Companies can now freely collect, use or disclose personal information without having to pay any compensation...”

This opinion cannot be accepted without reserves. The commodification of the information has been accompanied, in Europe at least, by enacting legislation aimed at protecting the interests of the consumers. However, empirical studies³³ show the low level of awareness among individuals about the appropriate privacy enhancing technical mechanisms available on market as well as the ease with which the majority of consumers disclose personal information as long as they perceive an immediate benefit (access to a product or availability of a service) arising from this disclosure. Therefore, I

³² Ann Cavoukian, Information and Privacy Commissioner Ontario, “*Privacy as a fundamental human right vs. an economic right: an attempt to conciliation*” 1999 available at http://www.ipc.on.ca/userfiles/page_attachments/pr-right.pdf (last visited July 18th 2005), page 14

³³ see: Tamara Dinev & Paul Hart: ‘*Privacy Concerns And Internet Use – A Model Of Trade-Off Factors*’ (2004), G.R Milne & A. J Rohm & S. Bahl: ‘*Consumers’ Protection of Online Privacy and Identity*’ The Journal of Consumer Affairs, vol. 38, no. 2, 2004

do not envisage the lack of the “corresponding empowerment” as a legal vacuum, but rather as a practical consequence of the existing informational asymmetry between the parties.

One of the negative features of the secondary uses of the personal information is that the individual, even if he agreed to some “sharing” of his personal data to “favorite, selected, well reputed partners” knows very little about the processes actually involving the personal data he discloses (especially since his consent will not be further asked for when the “well reputed partner” sells further the data it received), but is only faced with the end-consequences of this disclosure: some advertisements rather than other, certain unsolicited commercial e-mails.

In this context, if the e-commerce is to enjoy further the consumer’s interest and trust, marketers and businesses should respect the individual’s preoccupation for their own privacy thus keeping in focus the difference between what is technologically possible to be achieved and what it is ethical to be achieved(and ultimately in the interest of a good public image). Respect in this case cannot be limited to a general declaration of good practice, but should be effectively implemented into the business practice of those dealing with it.

Section 2: E-mail address as personal data

As shown in the previous section, the use of personal data in direct marketing, raises concerns among the data subjects regarding their ability to exercise control and to keep track of the personal information available about them on-line and about the way this information is used. To be able to tell if their concerns are justified and to discuss whether or not appropriate protective mechanisms are in place, a more fundamental question needs to be answered first. What exactly is the information about which the individuals claim protection?

If few people would doubt that a social security or a personal ID number are personal data, as well as the credit card number or bank account and the information that can be drawn from it (spending patterns, purchases made, solvency). However, the e-mail address is more difficult to qualify due to its intrinsic features and its function. I will discuss these aspects in the following lines.

Formally speaking, an e-mail address is formed by two parts separated by the @ character.

The right part identifies the host where the recipient has an account. Since the mail server can host a great number of e-mail addresses, this part rarely constitutes personal data when the e-mail service is free of charge and accessible worldwide (take a.b@yahoo.com or a.b@gmail.com). On the other hand, if the rightful holder of an e-mail address is a business, the right part of the @ sign easily enables the identification, due to the fact that it coincides with the website address and most likely the trademark of the business. For example, a business registered as “Advances”, has <http://www.advances.ro/> as a website address and office@advances.ro as a contact e-mail address.

On the left side of the @sign, a group of characters (letters and numbers most if the times) describes “the name” with which a user is known by the e-mail service. While it is true this name is unique for every e-mail account opened within an e-mail host server, there is no technical obligation that the identifier be the actual name of the individual opening an account, and there are no limitations regarding the number of on-line identifiers (e-mail addresses) that a person can have. In fact, most of the users have at least two e-mail addresses, one for business, and the other one for personal

communications. At the same time, the e-mail account can be accessed from any computer connected to the Internet, no matter where it is located.

On the other hand, the most important criteria in order to qualify certain data as being personal is its ability to lead, directly or indirectly to the identification of the individual to whom they belong³⁴. In the law literature this criteria has been contextualized by reference to the relevant agent of the identification, the ease, the precision or the validity of the identification³⁵. What is important here is that the identification was seen as leading to a “flesh and blood” person, and not to a simple on-line identity, that does not necessarily coincide with the legal³⁶, off-line one. Can the e-mail address pass this test? Does the e-mail address contain enough information so as the identity of an actual living individual be brought to light by employing “all means likely reasonably to be used”³⁷. If the e-mail address was registered as belonging to a certain “John Smith”, does this mean that John Smith actually exists or that he is the one registered in the phone book as John Smith? Since the use of the e-mail address is not dependant on a fix IP address from where the real John Smith communicates, can we say that the identification process finished once it has been established, predictably otherwise, that the address belongs to “someone”? I was not able to find the final answer to any of these questions, although I’m convinced that it is technologically viable to claim that such a connection can be established in special circumstances, by using additional data regarding, for example the use of a certain credit card associated with someone registering on a site with the e-mail address and a password. It is my personal opinion that the “personal data” character of e-mail address is taken for granted since I was able to find lots of indications both in law, and in official documents³⁸, that e-mail address is, in fact, to be seen as personal data, but without any further explanations. As I see it, one reason for this is that is a real, actual person (legal or natural) who suffers the

³⁴ see article 2(a) of the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of the individuals with regard to processing of personal data and on the free movement of such data, Official Journal L 281, 23/11/ 1995 P. 0031-0050

³⁵ Lee A. Bygrave, “DATA PROTECTION LAW, Approaching its rationale, Logic and Limits”, Kluwer Law International, 2002, page 42

³⁶ and by legal identity I mean the one recognized by the law, and confirmed by identity cards, birth certificates, administrative acts and so on

³⁷ see recital 26 of the Directive 95/46/EC

³⁸ for example, Presidency Paper (2004) (15148/04), op.cit., and DPWP *Opinion 1/2000* (5007/00/EN/final)

costs (pecuniary or not) associated with any misuse of the e-mail address. But is it enough to make this person identifiable?

Although national laws implementing the 95/46/EC Directive have transposed the broad expression in article 2(a) of the Directive, making use of unquantifiable terms like “relating to” or “that can be linked” or “concerning” an identified/ identifiable individual³⁹, two examples can be offered to illustrate how, in practice, national courts can reinterpret the legal texts so as to introduce a supplementary criteria in order to determine if data should be regarded as personal in a certain context, and award it protection as such.

The first example is the Eastweek case⁴⁰, in front of the Hong Kong Court of Appeal, not an European case, however a good example of case law for the issue in discussion. Although the Personal Data (Privacy) Ordinance did not specify this explicitly⁴¹, the Court decided that it is of the essence of the act of personal data collection that the data user is compiling information about “an identified person” or about “**a person whom the data user intends or seeks to identify**”. In the case, the fact that photography, when published, was capable of conveying the identity of the subject did not make the act of taking the photograph an act of personal data collection if the photographer acted without knowing or being at all interested in ascertaining the identity of the person being photographed.

Depending on the interpretation given, two conclusions could be inferred from this case, and they are both relevant for the present discussion. We can say either that data is not to be regarded as personal if its collector did not intend to use it for identification purposes, or that not any collection of personal data is to be subjected to the same exigencies: if the data controller wishes to identify a person based on the collected data more stringent principles and rules should be in place than in the situation where such an intention is absent.

Referring now back to the explanations I provided in the second section of the first chapter, what has been reproached to spammers is the fact that, as opposed to the e-

³⁹ see http://europa.eu.int/comm/justice_home/fsj/privacy/nationalcomm/index_en.htm for texts of national data protection laws

⁴⁰ information about the case can be found at <http://www.hkreform.gov.hk> , *Eastweek Publisher Ltd v Privacy Commissioner for Personal Data* [2000] 1 HKC 692

⁴¹ see article 1(2) of the Ordinance

mail marketers, they send the commercial e-mails indiscriminately and in bulk, and not adapt their message to the interests and wishes of the potential receiver. The addresses are collected from public spaces or guessed through specially designed software. It is obvious that the spammer has no intention to discover preferences and to establish a personal profile of the person whose address is collected and used. In fact as long as the address is active and in use, for a spammer it represents just an environment through which it makes known the indiscriminate message that was meant to be sent. If the European Courts would apply a similar criteria, there would be little justification for the individual's privacy intrusion claims (which does not mean they would not have an action if they proved the financial and personal damage subsequent to receiving spam, but this action would have a different legal basis than a privacy infringement claim)

The second example is the Durant case⁴², in the UK, where the Court of Appeal stated that some information shall not be regarded as personal, even if the name of the person appears on it. The "name will only be 'personal data' where its inclusion in the information affects the named individual's privacy." The mere reference to a person's name where the name is not associated with any other personal information is given as an example of information that is not to be regarded as personal.⁴³ Would the e-mail address pass this test? It is interesting that the name associated with the person's address is regarded by the UK Information Commissioner⁴⁴ as personal information. The e-mail address includes both, the person's on-line name (or at least one of them) and its on-line address (or at least a P.O box) so it would appear that the question could receive a positive answer.

As mentioned before, several official European documents state directly or let one infer that e-mail addresses are personal data. The 2002 Privacy Directive states in Recital 26 that the traffic data "contain information on the private life of natural persons and concern the right to respect for their correspondence or concern the legitimate interests of legal persons". Considering the provisions of Recital 15 and article 2(b) of the

⁴² Durant v Financial Services Authority [2003] EWCA Civ 1746, Court of Appeal (Civil Division), UK

⁴³ see <http://www.jonathanmitchell.info/uploads/Durant.pdf> for the Information Commissioner's comments

⁴⁴ *ibidem*.

same Directive, e-mails could be included in this category⁴⁵. More directly, in the wording of Data Protection Working Party, *“the e-mail address is indispensable in establishing a connection. It is also, however, a valuable source of information which includes personal data on the user”*⁴⁶. The same institution, the Data Protection Working Party, in a document regarding the minimum requirements for collecting personal data on-line, dedicates one chapter to the “Collection of addresses for direct marketing by e-mail and the dispatch of newsletters”⁴⁷. Moreover, the UK Direct Marketing Association in its Code of Practice, states explicitly that “business information and e-mail addresses from which a living individual can be identified may also be regarded as personal data and therefore should be covered by these rules”⁴⁸.

While the legal instruments quoted above have different binding force on the Member States⁴⁹, they have an unquestioned authority on the enforcement authorities of a Member State, especially absent an explicit provision in the Directives stating the fact that e-mail addresses are personal data.

⁴⁵ see also DPWP 5063/00/EN/FINAL The following items are normally considered to be included under the definition of "traffic data":

- ☐ e-mail address and IP address of sender
- ☐ type, version and language of the client agent
- ☐ e-mail address of receiver
- ☐ date and time of sending the e-mail

⁴⁶ DPWP “Privacy on the Internet” (2000), op.cit., pp. 32,

⁴⁷ DPWP “Recommendation 2/2001, 5020/01/EN/ Final, Chapter 4, point 28, available at: http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2001/wp43en.pdf (last visited July 31, 2005).

⁴⁸ section 5.3 of the Code of practice for direct marketing (3rd edition), available at www.dma.org.uk (last visited July 31, 2005).

⁴⁹ as pointed out in the Introductory Chapter, the opinions of the Data Protection Working Party are non binding instruments, whereas the provisions in the Directives need to be transposed, as a rule, by the Member States into national laws.

Section 3: E-mail marketing and spam practices⁵⁰

After having explored in the first section of this chapter the importance of personal data for the advertising practice today, and argued on the personal data features of the e-mail addresses, it is important to comment on some of the practices that, *de facto*, set the dividing line between e-mail marketing, as legitimate practice, with proven benefits both for the customers and marketers, and SPAM as nuisance and anomaly having “reached worrying proportions”⁵¹. The features of the two distinct practices will be high lightened through the four relevant categories used in the Introduction, for the purposes of defining spam.

1. the means to collect the e-mail addresses

It is possible for the interested parties⁵² to get hold of possible customers’ e-mail addresses :

- a. directly from the owner of the address, who agrees to disclose his address in order to receive certain types of commercial communication – this is a typical situation of permission based marketing. This method sets the basis for long-term commercial relation between the parties based on trust and mutually beneficial.
- b. indirectly, without the knowledge of the e-mail address owner,:
 - *who is unaware that his address will be used in the future for direct marketing* .

This is the typical situation where the user posts his address in a public space on the Internet. The user disclosed his address for purposes different than that of receiving commercial communications from different marketers. However, spamware tools can be employed in order to automatically navigate websites, newsgroups and chat rooms and collect the e-mail addresses found there.

Whereas the “collection of e-mail addresses from public spaces on the Internet

⁵⁰ more technical details relating to the e-marketing and spam practices can be found in two studies: Rubin & Lenard (2001), op.cit. and Gauthronet & Drouard (2001). However, it is beyond the scope of this thesis to present them in similar level of detail.

⁵¹ COM(2004) 28 final .

⁵² I will use the term “ marketer” to designate the person that uses direct marketing, as prescribed by the law and the various codes of good practice, and the term “spammer” in order to designate the person that does not comply with the same rules, while engaging in direct marketing.

for the purposes of unsolicited commercial e-mail ” has been considered “contrary to the existing community legislation”⁵³, studies have shown that the addresses posted on public spaces of the Internet are the main source of the spammers thus exposing their owners to the greatest amount of spam⁵⁴.

Another typical situation is that of the insufficiently attentive user that was misled by the wording or the design of the webpage and was not aware that he gave his consent (especially when the marketer uses a pre checked box, or a negative option statement⁵⁵). While this technique does not in theory amount to spam, as somehow consent was asked and given, marketers are recommended not to use this strategy, as the image they create in the eyes of the customers will be negative⁵⁶, and the results doubtful⁵⁷

- *who is unaware that that his address is being harvested at all.* This technique is clearly typical for spam. Such a "brute force" attack on the mail server, where the software used by the spammer sends spam messages to all possible combination of letters that could form an e-mail address, generated a tremendous amount of spam, even to addresses that hadn't been shared anywhere⁵⁸. There is little that can be done by an individual user when faced to this sort of spam, unless he chooses a more complicated e-mail, more difficult to detect through “dictionary attacks”.

See the following example:

⁵³ DPWP(2000), 5063/00/EN/FINAL, op.cit.






⁵⁴ “Why Am I Getting All This Spam?” Unsolicited Commercial E-mail Research, Center for Democracy & Technology March 2003, available at: <http://www.cdt.org/speech/spam/030319spamreport.pdf> (last visited July 28, 2005).

⁵⁵ checking a box, calling or writing the marketer if the customer does NOT want to be on a mailing list

⁵⁶ “It is in the interest of business to be able to use legitimate commercial e-mail and be associated with ethical e-mail marketing using industry codes of conduct such as these guidelines. Unfavorable attitudes generate consumer skepticism and can lead consumers to take actions that are catastrophic to businesses” ICC Guidelines on Marketing and Advertising using Electronic Media, 2004.

⁵⁷ “the negative option statements was relatively inefficient, whereas the yes/no format proved to be more efficient: more honest way of asking for permission than a negative format , more conducive to building customer relationships. Consumers see the direct yes no format as an invitation, whereas the negative option as a challenge”: George R. Milne (1997), study regarding consumer’s willingness to provide marketers with personal information and permission to rent this information given in varied permission formats. The author commented also that as customers become more aware of the transfer practices, they may come to expect that marketers will be more straightforward in their communications.

⁵⁸ According to CDT (2003) study, see footnote 54

Date:	Mon, 04 Jul 2005 07:24:41 -0500
From:	"Steve Dauman P.manager" <seabird@infinito.it>  Add to Address Book
To:	 dancohen58@yahoo.com
CC:	 dancohn1@yahoo.com,  dancoi2000@yahoo.com,  dancointl@yahoo.com, dancoj2000@yahoo.com
Subject:	The unique possibility to increase your income. Protection code:GE-4177

2. the transmission practices: are, in my opinion, the main trait distinguishing e-mail marketing from spam. Although both practices involve electronic unsolicited commercial messages, the marketers and spammers use different strategies to get their message through to their potential customers. First of all, spamware programs can automatically generate false headers and false return address information⁵⁹. On the other hand, this practice is banned by the existing legislation and the applicable codes of practice, both in Europe and in the US⁶⁰.

Also, mailing tools used by spammers are capable of sending bulk e-mail without going through a specific mail server or ISP⁶¹, which avoids the trouble of being detected or having their accounts terminated due to the way they exhaust the bandwidth. Although marketers send as well the same e-mail advertising message to a great number of potential customers, they usually belong to the same cluster or are considered to have a special interest in the product or service being advertised. "If marketers failed to identify proper target groups and send unsolicited e-mail to massive audiences, negative effects

⁵⁹ *Background paper for the OECD workshop on spam*, DSTI/ICCP (2003)10/FINAL, 2003.

⁶⁰ see for example Recital 43 of 2002/58/EC Directive and Section 5(a) of the US CAN-Spam Act, as well as article 3 of the ICC Guidelines on Marketing and Advertising using Electronic Media, 2004, Section 2.1 of the European Code of Practice for the use of personal data in Direct Marketing, FEDMA 2005.

⁶¹ Serge Gauthronet and Etienne Drouard (2001), *op.cit*, page 32.

could be tremendous”⁶², potentially facing the contempt of both the customers and the business community (complaints to upper administrative bodies, black listing).

Spam is also repetitive, and arguably very difficult to stop, since the unsubscribe lines do not work⁶³. According to the OECD Paper on Spam⁶⁴, spammers either open free e-mail accounts which they abandon before getting caught, or load in multiple accounts, so that when one of them is terminated, another one becomes automatically active. The marketers’ practice has to involve as a fundamental requirement, the possibility for the customers to opt out from receiving further commercial messages⁶⁵.

Taking into account the e-mail harvesting methods used, it is easy to realise that spam messages are untargeted and indiscriminate as to the potential receiver. In fact, a big part of the nuisance caused by spam to the users is represented by the discomfort of constantly having to spend time and effort, as well as money in order to get rid of unsolicited, useless⁶⁶ emails. On the matter, the Guidelines⁶⁷ issued by the International Chamber of Commerce recommend in article 9 to all marketers, that in case they do send unsolicited commercial e-mails as part of their marketing strategy, they should “have reasonable grounds to believe” that the consumer targeted will find the offer of interest for him.

3. the content

From the point of view of the content, there are similarities between spam practices and e-mail marketing. Although spam can include scams (humanitarian or phishing), pornographic content or viruses, the great majority of it is still aiming at

⁶² Susan Chang, Mariko Morimoto “An Assessment of Consumer Attitudes toward Direct Marketing Channels: A Comparison between Unsolicited E-Mail and Postal Direct Mail” Michigan State University April 1, 2003 available at <http://www.inma.org/subscribers/papers/2003-Chang-Morimoto.doc> (last visited 2005-07-28).

⁶³ in fact, users are advised not to click on the unsubscribe links (if they are provided), as they will only thereby confirm that the address is valid, used...and good to spam further.

⁶⁴ See above, footnote 59

⁶⁵ as I will point out both in Section 1 Chapter 3 of this thesis

⁶⁶ studies quoted in the OECD Paper on SPAM claim that even a very low response rate (0.001%) is enough to make spamming profitable (see page 9) due to the low costs involved in producing and sending them.

⁶⁷ “These Guidelines (...) are an expression of the business community's recognition of its social responsibilities in respect of marketing activities and communications. The Guidelines have been updated in light of experience acquired, and ICC, conscious of the ongoing development, commits itself to regularly review them to ensure their continued viability”

advertising products and services. What differs often is the quality and the truthfulness of whatever “special offer” is being presented there.

4. the position of the receiver with regard to the unsolicited communication received.

The overwhelming majority of customers don’t like receiving spam. It’s unsolicited, unwanted, useless and unstoppable. It imposes unjustified costs on the targeted end-users without bringing any benefit. Some distinctions should be made here regarding the terms used. While the offers received from a company that sold you a computer might be seen as “unsolicited”, there is a high likelihood that they are “wanted”, and “useful” (even if I don’t choose to buy the products or request the services, I can be thus informed about the latest products available and even compare prices and find out whether a better offer is available on market for something I’m interested in). According to EASA⁶⁸, once the individual has given his consent to the use of his contact details for marketing purposes, all the subsequent communications he receives from that source are deemed to be “solicited” even if the individual is not aware of the future content of these communications. While I don’t argue the level of expertise in this Communication, I don’t agree with the interpretation of the meaning of the verb “to solicit”⁶⁹. While the commercial communications subsequent to a manifestation of consent cannot be seen as spam, they are and remain unsolicited, but they deemed to be accepted, wanted, useful (for as long as the consent is not revoked through the exercise of the right to opt-out). In my view, you cannot solicit something and not know what you will receive as the result of your solicitation.

It can be argued that the customers had to deal with unsolicited commercial communications as a result of direct marketing long before the Internet came into play, and this is one of the risks inherent to having multiple choices in terms of offers for similar products and services. The marketers become more aggressive in bringing their offer in the attention of the public. However, the level of consumer annoyance when faced with unsolicited e-mails is, for some consumers, higher than in case of other forms

⁶⁸ “Recommendations for the issue paper for the EU Workshop on unsolicited commercial communications or spam”, November 4th 2003, page 4 available at, http://www.easa-alliance.org/news_views/en/position_spam%20issue.pdf (last visited July 28, 2005)

⁶⁹ To make solicitation or petition for something desired, to seek to obtain by persuasion, entreaty, or formal application, synonyms: to ask for, to request, to seek

of unsolicited direct marketing (brochures in the mail, for example)⁷⁰. The receivers have to bear the online service costs according to the time spent online, risk losing important mail due to limitation in the storage space of their e-mail boxes, and waste time sorting out the important e-mails from the unwanted ones.

These are inconveniences that the end users have not faced before and the cumulative social and economical impact of this unfair business practice, spam, called for special measures to limit and if possible put a stop to it.

⁷⁰ see Susan Chang, Mariko Morimoto, *op.cit*, page 6

CHAPTER 2

Values and interests involved in spam practices

“Whereas data-processing systems are designed to serve man; whereas they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably their right to privacy and contribute to economic and social progress, trade expansion and the well being of individuals”⁷¹

Section 1: Different interests that need to be safeguarded by the anti-spam legal provisions

The European legislator adopted a two-sided approach to the spam phenomenon. One of the approaches views spam as an illegitimate marketing technique and thus provides for corrective mechanisms pertaining to the e-commerce activity, reflecting at the same time the need to ensure the growth of e-commerce and the competitiveness of the European industry⁷². The other approach considers that spam involves most of the times, an illegal processing of personal data, and providing therefore safeguards aimed, for the most part, at protecting the individuals whose fundamental right of privacy is infringed through the personal data processing, and leaves to the Member States the choice of an appropriate mechanism for the protection of the “legitimate interests of the legal persons”.

It is manifest therefore, that in finding the appropriate dosage for the legislative antidote to the spam anomaly, the normative solutions (and all other solutions for that matter) have to weight the different values and interests that different actors claim recognition upon.

⁷¹ “Directive 95/46/EC, Recital 2.

⁷² See Recital 2 of the E-commerce Directive

On the one hand, as pointed out in Section 1 of the first chapter, direct marketers grasped the utility of building consumer profiles, targeting audience with their commercial message and allocating resources in a more cost-effective way. While “interruption marketing”⁷³, an advertising practice that interrupts people from whatever they are doing (watching a movie, reading a magazine, walking on the street) is losing its efficiency⁷⁴, permission based marketing is only starting to prove itself. Targeted advertising by e-mail, for example, involves limited costs and exposure of the advertised products or services potentially to a worldwide market. Hence, the main interest of the direct marketers is the economic profitability of businesses, both in terms of reducing the costs associated with the provision of the services or the supply of goods and in terms of increasing their revenues resulted from the business activity. This particular business interest can of course be correlated with additional ones, relating, for example to gaining the trust of customers, as well as with the overall development of competitive European e-commerce services. All of these might be broken down into smaller and more detailed interests and associated values. This fragmentation is however beyond the scope of this thesis. Using instead a simple mean of expression, I will refer to these interests as “economic incentive interests”.

On the other hand, within the e-mail marketing activities (and implicitly⁷⁵, in spam) the end – users have interests that pertain to the different perspectives from which their involvement can be seen: as prospective clients or as the holders of the e-mail addresses used to disseminate the commercial messages.

As prospective clients, the receivers of the commercial messages are first of all interested in having information, about a large number of products and services. However, if they are to benefit from the broad offer, the information about it needs to be complete (that is, to include all details that are needed for a subsequent purchase), accurate (truthful), and last but not least, useful (that is, to correspond to a present or potential need). Secondly, the potential clients are interested in having access to the goods and services available on the market, that is, to be able to use the appropriate

⁷³ Seth Godin: “Permission Marketing: Turning strangers into friends, and friends into customers” Simon & Schuster –New York-1999

⁷⁴ idem, pag.75

⁷⁵ i am considering here the traits that are common to the two activities, as explained in Chapter 1 Section 2

electronic communication tools that would enable them to purchase the good or service they desire. Once they discover various e-commerce applications (such as on-line reservations, ATMs, web purchases, goods and services readily available for on-line use or download, access to databases) and acquire positive experiences from using them, the great majority are not likely to give them up. When it comes to being the receivers of a commercial offer by e-mail, businesses as potential clients (within business-to-business relations) can be said to have the same interests as the consumers in that regard⁷⁶; this view is otherwise reflected by the E-commerce Directive, which subjects the commercial communications⁷⁷ to the same legal regime, without discrimination in relation to the type of legal personality of the receiver⁷⁸. In practice, this means the same freedom of choice for the Member States, according to the E-commerce Directive to permit or to forbid unsolicited commercial communications, and the same transparency requirements, though not necessarily the same rules will apply for business-to-business and business-to-consumer communications within the same Member State (that can prohibit one and permit the other, with associated safeguards).

From a different perspective, the end-users can be regarded as holders of the e-mail addresses used to disseminate the commercial messages. As explained in Section 2, most of the times, the e-mail addresses can be regarded as personal data (and in fact they are treated in the existing legislation and in the doctrine as such). By using the term “holders”, I do not intend to suggest my adhesion to the doctrine claiming the data subject’s ownership over his own personal data⁷⁹, but merely that e-mail addresses are the part of the on-line identity of a certain user, whether he is a corporate (office@business.ro) or a private person (a.b@serviceprovider.no). In what it is regarded as the European legislative answer to spam, the existing privacy legislation discriminates between the two categories, providing safeguards for the “privacy interests” of the

⁷⁶ this does not exclude a different valuation of these interests as well as a different manner to express them, and different safeguarding mechanisms available to each of the two groups: businesses and consumers

⁷⁷ see articles 6 and 7 of the E-Commerce Directive.

⁷⁸ one exception is the reference to the opt-out registries in which “natural persons” can register themselves (article 7(2)).

⁷⁹ see James Rule & Lawrence Hunter: *‘Towards property rights in Personal Data’*, Kenneth C. Laudon : *‘Extensions to the Theory of Markets and Privacy: Mechanisms of Pricing Information’*.

subscribers that are natural persons⁸⁰ and recognising the “legitimate interests of the legal persons”.

The privacy interests of the individuals have been thoroughly commented⁸¹, and some of the findings can be applied for the present discussion, which considers only those interests that are involved in the e-mail marketing activity and endangered by the spam practices. Empirical studies further document the nature and the intensity of privacy concerns perceived by the data subjects when approached by a direct marketer⁸². Considering the dichotomy made by Bygrave (2002)⁸³, they pertain mostly to the interests of individuals as data subjects, although it can be said that the individuals hold also some interest in the uses to which personal data is put (for example when spammers collect and use e-mail addresses beyond the original purpose of their release by the holder). As data subjects, the individuals are interested in maintaining control over and in determining freely how others process their personal data (informational self-determination)⁸⁴. This informational self determination includes⁸⁵, insight (the interest of the data subject in knowing who is processing data about him and why), outflow control (the flow of information from himself to others, in this case what information about him are known to the marketer) as well as inflow control (the end-user’s interest in controlling what information he receives from the others) and has close links with the interest in attentional self determination (that is the interest of the end-user in being able to direct his attention to what he chooses).

Due to their specificity, these interests still stand when the unsolicited commercial e-mail message is sent to the legal persons (although they might not be justified through privacy rights⁸⁶). They are the expression of a legal person’s need to act autonomously and to use rationally and efficiently the resources it possesses. Several studies attempt to calculate the financial loss of companies due to the spam messages sent

⁸⁰ see article 13 (5) of the 2002 Privacy Directive, read in accordance with Recital 40 of the same Directive.

⁸¹ See Lee Bygrave (2002) op.cit., Chapter 7 and the sources cited therein.

⁸² see, for example, Alessandro Acquisti, Jens Grossklags (2005), “*Privacy and rationality in individual decision making*”, Alessandro Acquisti, Jens Grossklags (2004) “*Privacy attitudes and privacy behaviour*”, Dinev & Hart (2004), op.cit., Bartel & Hoy (2000), op.cit., George R. Milne (2000), op.cit., George R. Milne (1997), op.cit., Ross D. PETTY (2000), op.cit., Chang, Morimoto (2003), op.cit.

⁸³ Bygrave (2002), op.cit, page 150.

⁸⁴ see Section 1 of Chapter 2 in this thesis

⁸⁵ See Bygrave (2002), op.cit, 151

⁸⁶ see Bygrave (2002), Chapter 12

to their e-mail addresses⁸⁷. These costs comprise the loss of productivity⁸⁸ as the employees are wasting time sorting and purging their accounts from unwanted mail (especially since they have to discern between spam messages and other unsolicited but wanted commercial e-mails), investment in spam filters and associated costs (implementation , supervision)⁸⁹ and increased dial up costs due to extra time spent on-line. It is obvious that the businesses have a legitimate interest in the profitability of their activity and therefore this interest needs “sufficient protection” too.

Although the interests presented above are not necessarily conflicting, in the attempt to protect one value from the negative effects of spam, other values suffer side effect limitations also. For example, in the attempt to cut down spam, measures aimed at controlling the collection of e-mail addresses and protect privacy can be regarded by the marketers as a disincentive for e-commerce and a barrier to entry, especially for SMEs starting to do business on-line. Similarly, the exchange between partner firms of lists of e-mail addresses collected within customer relations, arguably acceptable as business practice, is questionable from the personal data protection perspective.

Section 2: Unsolicited commercial communications – a concern for individual privacy?

The difficulty in answering this question resides in the complexity of the notion “privacy” and in the multitude of values and interests safeguarded by the data protection laws⁹⁰. By examining the specificity of the data processing conducted for the purposes of direct marketing, I can argue that the most significant privacy concern of the individual faced with the massive phenomenon of spam is the lack of control over the use of his personal data, including here the related interest in attentional self determination. Lack of

⁸⁷ See for example “SPAM-The serial ROI killer” (2004), available at <http://www.nucleusresearch.com/research/e50.pdf> (last visited 21 Aug. 05), See also Gauthronet, Drouard (2001), op.cit. at page 67. These findings are consistent with many others, such as:

⁸⁸ £460 per UK employee per year in wasted time, according to Jean-Jacques Sahel International Communications DTI, United Kingdom, see <http://www.oecd.org/dataoecd/34/3/33713587.pdf> (last visited 21 Aug. 05)

⁸⁹ see Matthew Prince (2004), op.cit. pp. 8 (last visited 21 Aug. 05)

⁹⁰ see L.A. Bygrave, op.cit., especially Chapters 3 and 7.

control implies also the inability to make choices about the boundaries of one's own privacy. First of all, the individual becomes little aware or not aware at all when his personal data is collected. Secondly, the individual becomes *post factum* aware that his personal data was subjected to secondary uses, to which he hasn't consented. Most spam studies consulted for the purposes of this thesis contained, at a certain point, an attempt to answer the question: "Where did the spammers get my address from?" The Data Protection Working Party underlined also the importance of providing to the subjects sufficient guarantees and adequate information so that they are able to "place their trust in the sites with which they enter into contact" and to "exercise choices"⁹¹.

While personal privacy is recognised as a fundamental human right⁹², its scope and ambit are difficult to define through the adoption of uniform and universal standards, as different individuals value differently their own privacy, thus building their own hierarchy of rights. Therefore, they are willing to sacrifice one for the sake of the other according to cognitive and emotional resolutions, that are hard to anticipate and even harder to generalise. However "while privacy protection is an individual concern, its effective enforcement may only come through collective action"⁹³.

Somehow spontaneously, individuals tend to regard personal information about them as "belonging" to them, that they feel like being its rightful owners, therefore claiming a right to choose to whom and in what circumstances to disclose it. Since the e-mail address as online identity is mine, and I am the only one using it, I must be given the right to choose to whom it will be disclosed (and I am not considering here the situation in which the disclosure is compelled by a public authority exercising its authority). At the same time, if the Inbox is my personal space online, it can be assimilated to my home: it is out there in the street so everyone can see it, however, I decide who is allowed to enter and for what purpose.

On the other hand, the large scale availability of personal data, as well as the apparent lack of any enforceable ownership rights over it, favours the direct marketers' tendency to view personal information as a public good, largely available, that can be simultaneously possessed by all the individuals, whose consumption rights are not

⁹¹ DPWP 5020/01/EN/Final Recommendation 2/2001

⁹² see article 8(1) of the European Convention of Human Rights

⁹³ see Ann Cavoukian (1999), *op.cit.*, page 7

exclusive⁹⁴, and whose exploitation can ultimately bring financial benefits for all the parties involved.

The need to settle this divergence of opinion over the ownership of information lead to the creation of the concept “information sensitivity” that was supposed to scale the level of privacy concern felt by a consumer in a particular situation about a certain type of data⁹⁵. However, it appears that the conclusion reached reinforced the belief that privacy concerns are mostly situational.

According to George R. Milne⁹⁶, consumer privacy has been defined as the consumer’s ability to control (a) the presence of other people in the environment during a market transaction or consumption behavior and (b) dissemination of information related to or provided during such transactions or behaviors to those who were not present.

As the marketers aim at targeting their offer to the manifested interests of their customers, today’s marketplace tends to be more and more customer tailored. Therefore participating in the commercial exchanges and benefiting from a wide variety of goods and services implies giving up some of your privacy. This trade-offs between equally important interests should be based on rational decisions reached by informed consumers. Many consumers provide willingly personal information when they sign up for mailing lists so they can be contacted at a later date. Others provide information if they are sufficiently rewarded with a benefit manifested through better targeted offers or guarantees about subsequent contact or use of the information.

According to Ross D Petty⁹⁷, consumers might be hesitant to provide marketers with information as long as the resulting contact they receive from direct marketers is too costly, including the non pecuniary transaction costs of ignoring and disposing of information, as well as pecuniary costs of paying for unexpected telephone charges or disposal/recycling fees.

⁹⁴ see Ann Cavoukian (1999), op.cit, page 14

⁹⁵ Kim Bartel Sheehan and Mariea Grubbs Hoy “ Dimensions of privacy concerns among online consumers” *Journal of public Policy and Marketing*(2000), 19 spring, 62-73

⁹⁶ George R.Milne, “ *Privacy and ethical issues in database/ interactive marketing and public policy: a research framework and overview of the special issue* ” in *Journal of public policy and marketing*, vol. 19(1), spring 2000, 1-6

⁹⁷ Ross D PETTY, “ Marketing without consent: consumer choice and costs, privacy and public policy”, *Journal of Public Policy and Marketing*, no.19 (spring) 2000, pages 42-53

I found most interesting and relevant to the discussion about privacy concerns related to the unsolicited commercial e-mails that, according to Bartel and Hoy (2000)⁹⁸, privacy concerns among on-line consumers appear when the information usage is not expected by the consumer, either because he was not aware that his personal data was used, or that the use was different from the one originally intended. The authors correlate their empirical findings with the ones reached by Cranor, Reagle and Ackerman (1999)⁹⁹, that evidenced the fact that when consumers were asked to provide their e-mail addresses, the information was not perceived as sensitive and therefore did not produce privacy concerns. However, the “fear of unfamiliar” caused by the inability to trace back the circumstances in which the marketer acquired the e-mail address increased their concerns¹⁰⁰

Overall, Bartel and Hoy (2000) estimate that their findings confirm earlier studies suggesting that privacy is a measure of the control of the transactions between the individual and others. When the transaction is immediate and involves only an exchange between a consumer and one entity, the consumer will feel more in control and thus, less concerned about privacy.

As the transaction extends to multiple entities, beyond the user’s knowledge (as it is often the case when e-mail lists are traded between marketers), the consumer experiences loss of control thus increasing its concern for privacy.

What seems obvious from the above mentioned studies is that in discussing privacy issues the private sector commercial interests need to be taken into account, in addition to the traditional human rights or ethical perspective. At the same time, the advantages provided by the direct marketing techniques can not be fully taken advantage of unless the personal data collected as part of the electronic transaction is strongly protected.

Moreover, this protection could, on the long run contribute to the correction of the anomalies such as spam.

⁹⁸ Sheehan Kim Bartel and Mariea Grubbs Hoy (2000), op.cit, page 66

⁹⁹ Lorrie Faith Cranor, Joseph Reagle, and Mark S. Ackerman “Beyond Concern: Understanding Net Users’ Attitudes About Online Privacy AT&T Labs-Research Technical Report TR 99.4.3” available at <http://www.research.att.com/resources/trs/TRs/99/99.4/99.4.3/report.htm> (last visited, August 03 2005)

¹⁰⁰ Bartel, Hoy, op.cit, page 68

Section 3: Privacy and economic interest –anti-spam initiatives between two focal points of interest

According to article 7 of the Directive 95/46/EC, the processing of personal data is legitimate, among others¹⁰¹, when “the data subject has unambiguously given his consent” according to paragraph (a), or when the processing “is necessary for the purposes of legitimate interests pursued by the controller or by third party or parties to whom the data is disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under article 1(1)”, according to paragraph (f), (my emphasis). Referring further to article 1(1), it becomes clear that the protection of personal data is seen, according to the Directive, as one such fundamental right of the data subject. Article 7 of the Directive 95/46/EC states the general rule with regard to the legitimacy of the personal data processing. However, turning to article 13 of the 2002 Privacy Directive, we notice the requirement that the processing of individual e-mail addresses for direct marketing is only permitted once the data subject has given his prior and informed consent. Using a simple “*per a contrario*” argument, it can be inferred that the balance of interests required by article 7(f) of the Directive 95/46/EC leaned in favour of the individual privacy although, direct marketing activities, as intrinsic part of e-commerce are, or can be conducted, legitimately¹⁰². We can conclude on this point by saying that the 2002 Privacy Directive imposes a stricter regime for the data processor when the processing is done for direct marketing purposes, since the marketer cannot invoke his legitimate interests in collecting and using the e-mail addresses of the natural persons as overriding the individual’s privacy rights. Therefore, he needs prior, informed consent in any processing of e-mail addresses done for direct marketing purposes.

On the other hand, as I pointed out in Section 3 of Chapter 1, the E-Commerce Directive refers back to the Privacy Directives that are “fully applicable to information

¹⁰¹ only two paragraphs of article 7 can be regarded as relevant in the context of the present discussion, that is paragraphs (a) and (f) ; the others do not find their applicability when the issue of unsolicited commercial communications is discussed

¹⁰² The conclusion is not surprising given the provisions of Recitals 6 and 7 of the 2002 Privacy Directive, which acknowledge the possibilities opened by the electronic communication services but highlight also the need for “legal, regulatory, and technical provisions” in order to protect “fundamental rights and freedoms of natural persons and legitimate interests of legal persons”

society services”¹⁰³ , and the implementation and application of the E-Commerce Directive is to be made “in full compliance with the principles relating to the protection of personal data, in particular as regards unsolicited commercial communication”¹⁰⁴. Would this include the view on the relative importance of privacy and data protection safeguards on one hand and economic incentive on the other?

Considering article 1(3) of the E-Commerce Directive, stating that the Directive “complements Community law applicable to information society services without prejudice to the level of protection for, in particular, public health and consumer interests, as established by Community acts and national legislation implementing them *in so far as this does not restrict the freedom to provide information society services*” (my emphasis) I would argue otherwise. Following the distinction made by Moor (2004)¹⁰⁵ between privacy as an instrumental value¹⁰⁶ and privacy as an intrinsic value¹⁰⁷ I would argue that the E-commerce Directive embraced the first view of privacy, while the Privacy Directive embraced the second one.

In that regard, Recital 2 of the E-commerce Directive strongly emphasises the opportunities brought by the development of electronic commerce, in terms of employment, economic growth and investment in innovation by European companies, and enhanced competitiveness. This approach does not exclude the preoccupation for the privacy¹⁰⁸ of the prospective client. This preoccupation is to be inferred also from the references made in Recital 11 to other pieces of Community legislation ensuring a narrower and thus a more targeted protection of the contractual weaker party. However, the main aim behind the provisions of article 6 and 7 of the Directive remains arguably, the development of e-commerce. Fair information practices as the ones contained in the Privacy Directives, if integrated in the privacy policy of a business, are there to send to the prospective client the message that the firm can be trusted¹⁰⁹ with personal

¹⁰³ according to Recital 14 of the E-Commerce Directive.

¹⁰⁴ *idem*.

¹⁰⁵ James H.Moor, *op cit*, page 252.

¹⁰⁶ instrumental values are those values that are good because they lead to something else which is good (Moor (2002) page 252).

¹⁰⁷ Intrinsic values are those that are good in themselves (*idem*).

¹⁰⁸ see the definition given to consumer privacy in chapter 2 of this thesis, and also in Cathy Goodman’s article “ Privacy: Recognition of a consumer right” in *Journal of Public Policy and Marketing*

¹⁰⁹ the concept of “ trust” has been interpreted as “ the willingness of one party, here a consumer, to be vulnerable to the actions of another party, here a firm, based on the expectation that the firm will perform a

information disclosed by the customer¹¹⁰. The idea is stated expressly in Recital 7 of the E-commerce directive, as “in order to ensure legal certainty and consumer confidence, this Directive must lay down a clear and general framework to cover certain legal aspects of electronic commerce in the internal market”(my emphasis).

The provisions of article 7 of the E-commerce Directive can be seen as serving well this purpose: commercial communications should be transparent (identifiable as such, originate from sources whose identity is disclosed), and the consumer should not be “annoyed” by commercial communications when he clearly manifested his intention not to receive such material in his Inbox.

The Privacy Directives on the other hand assert the need for the individual to have a high level of protection that would equilibrate the information and bargaining power asymmetry between the business party and the individual. Reflecting the divergent approach to the relative weight of the two values, the opt-in regime introduced by the 2002 Privacy Directive¹¹¹ met strong opposition¹¹² from the direct marketers, as they feared hindrance and unjustified restrictions in their activities as a consequence of the new privacy- friendly rules. Basically, according to the opt-in rules, the individual should not only be made to feel safe in disclosing data to a marketer, he should be the initiator of these relations and be able to bring them to an end by directly communicating his will to the marketer, not just by entering his address into a opt-out register. The consumer is therefore given not only knowledge, but also a certain amount of control.¹¹³

Despite this primary difference of focus between the normative acts analysed above, it is obvious that the processing personal data is becoming more and more closely

particular action of importance to the customer, independent of the customer’s ability to monitor or to control the firm” (Mayer et al. “An integrative Model of Organizational Trust” (1995), Academy of management review 20(3), 709-734,). I subscribe to this opinion.

¹¹⁰ Mary J.Culnan & Robert J. Bies, “Managing Privacy Concerns Strategically: The Implications of Fair Information Practices for Marketing in the Twenty first Century”, article in “Visions of Privacy . Policy Choices for the Digital Age”, Collin J Bennett & Rebecca Grant (ed.), University of Toronto Press, 1999

¹¹¹ a regime that is claimed to ensure an enhanced privacy protection compared to the previous, opt-out one, consecrated by the E-Commerce Directive and the Directive 97/66/EC

¹¹² see Chapter 2 of this thesis (footnote 35)

¹¹³ According to Moor (2002), reaching full control over the information other have about ourselves is almost a utopia in a highly computerized culture like ours today. It is more realistic to adopt a “restricted access view of privacy” and claim that only “the right kind of people” should have access to the information that is relevant for their purpose at the right time. See Moor (2002), op.cit , page 257.

connected to marketing and to the allocation of resources in e-commerce activities¹¹⁴. Privacy concerns will arise however when the speed and the convenience would be accompanied by, what is commonly referred in colloquial speech, improper, surprising use of this data¹¹⁵. Hence, while it is agreed that the individual needs in practice, a mechanism to acquire knowledge and be more in control of his personal data, the conceptual foundations such a mechanism differ. Is the public control legitimate and able to safeguard the fundamental human right to privacy through uniform principles stating “fair practices”? Should the individuals be given property rights over their personal data so as to trade their data according to their wishes?

The difference in focus between the fundamental values protected by the two legislations is a useful point to bear in mind when answering the three questions about the efficiency of the anti-spam European legislation, as it is reflected all along the mechanisms provided as a solution to spam.

¹¹⁴ see Mary J.Culnan & Robert J. Bies op.cit, pp. 161 for a description of e-commerce activities involving the collection of personal data; see also Chapter 1, Section 2 of this thesis.

¹¹⁵ See Sheehan & Hoy (2000), op cit.

CHAPTER 3:

Anti- spam legislation: a balance of interests

“To date, the vast majority of the laws passed to regulate spam have been what can be called,[...] “sentiment laws.” Sentiment laws are designed to send a message about a community’s sentiment (e.g.: “we, as a community, oppose unsolicited commercial communications”) but put little effort or design into how they will actually be enforced. Sentiment laws tend to work well only in situations where there is no moral ambiguity, or the problem is in a nascent enough stage that the law can steer public opinion. Moreover, sentiment laws are inappropriate in instances where a few actors can, with relatively low cost or effort, cause widespread problems”¹¹⁶.

While the first two chapters of this thesis evidenced the spam practices in the business context in which they occur and balanced the interests and values that need to be safeguarded by the anti-spam legislation, this chapter aims at analysing the integrated legislative answer to spam conveyed by the European legislator through provisions pertaining both to e-commerce and data protection.

Section 1: The response to “unsolicited commercial communications” in the e-commerce legislation

As it aims to “ensure legal certainty and consumer confidence”¹¹⁷ in the Internal Market, and to “lay down a clear and general framework to cover certain legal aspects of electronic commerce” the E-commerce Directive provisions should be,

¹¹⁶ Matthew B. Prince, “Countering spam: how to craft an effective anti-spam law” (2004), available at http://www.itu.int/osg/spu/spam/contributions/Background%20Paper_How%20to%20craft%20and%20effective%20anti-spam%20law.pdf (last visited 22 August 2005)

¹¹⁷ Recital 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, OJ L.178 of 17 July 2000 (commonly referred to as E-commerce Directive)

inevitably, the main starting point for an e-marketer wanting to conduct legitimate business on-line and to advertise the products and services it provides.

As analysed in the previous chapters, the response rate of the potential clients to advertising techniques that interrupt constantly a person's habitual activities, conveying an indiscriminate commercial content decreases, thus forcing the marketers to switch to a more permission based marketing and to adjust the content of the commercial communications to the profile of the potential targets. This can be achieved through using the personal data available on potential clients. It is at this point that the direct marketing techniques and especially e-mail marketing on one hand and spam practices on the other differentiate one from the other, justifying the regulatory intervention, with the view of reducing the latter phenomenon.

The E-commerce Directive defines the “commercial communications” as:

*“any form of communication designed to promote, directly or indirectly, the goods, services or image of a company, organisation or person pursuing a commercial, industrial or craft activity or exercising a regulated profession”*¹¹⁸

As expected, the main trait identified here is the promotional character of the communication. Section 2 of the Directive and especially article 6 instantiate the “transparency requirement” hinted at in Recital 29 of the same Directive. *In concreto*, all commercial communications should be “*clearly identifiable as such*”¹¹⁹, specify the person (legal or natural) whose products or services are being advertised¹²⁰, and clearly state any special conditions (promotions or offers, competitions or games) that are associated with the products or services being advertised¹²¹. These are general, basic conditions to be fulfilled by any commercial communication, solicited, or unsolicited by the customer (for example when a former client asks the firm to communicate him updated information about related products or services, as well as when, during an ongoing business relation, one of the parties communicate to the other some new services that it just started to provide). Although not explicitly targeted at spam messages, the

¹¹⁸ article 2(f) of the E-commerce Directive

¹¹⁹ article 6(a)

¹²⁰ article 6(b)

¹²¹ articles 6(c) and 6(d)

provisions in article 6 tackle two of the most common features of spam: the disguised commercial character and the forged sender information. The example provided in the beginning of Chapter 1 is illustrative on these two issues¹²².

As for the practical ways to achieve transparency with regard to the commercial character of communications, the simplest solution one might think of would be to impose that any person advertising products or services mark the commercial e-mail they send with ADV. or a similarly agreed note. Although such a marking will have the advantage of allowing the filters to screen out with ease unsolicited commercial communications, it is not very likely that such an initiative will have more success than in the US where REDUCE Spam Act¹²³ failed to meet the support of the US Congress because it imposed such an obligation. As it was shown¹²⁴, this would have been a clear example of regulatory overkill, with implications reaching beyond spammers and threatening legitimate commercial activities involving among others, some unsolicited commercial communications. The commercial growth and the opportunities offered by the Internet would have been threatened while sending other types of content (political, porno graphical) through spam messages would have received an indirect approval.

What could represent then the expression “*clearly identifiable as such*” (bearing in mind that the reference is made to all types of commercial communications- solicited or not). The Directive itself provides no supplementary guidance as to the practical steps that legal or natural persons have to follow in order to ensure this condition is fulfilled. As long as the Member States or the various National Direct Marketing Associations have the freedom to implement what they think is the most suitable strategy to transpose such standards of protection in the national laws, it is not very likely that the goal of ensuring a uniform level of protection all throughout the Internal Market will be




¹²² what I find amusing about this example, is that when I saved it from my e-mail, the automatic name of the picture representing the body text of the spam message was “cowman”...so much for genuine©. Needless to say that my e-mail address is not dancogs2@yahoo.com

¹²³ standing for “*Restrict and eliminate the delivery of unsolicited commercial electronic mail or Spam Act*”


¹²⁴ Adam Mossoff “*Spam- Oy, what a nuisance!*” in Berkley Technology Law Journal, vol.19:2 spring 2004, page 638

achieved. However, the interpretation given by the International Chamber of Commerce supplements this lack of clarity in the Directive. It states¹²⁵:

*“Where electronic communications have a commercial purpose, this should be apparent through the subject matter and context. Subject headers should not be misleading and the commercial nature should not be obscured”*¹²⁶

Date:	Tue, 21 Jun 2005 00:40:49 +0300
From:	 "Karla Groves" <lbxdbsympcuekfn@yahoo.com>  Add to Address Book
To:	 dancohen228@yahoo.com
Subject:	Re [22]:

Compare the spam message above with the e-mail marketing message below, coming from Dell Norge, unsolicited, still accepted as part of an existing business relation.

To:	dancoj2000@yahoo.com
Subject:	Utrolige sommertilbud online: Fri frakt + Dell 720 printer + skjermoppgradering!
From:	"Dell Norge" <no_gem_reply@dell.com>  Add to Address Book
Date:	Thu, 21 Jul 2005 10:45:53 -0600

Establishing a clear line between the spam practices involving disguised or misleading header information and direct marketing has the benefit of pointing out the legitimate needs and the benefits of the commercial economic communications and also of allowing governments and others to focus on the real problem of harmful, fraudulent, malicious, misleading or illegal communications¹²⁷.

¹²⁵ “ICC Guidelines on Marketing and Advertising using Electronic Media” 2003, available on the International Chamber of Commerce webpage at:

http://www.iccwbo.org/home/statements_rules/rules/2004/Guidelines-on-Marketing-and-Advertising-using-Electronic-Media.asp (last visited 20 July 2005)

¹²⁶ article 4 of the ICC Guidelines

¹²⁷ “ICC policy statement on 'spam' and unsolicited commercial electronic messages” available at http://www.camara-e.net/_upload%5C373-22_114_spam1.pdf, (last visited 20 July 2005)

Once the general framework of all commercial communications has been set by article 6 of the E-commerce Directive, article 7 of the Directive lays down the specific conditions that need to be fulfilled when the communications were neither solicited nor previously consented by the receiver. In addition to restating the same transparency requirement as to the commercial character of the communication, paragraph (a) of article 7 states that it is up to the Member States to allow or not unsolicited commercial communications by electronic mail. Read in accordance with article 3(1) and 3(2) of the E-commerce Directive¹²⁸ we could admit that paragraph (a) of article 7 could have as an effect a decrease in the amount of spam originating in a Member State that prohibits the unsolicited commercial communications by electronic mail. However, since the Commission views unsolicited commercial communications and spam as being synonyms¹²⁹ and it admitted on several occasions that spam is an international issue and it can only be addressed through international measures, I foresee only a limited positive effect in allowing the Member States that space of manoeuvre.

Article 7(2) of the E-Commerce Directive requires a much wider interpretation. The article states:

“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.

A first comment needs to be made about the reference to the two directives, Directive 97/7/EC¹³⁰ and Directive 97/66/EC, especially since the first one has been amended¹³¹ and the second¹³² has been repealed.

¹²⁸ “Each Member State shall ensure that the information society services provided by a service provider established on its territory comply with the national provisions applicable in the Member State in question which fall within the coordinated field” (article 3(1) of the E-Commerce Directive)

“Member States may not, for reasons falling within the coordinated field, restrict the freedom to provide information society services from another Member State.” (article 3(2) of the E-Commerce Directive)

¹²⁹ see the discussion in the Introduction

¹³⁰ 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, available at:

http://europa.eu.int/comm/consumers/policy/developments/dist_sell/dist01_en.pdf (last visited 21 July 2005)

Of relevance here is the fact that Directive 97/7/EC (commonly referred to as the Distance Selling Directive) prohibits in article 10 only the commercial communications through facsimile and automatic calling machines where the consumer didn't express his prior consent. Other means of distance communications (such as the e-mail) can be used for commercial communications "*where there is no clear objection from the consumer*". It is my understanding that it would be no restriction on e-mail marketing to a customer, website visitor or other Internet user who had not indicated clearly an opposition to receiving such information. But the onus would be on the Internet user to invoke the safeguard, as his consent is presumed until contrary is proven. One indication of a clear objection would be the user asking to be included in an opt – out registry, either in a general one (opting-out from any kind of commercial communications) or making use of the "unsubscribe link" provided in the end of the commercial message. Not respecting the consumer decision would make the legitimate direct marketer turn, according to a recent statement of the International Chamber of Commerce¹³³, into a spammer:

"Put simply, the entities that send spam differ from legitimate marketers because spammers do not respect applicable laws and regulations and do not honor users' preferences regarding commercial communications. This is the essence of spam".

But what exactly is the scope of the service provider's obligation according to article 7(2) of the E-commerce Directive? If they undertake unsolicited commercial communications, they have to "*consult regularly and respect the opt-out registers*" in which natural persons can register themselves. What would that mean in terms of frequency? "Regularly" does not equal with "systematic". And does this imply they have to consult the registers prior to every mailing campaign? Does that entitle them to send

¹³¹ Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 *concerning unfair business-to-consumer commercial practices in the internal market* amends the Directive 97/7/EC.

However, the amendments do not affect the provisions on unsolicited commercial communications.

¹³² 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, available at: http://europa.eu.int/eur-lex/pri/en/oj/dat/1998/l_024/l_02419980130en00010008.pdf (last visited 21 July 2005)

¹³³ "ICC policy statement on 'spam' and unsolicited commercial electronic messages", 2 December 2004, page 3

unsolicited commercial e-mails to corporate e-mail addresses (office@business.ro for example) without any restrictions? And which registers must they consult in case of a .com domain e-mail address? All the available ones¹³⁴? Only some of the national opt-out registries?

Another factor contributing to the unpredictability of the provisions of article 7(2) is that Directive 97/66/EC has been repealed and replaced by the Directive on privacy and electronic communications¹³⁵, implementing the “opt-in rule” in article 13 (1) and the “soft opt-in rule” for pre-existing business relations between the unsolicited commercial communication service provider and a natural person¹³⁶. These rules are formally the direct opposite of the “opt-out rule” in article 7(2), and according to article 19 of the 2002/58/EC Directive: “References made to the repealed Directive shall be construed as being made to this Directive”. It is clear that article 7(2) of the E-commerce Directive refers now to the 2002 Privacy Directive, but how can two apparently conflicting provisions be reconciled? It appears that¹³⁷ the two legal texts refer to different situations. By referring to “opt-out registers” the E-Commerce Directive introduces the right of ANY Internet user, European or non- European alike to opt-out of commercial communications coming from ANY European service provider, regardless of any previous links which may or may not exist between them, without requiring that the collecting party or the third party advertiser be informed as to the exercise of the right of objection.

While it is true that the 2002 Privacy Directive forbids all commercial communications in the absence of a prior consent from the potential receiver, in that sense being an “opt-in” rule, the right to object to the collection of its e-mail for marketing purposes and to the transmission of commercial e-mails without consent¹³⁸, according to article 14 (b) of the 95/46/EC Directive must be exercised against (and is expected to be offered by) the party who directly collected the e-mails. The right to object to the initial collector of the personal data (the e-mail address) covers not only the acts

¹³⁴ opt –out registers are established at a national level, with some initiatives of setting some for the whole Europe or even in collaboration with the FTC in the US.

¹³⁵ DIRECTIVE 2002/58/EC

¹³⁶ A more detailed analysis of the provisions in the 2002 Privacy Directive occurs in the following section

¹³⁷ Serge Gauthronet and Etienne Drouard (2001)

¹³⁸ which, as shown in the previous chapter can be regarded as a processing of personal data in the meaning of article 2 (b) of the 95/46/EC Directive

of the collector himself (“used for direct marketing purposes”), but also the acts of a third party who, following a disclosure of personal data by the initial collector, uses it for direct marketing purposes.

In order to sum up on the issue identified in the title of this section, we need to go again through the characteristics of spam, as classified in the introductory chapter of this thesis and explained in more detail in the first section of Chapter 1, and compare them with the requirements imposed by the e-commerce related legislation on all the unsolicited commercial communications, as identified above.

1. **the means to collect the e-mail addresses:** The E-commerce Directive does not address directly the issue of the initial collection of the e-mail addresses. The only reference that we can find is included in Recital 14 of the Directive. Since the protection of individuals with regard to the processing of personal data was already addressed by the 95/46/EC Directive, and the 97/66/EC Directive (as mentioned before, this reference can now be construed as being made to the new 2002 Privacy Directive), the implementation and application of the E-commerce Directive “*should be made in full compliance with the principles relating to the protection of personal data in particular as regards unsolicited commercial communications*”. Since the opt-out rule, as opposed to the opt-in rule legitimises the first e-mail sent (as no clear opposition to its sending was yet manifested), it is not surprising that the focus from the businesses side is not the original collection of the e-mails.

From the practical perspective, the service providers need a clear answer to the question: “How can I make myself known in the first place to the potential customer, without becoming a spammer, when I’m conducting activity exclusively on line?” You may be lucky enough for someone to simply find your site and then let all his friends now about it, but this won’t get you too far. The obvious temptation¹³⁹ would be to use targeted e-mail marketing, using an already existing list of e-mails from a list broker. But for the reasons presented above, and due to the personal data protection rules (as detailed in Chapter 2), the technique is unacceptable and is a safe ride to winning a “spammer title”. One acceptable method as an initial contact to potential customers would be the

¹³⁹ Serge Gauthronet and Etienne Drouard (2001), page 61

banner advertising on websites related to the advertiser's products or services. By clicking on the banner, the interested party would thus be directed to the website in question and the advertiser could thus initiate the opt-in e-mail relationship with the visitor.

2. the transmission practices. The E-commerce Directive imposes two obligations on the information society services providers, when they undergo unsolicited commercial communications through e-mail. First of all, to make sure that they make apparent the commercial character of the message transmitted. At the same time, they have to respect the clearly manifested opposition to receive this kind of unsolicited e-mail messages. Neither the E-commerce Directive nor the Distance Selling Directive (that contains the same safeguard in article 10) do not impose on the service providers the obligation to include in the unsolicited commercial e-mails they send a link through which the receiver can object directly to the message transmitted (a functional, real unsubscribe link). As one reads the text of the E-commerce Directive, the service provider has to "consult regularly and respect" the opt-out REGISTERS in which natural persons CAN register themselves. Since the scope of the service provider's liability is limited to the consultation of the opt-out registers (if they exist, where they exist, since standards as to how accurate or comprehensive these registers should be were not created), it is the responsibility of the individual to make sure that his e-mail address is listed in this registry. Objecting to receiving commercial e-mails turns into an expensive, time consuming chore, and only the unscrupulous spammers stand to gain from the uncertainties. At the same time, no obligations to sending commercial e-mails to legal person addresses were included. Does that make spamming these addresses less detrimental to legal entities and more justifiable?

3. the content. This is, in my opinion, one of the aspects the best addressed in the e-commerce related European legislation, making the deceiving advertising contents used by spammers clearly illegal (see annex 2, example 2 for illustration purposes) . I'm not referring here to the general E-commerce Directive but to the 'Unfair Commercial Practices Directive'¹⁴⁰, as well as to the Directive 84/450/EEC (as amended by Directive

¹⁴⁰ Directive 2005/29/EC

97/55/EC)¹⁴¹ stating the conditions to be fulfilled by an advertising message. There are also more specific Directives stating the requirements for advertising products like tobacco¹⁴² or medicines¹⁴³. To go into more details about these Directives would be beyond the scope of this thesis and would not serve its aim.

4. the position of the receiver with regard to the unsolicited communication received. Spam messages are unwanted, unsolicited and unstoppable, as discussed previously. The E-commerce Directive tackles these features not by prohibiting the marketers to send unsolicited commercial messages (advertising e-mail messages that haven't been asked beforehand by the receiver) but by making sure that unsolicited e-mails are not sent to natural persons that have clearly manifested their wish not to receive such content in their Inbox. The Directive does not deal with the issue of whether or not the unsolicited mail is still of interest to the receiver (unsolicited but wanted as opposed to unsolicited and unwanted, a typical situation of spam).

I can conclude on the issue by saying that the receiver has, following the E-Commerce Directive, the possibility to do an “ex-post control”, by saying NO and stopping the flood of unsolicited commercial e-mails in his Inbox. This is, as we shall see in the following chapter, a different type of involvement then the one intrinsic to the opt-in rule, where the individual is (or it's supposed to be) the initiator of the commercial communication process, as he said YES to receiving commercial communications that can be included within his field of interest.

Section 2: The data protection legislative response to spam practices

Two types of provisions can be said to aim, among others, at reducing and even stopping the spam practices: on the one hand there are the general data protection rules, establishing the legal practices as well as the safeguards available for natural and legal

¹⁴¹ Directive 97/55/EC of the European Parliament and of the Council of 6 October 1997 amending Directive 84/450/EEC concerning misleading advertising so as to include comparative advertising (OJ L 290, 23.10.1997, p. 18)

¹⁴² Directive 98/43/EC of the European Parliament and of the Council of 6 July 1998 on the approximation of the laws, regulations and administrative provisions of the Member States relating to the advertising and sponsorship of tobacco products

¹⁴³ Directive 92/28/EEC of 31 March 1992 on the advertising of medicinal products for human use .

persons against the illegal collection, use and third party disclosure of personal data¹⁴⁴. On the other hand, article 13 of the 2002 Privacy Directive and the related Recitals establish a special regime for the personal data processing occurring in the context of unsolicited communications for direct marketing. Due to the limited scope of this thesis, I will focus on the latter provisions, whereas the general regime will serve as comparative element, when and if the special regime derogates from the general rules.

Subsection 1: Principles and rules regarding the COLLECTION of e-mail addresses

Although the term “electronic mail” has been given a broad and technologically neuter interpretation, both in the 2002 Privacy Directive itself¹⁴⁵ and in the Data Protection Working Party Opinion¹⁴⁶, due to the scope of this thesis I will only consider some issues raised by the classic e-mail (SMTP¹⁴⁷ based) spam.

The current regime¹⁴⁸ of personal data protection, when the purpose of the data collection is direct marketing, distinguishes between the protection awarded to natural persons (article 13 (1) and (3)) and the one awarded to legal persons (article 13 (4)). The difference in regime is quite significant, so I will structure my discourse based on this distinction:

1.1. COLLECTION OF E-MAIL ADDRESSES BELONGING TO NATURAL PERSONS:

The rule in article 13 (1) provides among others, that the e-mail addresses belonging to natural persons can only be collected for marketing purposes if the subscribers have given their prior consent. At the same time, according to article 13(2), during existing customer relations, a business can use the e-mail addresses collected from its clients in order to market its own products (with the limitations that will be discussed below)

¹⁴⁴ See Directives 95/46/EC and 2002/58/EC.

¹⁴⁵ article 2 (h) read in accordance with Recitals 4 and 40 of the 2002/58/EC Directive.

¹⁴⁶ Opinion 5/2004 on unsolicited communications for marketing purposes under article 13 of Directive 2002/58/EC, 11601/EN WP90 specifies at point 3.1 that “any message by electronic communications where the simultaneous participation of the sender and the recipient is not required” can be included in the concept of electronic mail.

¹⁴⁷ Simple Mail Transport Protocol.

¹⁴⁸ introduced through the 2002 Privacy Directive.

1.1.1 **opt-in rule** Despite the fact that the rule allowing the processing¹⁴⁹ of personal data only when the data subject has “unambiguously given his consent”¹⁵⁰ has governed the practice of data processors in Europe since the implementation of the 95/46/EC Directive, its express adoption for this particular type of data processing met the sustained opposition from the direct marketing associations¹⁵¹. Article 13(1) of the 2002/58/EC Directive read in accordance with article 2(f) of the same Directive extends the existing meaning of consent¹⁵² to the processing done in the context of direct marketing. That means that any commercial communication done in the absence of the prior, freely given, specific and informed consent of the e-mail address owner is deemed to be unsolicited and thus prohibited. From the point of view of the attempts to stop spam (and assuming for the moment that spammers really do care about the legal provisions) this provision arguably¹⁵³ goes directly to the “root of all evil”: the illegitimate collection of e-mail addresses, and their subsequent use for unsolicited bulk, commercial emails. It prohibits the first e-mail sent without the proper consent¹⁵⁴ and it moves the burden of proof on the business party, which has to show that it has requested and received the

¹⁴⁹ according to article 2 (b) of the Directive 95/46/EC, processing of personal data includes, among other, acts of collection, use, disclosure by transmission

¹⁵⁰ according to article 7 (a) of the Directive 95/46/EC, considering that none of the other criteria in article 7 could apply to the processing of e-mail addresses in the context of spam

¹⁵¹ see **FEDMA** comments regarding the Working Document on the processing of personal data and the protection of privacy in the electronic communication sector, 18 may 2000, claiming that article 13 and the opt-in rule represents a “radical and non-justified solution”; document available at: <http://europa.eu.int/ISPO/infosoc/telecompolicy/review99/nrfwd/FEDMA22e.htm> (last visited 2005-08-01)

Also the comments of the **DMA** in UK, claiming article 13 of the 2002 Privacy Directive “would create an insuperable barrier to the effective development of electronic commerce thereby preventing the creation of a true single market which would allow EU citizens wide access to the fullest range of goods and services” see “The Direct Marketing Association (UK)’s comments on the Working Document on the processing of personal data and the protection of privacy in the electronic communication sector”, available at: <http://europa.eu.int/ISPO/infosoc/telecompolicy/review99/nrfwd/DMA22e.htm> (last visited 2005-08-01)

¹⁵² art 2(h) of Directive 95/46/EC defines consent as “any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed”

¹⁵³ it has been claimed that spammers do not care about the legal provisions, whatever they are, and that the studies indicate that the majority of spam comes from outside Europe and will not be subjected to the opt-in rule anyway. See for reference the FEDMA document quoted above.

¹⁵⁴ see however the Belgian law implementing the Directive, available at http://www.juridat.be/cgi_loi/loi_a.pl?language=fr&caller=list&cn=2003031132&la=f&fromtab=loi&sql=dt='loi'&tri=dd+as+rank&rech=1&numero=1, whose article 14(1) was interpreted as permitting the business party to send a first e-mail in which they ask for the e-mail owner’s consent to the sending of commercial communications at that address. The requirements that this first prospective e-mail should fulfil can be found at : “FPS Economy, SMEs, Self-Employed and Energy – Belgium « Spamming » 24 questions & answers” – January 2005, page 10.

private individual's consent. This opposed to the previous opt-out regime, which, as shown in Chapter one, left the end-user with the responsibility to make the communications stop.

The rule seems, in theory, to be pretty clear. However, the law has to be tailored on social realities and in practice it is more difficult to keep the balance between the legitimate interests of direct marketers (affected as well by the opt-in regime¹⁵⁵) and the privacy concerns of the individuals. Most discussions revolve around the quality of the consent that would provide adequate level of control to the individuals over the use of personal information, while allowing marketers to get as many "opt-ins" as needed for efficient business operations. First of all, the Data Protection Working Party explicitly stated that the "e-mail addresses picked up in public areas of the Internet¹⁵⁶ such as news groups without the informed knowledge of the individual are not lawfully collected. They can thus not be used for any purpose than the one for which they have been made public, in particular not for direct marketing"¹⁵⁷. Similarly, the implied consent, the use of pre-checked boxes, and broad general requests for consent would not meet the requirements of the Directive with respect to transparency and fairness¹⁵⁸. However, as stated by Recital 17 of the 2002 Privacy Directive, ticking a box when visiting an Internet website is an appropriate method of expressing consent.

In my view, the most important requirement for obtaining the user's consent is that it has to be an INFORMED indication of the user's wishes. Although I fully realize that a marketer cannot be expected to negotiate individually every user's declaration of will, I believe that the exact wording of the text accompanying the box to be ticked makes the difference between an informed consent as opposed to a speculative, "semi-informed" one¹⁵⁹. The consequence of this distinction is, for the purposes of the current

¹⁵⁵ the direct marketers face one additional limit to the legal ways in which they can approach prospective clients for the first time

¹⁵⁶ which, as I have pointed out in the first chapter, are the main target of the spammers when looking for e-mail addresses

¹⁵⁷ Recommendation 2/2001 on certain minimum requirements for collecting personal data on-line in the European Union, 5020/01/EN/ Final, WP 43

¹⁵⁸ DPWP (2000), 5063/00/EN/FINAL Chapter 4, §V; Chapter 8, §4.

¹⁵⁹ An extremely interesting experiment was conducted on the issue by George R. Milne in 1997. Among the conclusions of this study (see the article for concrete examples of opt-in statements) was that the "format of the question asking customers to join a mailing list can affect their willingness to transfer personal information. The direct yes or no format question that asked consumers to join a mailing list

discussion, that even if a certain procedure of information has been followed by the marketer, the individual might experience the same lost of control over the personal information as in the context of spam.

1.1.2 **Soft opt -in** rule, introduced by article 13(2) of the 2002 Privacy Directive is, regards more the “use of e-mail addresses ” than the “ e-mail addresses collection”. Moreover, it applies both to natural and legal person’s e-mail addresses, so I will discuss it in more detail in Subsection 2. What is worth saying at this point, is that the soft opt- in rule was interpreted as allowing the marketers to use further customer lists that were compiled before 31 October 2003¹⁶⁰, in accordance with the previous opt-out regime¹⁶¹, as long as they have been used recently and the subscribers are given, with every new message sent, the opportunity to object to further use of their addresses¹⁶².

1.2. COLLECTION OF E-MAIL ADDRESSES BELONGING TO LEGAL PERSONS:

According to article 13(5) of the 2002 Privacy Directive, the Member States are supposed to make sure that the legitimate interests of the subscribers¹⁶³ other than natural persons are “sufficiently protected”¹⁶⁴ with regard to unsolicited commercial communications. In other words, the Member States can chose to impose on the marketers collecting and using e-mail addresses belonging to legal persons either the opt-in or the opt-out regime, or any other level of protection they might consider fit “in the framework of Community law and applicable national legislation”. The solution was a compromise one, meant to alleviate the concern of marketers that the data protection laws might restrict the content of communications exchanged within business- to- business relations thus exceeding its ambit. Since the basic difference between legitimate e-mail marketers and spammers is that the first ones are compliant with the existing legislation

caused the consumers to be more protective with their names. Yes/no caused consumers to process the information more carefully on the 1st question and this heightened the level of cognitive activity thus forcing a more intense scrutiny on the transfer question”.

¹⁶⁰ the deadline for the transposition of the 2002 Privacy Directive in national laws, according to article 17 of the Directive

¹⁶¹ used in accordance with Directive 97/66/EC, repealed according to article 19 of the 2002 Privacy Directive

¹⁶² see http://www.dti.gov.uk/industry_files/pdf/ico_guidance_dpec_part2.pdf

¹⁶³ see Recital 12 of the 2002 Privacy Directive for a clarification of the term “subscriber”

¹⁶⁴ The issue of what are those interests and why do they justify a different standard of protection than the natural persons, as well as the issue of how “sufficiently protected” are the natural persons following the provisions in article 13 (4) will be addressed in Section 3

and pay special attention to consumers' wishes, expressing in very clear terms the permitted behaviour was essential for the e-mail marketer's activity. On the other hand, from the perspective of the common fight against spam, the effect of this freedom of decision awarded to the states can only be detrimental.

Four examples will serve my purpose of illustrating how different the national implementation of the Directive can be:

Due to the provisions of article 19 (3) of the Basic Law (Grundgesetz) ¹⁶⁵, in Germany the same level of protection was awarded to both natural and corporate e-mail addresses.

In Great Britain¹⁶⁶, the term "individual subscriber" was interpreted broadly so as to include not only natural persons, but also "unincorporated partnerships and sole traders", in the first case because the unincorporated partnership is not a legal person, in the second case since the legal and the natural person coincide. In other words, it is forbidden to send commercial e-mails in the absence of informed and specific prior consent not only to e-mail addresses belonging to natural persons, but also to business e-mail addresses in the two mentioned situations.

In Belgium¹⁶⁷, it is possible to send unsolicited commercial communications to addresses like info@company.be or customer.services@company.be or contact@...office@..., as long as, according to the circumstances, it is obvious that they belong to a legal person.¹⁶⁸ Contrarily, once a company creates to its employee business addresses like name.surname@company.be, the address is to be considered as belonging to a natural person, despite its use for business related communications. It is the marketer's responsibility to appreciate in each case, before sending the commercial e-mails, what kind of address (belonging to a natural or a legal person) is the one targeted, and the evidentiary burden (with regard to applicability of this exception) rests on him. One

¹⁶⁵ <http://www.datenschutz-berlin.de/recht/de/bdsg/summary-gutachten.pdf>, page 2, (last visited, August 1, 2005)

¹⁶⁶ see further,

<http://ico-cms.amaze.co.uk/DocumentUploads/New%20rules%20on%20email%20marketing.pdf> (last visited, August 1, 2005)

¹⁶⁷ According to the "Arrêté royal visant à réglementer l'envoi de publicités par courrier électronique", 4.04.2003, published in the MONITEUR BELGE- BELGISCH STAATSBLAD on 28.05.2003, page 29292" <http://www.iab-belgium.be/Media/pdf/kb040403.pdf> (last visited, August 1, 2005)

¹⁶⁸ "Des publicités non sollicitées par courrier électronique peuvent être envoyées à ces adresses, dans la mesure où, en raison des circonstances, il est manifeste que ces adresses concernent des personnes morales"

additional and essential condition is that a marketer is not allowed to send unsolicited commercial communications to legal persons in order to advertise products and services addressed actually to natural persons¹⁶⁹.

The fourth and the last example is the French approach. In its initial interpretation, the law of 21 June 2004¹⁷⁰ stated that the prior consent rule applied to addresses such as name.surname@company.fr (nominative professional e-mail addresses) but did not apply to addresses from which the identity of the person could not be inferred, such as office@company.fr.

Following negotiations between the CNIL and the representatives of the direct marketers in France, in a decision in 17th of February 2005, CNIL reconsidered its position on the issue¹⁷¹, ruling that natural persons can receive commercial e-mails without their prior consent on their nominative professional e-mail addresses if these unsolicited e-mails are related to the function they fulfil within the company¹⁷². In other words, the director of informatics systems within a company can receive “special offers” for hardware on its nominative business e-mail address, but not offers for summer vacations on some exotic islands.

As it is obvious from the examples presented above, the different national transpositions of the Directive leads to a fragmented and inefficient approach to spam and creates additional difficulties for the direct marketers that have to figure out what is the permitted behaviour in every jurisdiction. Neither the Directive itself, nor the 2004 Opinion of the Data Protection Working Party specify the level of diligence that can be expected from the marketers in getting to know the applicable regime and the type of address that he is prospecting.

¹⁶⁹ “En outre, les produits ou services offerts à travers les publicités ainsi envoyées doivent viser des personnes morales, et non des personnes physiques. En effet, un annonceur ne saurait se prévaloir de l’exception pour envoyer à des adresses de personnes morales des publicités visant en réalité des personnes physiques, contournant ainsi l’obligation de solliciter le consentement préalable de ces dernières”

¹⁷⁰ Loi pour la confiance dans l’économie numérique ([article L 34-5](#) du code des postes et télécommunications, available at: <http://www.legifrance.gouv.fr/WAspad/UnArticleDeCode?commun=CPOSTE&art=L34-5> (last visited, August 1, 2005).

¹⁷¹ the decision is available on [http://www.cnil.fr/index.php?id=1780&print=&news\[uid\]=238&cHash=afcf8a5adf](http://www.cnil.fr/index.php?id=1780&print=&news[uid]=238&cHash=afcf8a5adf) (last visited, August 1, 2005).

¹⁷² les personnes physiques puissent être prospectées sans leur accord préalable à leur adresse électronique professionnelle, «au titre de la fonction dans l'organisme (...) que leur a attribué cette adresse.

In any event, both legal and natural persons must be offered the general possibility to object easily and free of charge to having their address collected for direct marketing communications, both at the time of collection, and subsequently, on the occasion of each message sent in case the customer had not refused initially such use. Moreover, similarly to the obligation imposed on the service providers in the E-Commerce Directive, it is prohibited to send commercial e-mails “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” (art 13 (4) of the 2002 Privacy Directive. The very common spam practice is obviously targeted here.

Subsection 2: Principles and rules regarding the USE of personal data FOR DIRECT MARKETING PURPOSES;

The obligations of the direct marketers with regard to the use of individual e-mail addresses for commercial communications depend on the manner in which the addresses were initially collected and whether or not a business relationship was previously established between them. Some of the applicable rules were already mentioned, so they don't require further analysis. These rules regard the prohibition to use e-mail addresses that were illegally collected and the obligation to give the opportunity to object to any further use of the e-mail address for commercial communications with every such communication sent, even though the initial collection was agreed to.

Two issues will be discussed in this section:

2.1 The use of e-mail addresses for direct marketing purposes within an existing customer relationship (sending unsolicited commercial e-mails to current or former clients)

Once the client's contact details have been obtained by the marketer “in the context of a sale”, the same marketer can use the personal data in order to “market its own similar products and services”. Of course the general requirement regarding the right to object applies here too. Although the provisions of article 13 (2) of the 2002 Privacy

Directive have been interpreted by the Data Protection Working Party¹⁷³, the comments leave as well much room for interpretation by the Member States.

The wording “in the context of a sale” was interpreted sometimes as not being limited to completed sales, but also to its preceding stages, for example when a customer shows interest in the products and services of a company, and does not object to receiving further communications relating to the same or similar items, but without buying any.¹⁷⁴ In other interpretations, at least one contractual direct link between the marketer and the e-mail address owner it is necessary to have been established¹⁷⁵. However, the Working Party raises the question on the period of time during which the consent is to be reasonably considered to be valid. In my opinion, if we call the applicability of the general principles applicable, and give within every communication the option to opt-out from receiving further commercial messages from the same source, we do not need to decide on a time frame in which the consent is validly given, as it is reinforced after every communication. A more interesting question relating to the temporal validity of the consent is raised when a relatively large time interval has passed between the moment of collection and the moment when the first unsolicited communication is sent. This question, however is strictly linked to the nature of the offer, and cannot be answered *a priori*.

Therefore, the client relations with the mother company would not entitle a daughter company to send unsolicited commercial e-mails to the client, even for similar products and services. In this case, the daughter company, as well as any partner or company belonging to the same group of companies, are considered separate legal entities, and they are not therefore covered by the term “its own similar products and services”.

Thirdly, the concept of “similar products and services” received different, even contradictory interpretations. According to the Data Protection Working Party, the similarity will have to be interpreted according to the objective perspective (that is

¹⁷³ See DPWP, Opinion 5/2004, op.cit.

¹⁷⁴ see http://www.dti.gov.uk/industry_files/pdf/ico_guidance_dpec_part2.pdf, pp. 24.

¹⁷⁵ “In practice a provider may legally sent his catalogue of products and services by electronic mail to all clients having subscribed at least once to one of these products or services (asking for specifications is not sufficient to fulfill the condition), and having communicated their particulars on that occasion” see the Belgian interpretation, in FPS Economy, SMEs, Self-Employed and Energy – Belgium « Spamming » 24 questions & answers” – January 2005 and footnote 152.

according to the reasonable expectations) of the recipient, and not from the perspective of the sender¹⁷⁶. For example, if I buy Milan Kundera's book "The Joke" from an on-line bookshop, and do not object to receiving further offers from the same shop, can the marketer be entitled to assume that I reasonably expect to receive special offers on all the books available, all Kundera's books, all the fiction books about communism?

According to the interpretation given to the Directive in the Belgian Law, similar products and services are considered the ones belonging to the same category of products and services¹⁷⁷, that is, according to the current stage of the technological development (so we see here a completely different criteria than the one presented by the Data Protection Working Party), the CDs, the DVDs, the video cassettes and even the books belong to the same group of products and services, so they are similar. Again, the wording chosen by the marketer when asking for the consent of the customer is extremely relevant as a factor against which the reasonable expectations of the person could be examined.

The discussion about similarity, especially since the proposed European criteria refers to the reasonable expectations of the recipient could be very extensive. But since I'm focusing on the legislative response to the spam with the view of protecting the privacy interests of the natural persons that become victim of spam attacks and suffer its negative consequences, it is not relevant to go into more details on the point. A marketing study made in 2000 by Susan Chang, Mariko Morimoto¹⁷⁸ pointed out, referring also to previous studies that the customers did not consider unsolicited messages coming from companies with whom they have done business in the past to be SPAM¹⁷⁹.

The fact that they had built already a relation with a company in the past made the individuals feel less annoyed when they received other offers from the same company. Although rules had to be set in order to prevent the marketers abuse an existing customer relation, I believe that as long as the marketers keep their commercial

¹⁷⁶ see the DPWP Opinion nr 5/2004, page 9

¹⁷⁷ "Sont considérés comme produits ou services analogues ceux qui appartiennent à une même catégorie de produits ou de services", see "Arrêté royal visant à réglementer l'envoi de publicités par courrier électronique" (2003)

¹⁷⁸ Chang, Morimoto (2003), op.cit.

¹⁷⁹ idem, pp. 9

communications at a reasonable level, they will not be accused by their existing clients of spam.

2.2 The use of e-mail addresses that were not collected directly from their authorised user. This issue is not directly addressed by article 13 of the 2002 Privacy Directive. However, the rules applicable according to the data protection legislation have an obvious applicability, since the spammers collect e-mail addresses into lists and sell them to third parties, or use themselves existing lists which they bought from other list brokers.

The rules that govern the transfer of personal data (and in our case, the transfer of a natural or legal person's e-mail addresses) will be dealt with in the next subsection. The issue in discussion here is whether or not the marketers buying or renting the e-mail lists from a third party to whom they were consensually given have any duties to check if the consent was legally obtained for all the e-mails in the lists or to inform the persons about the purpose for which they intend to use their e-mail addresses (and, if applicable, ask again for prior consent). Although it is probably recommended to have such a preventive behaviour, are the marketers, as data controllers compelled to do so?

As stated, the 2002 Privacy Directive deals only with the obligations of the party collecting e-mail addresses with the intent to share/ sell/ rent the lists to a third party. Once the e-mail owner has given his informed prior consent to the collection for this purpose, the third party to whom they are entrusted can use them for the same purpose (direct marketing). The idea is present also in Recital 39 of the 2002 Privacy Directive and is in accordance with the purpose specification principle. But article 11 of the 95/46/EC Directive would be applicable also, first because the data has not been obtained by the current controller directly from the data subject (but indirectly from the party to whom they have been entrusted), and secondly because the application of the general data protection principles is in accordance with article 1(2) of the 2002 Privacy Directive. Therefore, "at the time of undertaking the recording of personal data", or at the time of the first disclosure, the data subject should be informed about the identity of the controller, the purposes of the processing, and about any other issues that, according to the principles of fair processing, are considered as necessary. In my opinion, according

to the obligations stated already in article 13 of the 2002 Privacy Directive, all these information become available to the e-mail address owner at the time the first unsolicited commercial e-mail is send by the new data controller. However, if the list of addresses was compiled during the previous opt-out regime, the new controller might find himself accused of spam, with all the associated negative consequences for his business.

Subsection 3: Principles and rules regarding the TRANSFER of personal data to third parties

The marketing research literature has explored extensively the impact of the individual's privacy concerns on their on-line behaviour and on the trust they are willing to award to the marketers with which they interact. According to Kim Bartel Sheehan and Mariea Grubbs Hoy¹⁸⁰, prior studies seem to indicate that "two expressions of control, awareness of information collection and usage beyond original transactions are the predominant influences on the degree to which consumers experience privacy concern." The consumer's concerns are justified, considering they only become aware of the secondary use of the personal information ex-post, when they receive unsolicited and unwanted communications from parties to whom their data has been transferred.

The data protection core principles, especially the principles of disclosure limitation and purpose specification¹⁸¹, minimality¹⁸² as well as data subject participation and control¹⁸³ oppose, among others, to the disclosure of personal data to a third party without the data subject's prior consent. The definition of consent, in itself contains the requirement that a separate and specific manifestation of will has to be obtained from the data subject in case the marketer wishes to disclose customer data to other third parties.

This requirement is founded on the desire to empower the individual with the ability to control the identity of the entity managing his personal data (in this case, its e-mail address) and the purposes of the processing done upon them. From the individual's perspective however, the theoretical ability to exercise control is limited due to asymmetrical information:

¹⁸⁰ Sheehan & Hoy (2000), op.cit., pp. 63.

¹⁸¹ article 6(b) of the 95/46/EC Directive.

¹⁸² article 6(c) of the 95/46/EC Directive.

¹⁸³ article 12 (a), first stance, in the 95/46/EC Directive

*“Asymmetrical information refers to the imperfect knowledge or information that consumers may have about a product, the company that made the product, alternative products, and so on when they enter the marketplace (...) Applied to our privacy context, individuals would need to have fairly detailed information about the behavior of businesses and the value of their personal information to their operations to determine how their information will be handled and what commercial value it may possess”*¹⁸⁴

Moreover, according to a marketing study¹⁸⁵, consumers will be less willing to provide permission to transfer their name when the financial gain to the marketer is explicit and the third party selectivity is absent. Question format and disclosure statements affected significantly the response levels:

*“In particular, both revealing the actual practice of renting names, and not informing customers of the type of third party that might receive transferred names lowered the customer’s willingness to transfer personal information. These results might help explain the accepted practice of direct marketers that use euphemistic expressions and try to assure customers that their names are sold only to responsible parties that have goods and services of interest to the consumer”*¹⁸⁶

Take for example the following statement: “Occasionally we make a portion of our mailing lists available to a few, reputable, carefully screened companies whose products you might find of interest.” Or, a similar statement: “We occasionally exchange our customer lists with other reputable companies whose products and services we believe might be of interest to our clients”. In both cases, the client is given the option to tick a box in which he consents to the actions specified in the statements. The marketer’s intention is obvious and prior consent has been obtained. According to the study above, there are high chances these statements will produce a high positive response rate.

¹⁸⁴ Ann Cavoukian (1999), op.cit. page 15

¹⁸⁵ see George R.Milne (1997), op.cit. page 301

¹⁸⁶ idem, page 304

But can we truly say the consumer is giving a fully informed and specific consent?

Section 3: The efficiency of the anti-spam solution provided by the European legislator

The investigation will, inevitably be centred on the spam issues identified in the previous two sections. For the purposes of the analysis I adopted a broad interpretation of the term “efficiency”, including not only an evaluation of the costs of enforcing the system vs. the practical results achieved, but also a balance of the practical results vs. the basic aims of the legal framework; the latter evaluation might be otherwise included under the term “effectiveness”. Therefore, we also need to look into the equilibrium that can be inferred from the legal text, in as much as some of the interests of the different actors (direct marketers, end-users) modelling their behaviour in accordance with the chosen normative texts¹⁸⁷, might conflict.

In essence, I will try to provide a possible answer to three questions:

1. Do the different mechanisms provided by the E-commerce Directive, on the one hand, and Privacy and Data Protection European Directives on the other converge towards a unitary solution or do they clash?
2. Is this solution (Or are the two mechanisms) fit for the purpose it (they) aim(s) at?
3. Are there negative consequences arising from this regulatory approach and if the answer is affirmative, do they exceed the positive consequences?

Subsection 1 Different mechanisms –one solution?

Comparing the provisions of the E-commerce Directive (articles 6 and 7) with the provisions of the 2002 Privacy Directive (mainly article 13), the first point that becomes obvious is that they employ different mechanisms in the fight against spam, and therefore establish different duties for the marketers that wish to interact with potential customers through e-mail commercial messages and to send unsolicited messages. While

¹⁸⁷ that is, the provisions referring to unsolicited commercial communications in the E-commerce and Privacy and Data Protection European Directives

the first one leaves it up to the Member States to permit or to forbid unsolicited commercial communications through e-mail and imposes on the marketers a mandatory consultation of the opt-out registers in which natural person might register themselves, the 2002 Privacy Directive divides the obligations of the marketers depending on the legal personality of the receiver (natural or legal person): an opt-in mechanism for natural persons, and a different regime, as chosen by the Member States, for legal persons. As hybrid between the opt-in and the opt-out regime, the rule commonly referred to as soft opt-in, distinguishes further between the type of relations that exist between the marketer and the prospected customer.

Therefore, the dilemma of a marketer conducting businesses on line and wishing to start a targeted advertising campaign through e-mail, consists first of all in determining which of the two directives to follow so as not to suffer the consequences arisen from being labelled a spammer. Both Directives are still in force, so their provisions are applicable, and other than the temporal primacy of the Privacy Directive (more recent compared to the E-commerce one), no subordination of one towards the other can be expressly established from reading their provisions. Following the E-Commerce Directive, a marketer will be bound to the jurisdiction that applies to him¹⁸⁸, with the associated controversies regarding the meaning of the phrase “established on its territory” and the associated risks of forum shopping.

Secondly, a marketer should “regularly” check for the opt-out registers in which the natural persons can register their wish not to receive more advertisements via e-mail. Several points are questionable here. The main one relates to how thorough is this control expected to be? The legislator chose regularity as a criteria, but as showed in Chapter 1 of this thesis, a check-up scheduled every six months according to self determined rules of practice and followed by the marketer is just as “regular” as a check-up done before every marketing campaign, although they are the expression of different levels of diligence from the marketer. Since the expected outcome of this safeguard is to make sure the wishes of the customer are respected, what is truly relevant here is neither the time frequency not the pattern-like occurrence, but the “*bona fides*” behaviour of the marketer in making sure that his commercial message does not conflict with an express

¹⁸⁸ according to article 3(1) of the E-Commerce Directive

wish of the customer. An additional point connected to the level of diligence expected from a marketer (and intrinsically reflecting the etiquette-related dividing line between spammers and marketers) questions the timeliness of an opt-out manifestation of will. Does a refusal to receive commercial communications registered six months before still reflects the wishes of the client at the moment? If the economic behaviour of a legal person is arguably more rational and thus more predictable, individuals are driven by a multitude of objective and subjective factors that are close to impossible to predict in an on-line internationally open market, even through assessing past behaviours and through profiling. Of course, the practicalities of choosing the appropriate register to check should not be ignored.

Reflecting the above analyzed preoccupation for gaining and enforcing consumer confidence in e-mail marketing, the E-commerce Directive imposes transparency obligations on the marketer, regarding both the commercial character of the e-mails and the identity of the business sending them, as well as obligations on the Member States regarding the empowerment of the customer through the recognition of his free will and the actual opportunity to request the termination of commercial communications by subscribing to an opt-out list. Bear in mind however that these registers ought to be set only for natural persons that object to receiving such contents in their inbox. Although by looking at the definitions provided by articles 2(b) and 2(d) I can argue that the Directive deals also with business –to – business relations¹⁸⁹, it can be inferred from the rules in article 6 and 7 (or better yet, from the absence of any of such rules), that there are few restrictions to sending unsolicited commercial communications to e-mail addresses belonging to legal persons.

Having presented the E-commerce Directive mechanism addressing the unsolicited communications¹⁹⁰, I will direct my attention to the relevant provisions of the 2002 Privacy Directive.

¹⁸⁹ the Directive defines in article 2(b) the term "service provider" as any natural or legal person providing an information society service and in article 2(d) the term "recipient of the service": any natural or legal person who, for professional ends or otherwise, uses an information society service, in particular for the purposes of seeking information or making it accessible".

¹⁹⁰ and reference should be made to Section 1 for the more detailed analysis of its provisions.

The new¹⁹¹ rules¹⁹² regarding unsolicited commercial e-mails make a basic distinction between the commercial e-mails sent to natural persons and the commercial e-mails sent to legal persons.

The first rule requires that the prior and informed consent of the natural person targeted (article 13.1) before the sending of the first message and a separate consent needs to be obtained for any secondary uses of the e-mail address obtained¹⁹³. The natural person should also be given the possibility to stop at any point in time, free of charge and in an easy manner, further commercial communications.

The second rule concerns “subscribers other than the natural persons” (article 13.4) whose “legitimate interests” have to be sufficiently protected in this respect (unsolicited commercial communications). The provision is rather broad and unclear, since no further guidance is provided on relevant issues such as: what legitimate interests are being referred to in the context, what are the criteria that serve in the assessment of the “sufficiency” of protection, whether or not unincorporated companies, or structures without legal personality (such as daughter companies or virtual organizations), as well as sole traders should be included under the umbrella of “subscribers other than the natural persons” *Ad litteram* they should, as these entities are not and do not accomplish the functions on a natural person, but as showed previously¹⁹⁴ the Member States have found different solutions to steer clear of the ambiguities in the European text.

The third rule in the 2002 Privacy Directive (article 13.2) deals with existing business relations, involving both natural and legal person subscribers. Basically, marketers that obtained the e-mail addresses from their customers can continue to use them for sending commercial e-mails advertising their own similar products and services. Similar safeguards regarding the possibility for the customer to object to the communication should also be provided.

This short description of the two mechanisms introduced by the European legislator as a legal tool to shield the Member States in the fight against spam already

¹⁹¹ the former Privacy in Telecommunications Directive (97/66/EC) had in art. 12 opt-out rules for unsolicited commercial e-mails, similar to the ones in the E-Commerce Directive

¹⁹² refer to Section 3 of Chapter 2 in this thesis for a detailed description of the provisions in article 13 of the 2002 Privacy Directive and the definition of the key terms used therein.

¹⁹³ such as selling or renting the e-mail address to a third party.

¹⁹⁴ See Chapter 2, Section 3 Subsection 1.2 of this thesis.

highlighted some of the discrepancies. My goal is to explore the possibility for them to aggregate into a unitary solution, if this possibility exists, or to underline the contradictions that prevent them to become such unity.

The two mechanisms have certain features in common:

First of all, they both use the term “unsolicited communications”, and expressly (E-commerce Directive) or implicitly (2002 Privacy Directive) refer in terms of the content only to the commercial communications. As such, they regulate a larger sphere of behaviours that if they would have to address only spam and not legitimate e-mail marketing as well. At the same time, only part of the content commonly associated with spam is covered, since as I mentioned in the introductory chapter, spam e-mail messages are only in part commercial in nature, but can include political, religious, humanitarian and illegal material (viruses, child pornography).

Secondly, they both outlaw the sending of commercial e-mail messages when the identity of the sender or of the person on whose behalf the sending is done is hidden or disguised (article 6 (b) of the E-Commerce Directive and article 13(4) of the 2002 Privacy Directive). Both the interest in gaining client confidence and the privacy interest on having insight on the identity of the data processor justify and are well served by this requirement.

Thirdly, they both reveal the need to look after the manifested wishes of the potential receiver, although the manner of expression and the role of such manifestation differs.

Somehow surprisingly, this is about all the two legal texts have in common. The rest of the provisions, when they are faced one against the other, reveal either cross references or contradictions.

The first cross reference is again related to the terminology used in the two directives. The E-commerce Directive contains in article 2(f) the definition of “commercial communications” and it seems that although the 2002 Privacy Directive does not expressly refer to the E-commerce Directive, it uses the term alike. The same can be said about the term “direct marketing” used by the Privacy Directive in both the text of article 13 and in the related Recitals (41, 42, 43, 45). Although the Recitals mention some of the features of the direct marketing, such as the low costs involved in

sending them (40), some media through which the direct marketing message can be conveyed, no definition is provided.

The second cross reference concerns the level of protection awarded to legal persons. A partial reference is made in Recital 45 of the 2002 Privacy Directive, to those States that would chose to set up an opt-out register for **legal persons**, that they should apply the provisions in article 7 of the E-Commerce Directive. Again, the terminological reference is misleading, since the scope of the terms “legal person” (Recital 45) and “recipients other than natural persons”(article 13(4)) is different.

The broadest cross reference between the two texts is to be found in article 7 of the E-Commerce Directive, stating that the provisions found in the E-Commerce Directive are “without prejudice to Directive 97/7/EC and Directive 97/66/EC”. This is an indirect reference to the 2002 Privacy Directive, as it mentions the former Privacy Directive that was repealed by the 2002 one. In this context, given the fact that the 2002 Privacy Directive changed in the most part the content of the provisions referring to unsolicited commercial communications, it is questionable if the reference can still be considered valid. Taking into account the opposition to the current Privacy Directive in the business circles, as well as the incompatibility that would result from the application of both provisions, it is my opinion that the reference can no longer be seen as justified.

The E-Commerce Directive does not address however the issue of the initial collection of the e-mail addresses by the marketers and does not distinguish further regarding the different types of business relations that the marketer and the targeted e-mail address owner might be in. Although the references to “other requirements established by Community law”¹⁹⁵ (additional to the E-commerce Directive provisions) cannot be ignored, still it is my opinion that some rules regarding the initial collection of the e-mail addresses should have been also included in a directive aiming to set up the general framework in which e-commerce activities are supposed to take place. These rules could have referred not to the issues pertaining more to personal data protection, but at least to the sources from where the collection of the e-mail addresses can occur. All the more reason to instantiate the rules for unsolicited commercial communications to the possible pre-existing relations between the service provider and the receiver: is the

¹⁹⁵ Article 7(1), E-commerce Directive

receiver a customer already? Is it a visitor to the website, who provided the e-mail address just in order to take part in a competition? Is he simply an Internet user with whom the marketer had no previous contact? Of course, all of them are granted the general right to opt-out to receiving commercial communications, however such an instantiation would still provide useful guidance to the marketers as to how to behave in order not to be associated with a spammer

From the point of view of the content, the E-Commerce Directive does not include even a general obligation for the marketers to personalise the content of the commercial e-mails sent according to the receiver's profile, although such a distinction is claimed¹⁹⁶ to exist between the legitimate direct marketing and spam.

These minuses are partially covered by the 2002 Privacy Directive, at least at the level of express provisions, still the role they accomplish and the values they serve are different from the ones likely to be found in an E-commerce Directive (I consider here the different interests and values safeguarded by the two texts, as presented above).

The 2002 Privacy Directive introduces the notion of "informed, prior consent" of the receiver as the only factor legitimizing the sending of commercial e-mails. Even in a situation covered by the soft opt-in rule, the e-mail address was originally collected following a clear manifestation of consent from the part of the individual with rights to decide upon the kind of content that will subsequently fill in the Inbox (it can be the individual holder of the address, or the individual in charge with administering the contact address of a legal person). Therefore as opposed to the E-Commerce Directive, an e-mail marketer risks being labelled as a spammer from the first message sent without a clear manifestation of consent¹⁹⁷, and not at a later point when it overlooks the wishes of an end-user.

The 2002 Privacy Directive also changes the manner in which the natural persons can object to and stop further commercial e-mails as well as the actors involved. In the E-Commerce Directive, it was the Member State's obligation to set up easily accessible registries in which the natural persons could register their objection. The marketers had only to make sure they check them "regularly". According to the rules in

¹⁹⁶ see the ICC Code of Conduct

¹⁹⁷ clearly a point found objectionable by the majority of marketers

the 2002 Privacy Directive the objection is to be sent directly to the marketer (through unsubscribe links) and has to be handled by the marketer himself.

Last but not least, it is unclear how the Privacy Directive envisages the functioning of an opt-out registry for legal persons and what rules would apply regarding timeliness of the recordings, the authority of the mother company to decide over the commercial e-mails received by the daughter company or the situation of the business entities lacking legal personality.

To sum up and answer the question in the title of this subsection, I find little grounds to consider the provisions in the two directives as representing one legislative solution in the fight against spam, but rather as being two separate parts of a legal framework that is supposedly in place to deal with spam. Either we consider that the provisions of article 7 of the E-commerce directive have been implicitly and partially abrogated by the enactment of the 2002 Privacy Directive¹⁹⁸, and they remain in force only in what regards the legal persons¹⁹⁹, or they are both in force and refer however to different business practices²⁰⁰. E-commerce Directive refers to commercial communications in general in article 6 and 7 to unsolicited commercial communications that are part of a marketer's practice, but without having the features usually associated with spam, while the 2002 Privacy Directive is a regulation designed to address spam issues. I will argue the latter point in Subsection 2.

Subsection 2 Fitness for the purpose

Up until now Europe does not have a special law dealing especially with the spam issue. Although the negative effects of spam have been stated on numerous occasions by the European officials, the topic is still addressed mainly by the two directives analysed in this thesis. There are legitimate grounds to believe that the provisions in article 7 of the E-commerce Directive, as much as they contain divergent

¹⁹⁸ this idea seems to be conveyed by the First Report on the Application of the E-Commerce Directive (COM(2003) 702 final) which states that "*the issue of unsolicited commercial communications via e-mail has now been dealt with at Community level by Directive 2002/58/EC*" (section 4.3)

¹⁹⁹ see Recital 45 of the 2002 Privacy Directive

²⁰⁰ Surprisingly, the idea is conveyed by the same document mentioned in footnote 198 (COM(2003) 702 final), stating that the issue of unsolicited commercial communications is being dealt with now by the 2002 Privacy Directive, as this issue has "increasingly become a problem for consumers and business alike", see page 10.

points from the 2002 Privacy Directive, are still in force and a relevant piece of the framework. First of all, although the 2002 Privacy Directive repeals expressly Directive 97/66/EC, it refers to the provisions of article 7 of the E-Commerce Directive without questioning their validity. Secondly, international fore²⁰¹ treats the E-Commerce provisions as a piece of the European anti-spam answer. Other reasons relate more to the circumstances in which the Directive was enacted. Gauthronet and Drouard (2001)²⁰² argue that the European anti-spam legislation was “a reaction to American privacy issues” and “the relevant law was in place before the phenomenon ever emerged in Europe”, while “the research conducted for this study reveal that Europe has not yet experienced an acute outbreak of unsolicited commercial e-mail or of spam”. If this is the case, the provisions in E-commerce Directive can be seen as a general framework²⁰³ stating the expected behaviour of all the marketers that do send unsolicited commercial communications and not a spam targeted norm per se. On the other hand, article 13 of the 2002 Privacy Directive is seen as a “victory” in the fight against spam²⁰⁴.

It is this “victory” that I question.

Without doubt, the opt-in regime introduced by the 2002 Privacy Directive changed some of the provisions of the Directive 97/66/EC that proved inefficient in the fight against spam. It attempted and partially succeeded in unifying the legal regime applicable all throughout Europe bringing a plus of legal certainty. Previously, through making use of their autonomy to chose either an opt-in or an opt-out²⁰⁵ regime for unsolicited communications²⁰⁶, the Member States fragmented the unity of the legal market failing to reach a common anti-spam approach. Therefore, the behaviour of the same marketer pursuing an e-mail marketing campaign and targeting e-mail holders without their prior consent, could have been regarded at the same time as spam in his

²⁰¹ http://www.itu.int/osg/spu/spam/legislation/legislation_europeanunion.html.

²⁰² Gauthronet & Drouard, op.cit, at 82.

²⁰³ See Recital (10) stating “In accordance with the principle of proportionality, the measures provided for in this Directive *are strictly limited to the minimum needed* to achieve the objective of the proper functioning of the internal market...”

²⁰⁴ “We Did It! *EU Parliament "Opts In"* Commercial Email in *European Economic Area* will not be allowed without *recipients' prior consent*, states the European Coalition Against Unsolicited Commercial Email, <http://www.euro.cauce.org/en/index.html> (last visited 20 August 2005). It is relevant that the quoted source considers unsolicited commercial email (UCE) as being “more commonly known as “spam”.

²⁰⁵ See an overview of the option of the European countries between opt-in /opt-out regime in May 2002 at <http://www.euro.cauce.org/en/lchaos.html> (last visited 20 Aug. 05).

²⁰⁶ According to article 12 of the Directive 97/66/EC.

own country (if that country implemented the opt-in regime) and a legitimate marketer in countries that implemented an opt-out regime. Additional difficulties were raised by the impossibility to link sometimes the e-mail address to a certain country and by the difficult detection of the right opt-out register to check.

At the same time, the newly introduced opt-in regime addressed the issue of the initial collection of the e-mail addresses, one of the problems commonly associated with spam. The previous opt-out regime legitimised the sending of the first commercial e-mail. It represented a weak defence against spam, as the commercial e-mail, once sent and received by the end-user, rarely allowed for subsequent removal (and the activation of the unsubscribe link, if present, did nothing more than confirming the address as valid, thus leading to more spam). At the same time, the opt-out regime placed additional burden on the end-user, making him responsible to stop the flooding of his address with unwanted mail (so he had to spend time and energy both in removing the existent unwanted content, and to take action to stop further messages). As the role of the end-user changed following the introduction of the opt-in regime (he is now the initiator of the commercial dialogue), it has become arguably easier to set the anti-spam filters to let in only the content that was expressly and knowingly agreed by the user. The opt-in targets also the uselessness of the spam messages. It is improbable that the user will give his prior and informed consent to something that he might later on claim as useless, and in any event, a legitimate marketer, as opposed to a spammer, would have a defence and a justification for having sent that particular content to that particular e-mail address, through stating the circumstances in which the consent was asked and received.

By changing the procedure through which the end-user manifests his will not to receive further commercial e-mails and relying not a third administrative party but the two parties involved (the sender and the receiver), the provisions in article 13 created a standard requirement for the inclusion of a workable opt-out link²⁰⁷, considering that most spam messages do not allow the receiver to refuse receiving the spam e-mails. Of course, a good point regarding the prohibition of disguised or concealed sender identity was maintained in the intention to outlaw the practice used by spammers to hide their

²⁰⁷ as reflected in the existing FEDMA and ICC Codes of Conduct.

tracks either by using a third party e-mail address as an alleged sender address or to use a fake address and abandon it immediately after.

The most important critique that can be brought to the current anti-spam legal provisions is that they attempt to treat two separate activities as being one and the same. The definitional inconsistency called for the compromise solution of the soft opt-in as a way to alleviate the concerns of direct marketers regarding regulatory overkill. In my opinion, a clear definition of both terms (“commercial communication” and “direct marketing”) would have been of increased importance, especially since official documents use the term “spam” as being synonym with “unsolicited commercial electronic mail”²⁰⁸ with reference to article 13 of the 2002 Privacy Directive²⁰⁹, but attention, documents issued before and after 2002, by the marketing associations set clear parameters distinguishing the two activities²¹⁰. In this context it seems misguided to borrow the terminology from one context and try to fit it into another while changing the scope of the activities comprised therein.

The effect of this inconsistency of approach is best reflected in the different regime applicable to the commercial e-mails sent to legal persons. An approach consistent with the stated synonymy between spam and unsolicited commercial communications would have justified one single regime for both natural and legal persons. Several reasons concur to my opinion:

While the difference in regime between business-to-business and business-to-consumer relations is well founded in general²¹¹, businesses and consumers alike suffer the negative consequences of spam, and the legal personality is absolutely irrelevant from the spammers’ point of view. The definition of spam does not relate the spam features with the legal personality of the potential receiver. Therefore, an opt-in regime for legal persons would have condemned the spam in general as business practice and as illegal personal data processing no matter to whom the e-mail addresses belongs, considering

²⁰⁸ see the introductory chapter of this thesis.

²⁰⁹ COM(2004) 28 final.

²¹⁰ See the final comments in the introductory Chapter of this thesis, especially footnotes 21 and 22.

²¹¹ Being a reflection of the more general principles of equity and the protection of the contractual weaker party.

the overall detrimental effect²¹² and not associate it solely to the “distress” caused to the individuals.

It is unlikely that a business will consider a CV sent by a private person without previous solicitation to be spam. It is even more unlikely that a newcomer on the market, sending information about the products and services it offers to all of the parties that he considers possibly interested, will be seen as a spammer and it is unlikely that he will continue to send e-mails to the same business that already rejected his proposal (that would not be in the interest of a good public image). But as previously analysed, spam is not about this kind of messages.

Since the European legislator did not provide a clear distinction between e-mail marketing involving also unsolicited commercial communications and spam, using instead the etiquette neuter terms consecrated by the business practice and literature, special cautions were required in order not to short-circuit legitimate communications that are intrinsic to the e-commerce practice.

To sum up, the European anti spam solution seems to be, for the most part, an appropriate tool against spam as it tackles some of the most important features of the commercial communications that can be regarded as spam. However, the definitional issues and the inconsistency regarding the level of protection for legal persons cannot be overlooked. Some of the negative consequences of the above mentioned minuses and relevant issues that have been disregarded by the European legislator will be addressed in the following section.

Subsection 3 Negative consequences?

One of the negative points regarding the European anti-spam legislative tool is that its constituent provisions are scattered throughout various Directives whose applicability is called by unclear references. SUA, Japan, Australia to give just a few examples, have enacted special legislation to deal with the particular issues involved by spam. In Europe, however, it seems that general principles of data processing, 3 articles

²¹² “Spam has negative impacts for consumers, businesses, Internet Service Providers (ISPs), legitimate e-mail marketers and virtually anyone else who uses e-mail for any reason”, Cristina Bueti “ITU Survey on anti-spam legislation worldwide” (July 2005), available at: http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_ITU_Bueti_Survey.pdf

dealing with the unclearly defined notion of “unsolicited commercial communications” and several provisions dealing with consumer protection are supposed to provide the national enforcement authorities²¹³ with sufficient legislative guidance in order to ensure an efficient fight against spam²¹⁴. This option translates however in supplementary difficulties in identifying the relevant provisions as well as in finding the way they fit in a “Lego” like framework.

In terms of content of the legal provisions, despite the numerous advantages of the opt-in rule, the inconsistency of approach with regard to the scope of unsolicited commercial communications leads to an overprotection for legitimate direct marketers and an reduced level of protection in the fight against spam. The need of a compromise required by the inclusion in the same term of two very distinct business practices is reflected in the need to discriminate between the regime applicable to natural and to legal persons (which does not reflect an existing difference in the practice of the spammers) and in the provisions referring to preexisting business relations (a framework preventing the marketers to abuse an existing customer relation is welcomed, but as empirical studies referred to in this thesis showed, customers don’t regard commercial e-mails coming from businesses to whom they previously dealt with as spam). Although a broader discussion on the topic is beyond the scope of this thesis, equating spam with the notion of “unsolicited commercial communications” indirectly legitimizes other types of spam, which are not commercial in nature.

Due to article 4 of the Directive 95/46/EC, the provisions of the 2002 Privacy Directive (and therefore the opt-in rules) do not apply when the data controller is not established in a Member State or does not make use of equipment located in a Member State. Therefore, the solution found by the European legislator does little to protect the end-users from the spam coming from outside the European Union, which according to some studies²¹⁵ accounts for the most part of spam (see Annex 3).

²¹³ either courts, or administrative bodies such as consumer protection authorities or data protection units (see the Anti-Spam Law Enforcement Report (May 2005) , OECD, available at <http://www.oecd.org/dataoecd/18/43/34886680.pdf> (last visited 21 August 2005) for a list of authorities with responsibilities for enforcement of laws related to spam).

²¹⁴ I am not questioning the role of the codes of conduct, what is in focus now is the legislative answer.

²¹⁵ See for example ITU survey (2005), op.cit.

Although I can't argue that the negative consequences presented above outweigh the positive aspects, I see the European anti-spam legislation as more of a verbal declaration of war than as a machine-gun pointed at spammers and their activity. This statement does not overlook the role that the Member States themselves have in transposing the Directives and in making its provisions more concrete, but as long as the general framework is unclear and leaves room for interpretation, the overall result can't be other than divergent national solutions and ultimately a fragmented approach.

Section 4: Other legislative solutions.

As a business practice that transcends all geographic and jurisdictional boundaries and as a “plague” on the Internet communications, spam is a worldwide challenge. Therefore, I consider appropriate to point out some²¹⁶ of the main convergent and divergent attempts made worldwide in order to bring spam to a halt, through legislative measures. Ultimately, the efficiency of legislative measures supposed to bring it to a halt depends ultimately of the results of a common effort of harmonization between existing anti-spam laws.

Most of the laws that try to deal with spam associate this notion with the term “unsolicited commercial communications”. The association is not surprising since spam has originally emerged like an advertising practice, and a large part of the spam messages are oriented towards promoting various products and services²¹⁷. Although some laws use the term “spam” in the title (see for example the American CAN-Spam Act(2003)²¹⁸, or the Australian Spam Act(2003)²¹⁹), their definition section addresses the meaning of commercial messages and the circumstances in which they are deemed to be

²¹⁶ for a detailed comparative analysis of spam laws, see Derek E.Bambauer et.al., A COMPARATIVE ANALYSIS OF SPAM LAWS: THE QUEST FOR A MODEL LAW (July 2005), available at http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Comparative_Analysis_of_Spam_Laws.pdf (last visited 22 August 2005)

²¹⁷ see the definitions provided in the Introductory chapter of this thesis

²¹⁸ “Controlling the Assault of Non- Solicited Pornography and Marketing Act of 2003 ”, USA, available at <http://news.com.com/pdf/ne/2003/FINALSPAM.pdf> (last visited 22 August 2005)

²¹⁹ “An Act about spam, and for related purposes” Australia (2003), available at <http://scaleplus.law.gov.au/html/pasteact/3/3628/top.htm> (last visited 22 August 2005)

unsolicited²²⁰. However, there is no common approach whether spam equals unsolicited commercial communications in general (as it is the case in the European Directives) or apart from being unsolicited and commercial, spam messages infringe some other statutory provisions. The Japanese Law²²¹ is to be noted in this context, since it defines “specified e-mail (spam)” as referring to “the action whereby e-mailers (limited to organizations looking to make a profit or individuals carrying out a business) send out emails advertising or promoting either their or someone else's business to people other than those who have agreed to receive these”. Not only it contains an express reference to “spam” but it limits the range of possible senders to businesses.

As previously shown in this thesis, the European Privacy Directive from 2002 establishes different anti-spam rules when the targeted e-mail address belongs to a natural person as opposed to a legal person. I questioned the opportunity of this dichotomy in the context of spam throughout this Chapter. In fact, the solution is not embraced by any of the non-European laws examined. The CAN-Spam act refers to the “recipient” of the unsolicited e-mails as being the “authorized user of the electronic mail address to which the message was sent or delivered”. Similarly, the Australian Act defines the notion of “consent”²²² by referring to the manifestation of will of “the individual or organization concerned”. Other laws²²³ are not referring at all to the potential receiver of the spam messages, dealing exclusively with those involved in the illegal collection of the e-mails and those using the e-mails thus collected for direct marketing purposes.

According to the study done by Bambauer (2005)²²⁴, there are no standard rules establishing the permitted sources from which the e-mail addresses can be collected. The country that is nowadays responsible for the most spam, the United States, prohibits²²⁵ address harvesting from Internet websites or proprietary online services only when such collection contravenes to a stated declaration that such website or online service “will not give, sell, or otherwise transfer addresses maintained by such website or online service to

²²⁰ see Section 3 (2)a of the American act defining the term “commercial electronic mail message” and section 6(1) of the Australian act defining the meaning of commercial electronic messages

²²¹ “Law on Regulation of transmission of Specified Electronic Mail(2004), http://www.soumu.go.jp/joho_tsusin/eng/Releases/Telecommunications/news041227_8.html

²²² see Schedule 2 of the Australian Act

²²³ links to several anti-spam laws are provided at <http://www.itu.int/osg/spu/spam/law.html>.

²²⁴ Derek E.Bambauer, op cit.

²²⁵ Section 5 (b)(1) of the CAN-Spam Act

any other party for the purposes of initiating, or enabling others to initiate, electronic mail messages”. The same idea is present also in the S-Korean Law from 2001²²⁶. Moreover, the Argentinean Law from 2000²²⁷ states that the consent of the data subject is not necessary when the personal data (including the e-mail address) was collected from publicly available websites. On the other hand, while the European Union legislation makes no reference to the prohibition of the production, use, making available of software tools that can be used in order to generate addresses (what is referred to as dictionary attacks), several other legislations outlaw expressly this practice. Section 5(b)(1)(A)(ii) of the CAN-Spam Act prohibits the initiation of transmissions to addresses that were obtained through “combining names, letters, or numbers into numerous permutations”. Section 16 (6) of the Australian Act prohibits the “sending of commercial electronic message to a non-existent electronic address”. Similarly, article 50 (6) of the S-Korean Law prohibits the use of “programs and other technical devices which make it possible to automatically identify contact information of receivers such as phone numbers, e-mail addresses, addresses, etc. through the combination of numbers, codes and letters”.

Although some differences might be emphasized in this regard as well²²⁸, the countries that have enacted anti-spam legislations agree on the importance of prohibiting the use of false header information in all commercial communications. This includes the prohibition of false sender addresses, false or misleading return addresses and most importantly false subject lines. Similarly, giving the end-user the possibility to object at any point to further commercial communications and honoring this option has become a standard requirement in the anti-spam laws.²²⁹

²²⁶ Act on Promotion of Information and Communication and Communications Network Utilization and Information Protection of 2001, available at: http://www.mic.go.kr/eng/res/res_pub_db/res_pub_mic_wp/2003/whitepaper2003/in3_7_5.htm, section 50-2 (1)

²²⁷ Personal Data Protection Act (2000), available at <http://infoleg.mecon.gov.ar/infolegInternet/anexos/60000-64999/64790/norma.htm>, see article 5(2)(a) .

²²⁸ for example, some countries request not only that the subject line is not misleading, but impose also a labeling requirement for the easy identification of the commercial messages: South Korea uses “@”, the United States and Singapore have proposed “ADV”.

²²⁹ However, different requirements are formulated regarding the unsubscribe function and the ways in which the end-users might communicate their will to the marketer. Australia compels the senders to provide the opt-out function through the same technology that was used to convey the commercial message. US require that the opt-out mechanism that was offered to the receiver remain usable for at least

If some of these provisions might be easily reconciled in a harmonization initiative aimed at achieving an effective enforcement, the key factor on which the States are still far from reaching an agreement is whether or not the prior consent of the legitimate e-mail address holder is required, as well as on the desired quality of the consent. Among the states that are considered nowadays to be on the top 10 list of spam senders, US, S-Korea, Japan, Argentina and Hong Kong have an opt-out regime. Russia and China do not have yet anti-spam rules, although in the first case, the drafting of anti spam laws with an opt-in approach has been initiated²³⁰. Canada²³¹ has an opt-in regime, since article 7 of the PIPEDA Act of 2000 states expressly the circumstances where the collection of the personal data can be done without the consent of the data subject, and the direct marketing purposes are not within the scope of these exceptions. Australia and the European Union have adopted also an opt-in approach. However, the meaning of consent in the two legislations is dissimilar in an essential way: while the European Union requires a “prior, express and informed consent” of the e-mail address owner, Schedule 2 of the Australian Act permits both the express and the “reasonably inferred consent” of the individual or the organization concerned. The consent can be inferred by examining both the conduct of the parties in the particular case and the existing business or other relations between them.

There is a reduced likelihood that a compromise solution can be found: either the first commercial e-mail is permitted and the end-user is given the option to stop the commercial e-mails, or it is prohibited to send commercial e-mails without the user’s prior consent.

“While a model law could allow adopting states to make their own decision on this element, doing so would weaken consistency and enforcement since messages sent from an opt-out regime would not (absent a reciprocal enforcement agreement) constitute an offense, even if sent to a recipient in an opt-in jurisdiction. Any anti-spam

30 days after the commercial message was sent. Similarly, S-Korea prohibits the marketer to take “technical measures with the aim of evading or obstructing the rejection of receiving such advertisement information by receivers”.

²³⁰ The project started in 2003 at the initiative of the UNESCO IFAP (Information for All Programme) National Committee of Russia, see <http://www.ifap.ru/eng/projects/antispam.htm> for details.

²³¹ See Personal Information Protection and Electronic Documents Act (PIPEDA) <http://laws.justice.gc.ca/en/p-8.6/93196.html> ,

regime with an opt-in system at its core is almost certain to be a more aggressive anti-spam regime than an opt-out system. This divide in existing provisions will constitute a major issue with which harmonization must contend”²³².

The above comparison highlighted somehow surprisingly that the great majority of the countries that are among the first 10 world spammers do have detailed provisions outlawing the activities commonly associated with spam. Therefore their partial ineffectiveness in stopping the continuous flooding of e-mail addresses has to be associated with other factors than a regulatory black hole. One might thus wonder about the role that the legislation alone can be expected to play in the fight against spam.

²³² Derek E.Bambauer(2005), op.cit, page 17

CONCLUSION

*“Regulators must consider how their traditional laws interact with other modes of governing behavior, including the use of technological restrictions implemented through software code, economic incentives via market mechanisms, and social controls brought to bear through norms”.*²³³

This thesis aimed at analyzing the anti-spam European provisions by examining the manner in which they respond to the spam anomaly. Instead of choosing to fragment the normative text into easily definable concepts, my goal was to look at spam in the business context in which it occurs. That required first of all to clearly identify the investigated business practice and to point out similarities and discrepancies between this advertising practice and other, related ones. All business practices are the result of an opportunity and survive only if they are mutually beneficial for the business party and for the potential customer. Therefore, Chapter 1 started by stressing the existing opportunity that marketers have in collecting, using and commercializing personal information, largely available from different sources, at virtually no cost. It subsequently discussed the crucial issue of the personal data character of the e-mail address. Chapter 1 highlighted in its final part the ethical and behavioural differences between the legitimate e-mail practices and spam.

The conclusions reached in the first chapter, especially those related to the personal data character of the e-mail addresses are used in Chapter 2 as premises for a discussion about values and about the potential conflicts that might arise in the attempt to find a balance between potentially conflicting interests of the actors involved (end-users and direct marketers). Most importantly, this chapter identifies and arguments the difference in focus between the two main legal instruments analyzed and the different weight awarded by the European legislator, through these legal provisions, to the economic interest of the marketer, on one side, and the privacy and associated interests of the end-users, on the other.

²³³ Derek E.Bambauer, op.cit, page 15

The evaluation of the efficiency and the effectiveness of the European anti-spam legislation, which is the focus of Chapter 3, takes into account three elements: the business practices that are commonly associated with spam, as a factual argument, the interests of the actors involved, that generates the dynamic of the relations established between direct marketers and potential receivers of the commercial messages as well as the reflection of these two elements in the legal provisions of the E-Commerce Directive and the 2002 Privacy Directive. Therefore, the conclusion reached is not based only on a limited legal text dissection, but includes arguments relating to social psychology, marketing, economic theory.

Using this method I managed to identify several impediments that prevent the European response to spam to become an appropriate tool to be used in annihilating spam. They relate to definitional inconsistencies, to clashes between legal texts equally applicable, to differences in regime not justified by the practices involved in spam and to the insufficient level of protection for the legal persons that become victim of this unethical, unfair and generally detrimental business practice.

De lege ferenda, the anti-spam normative solution could benefit from an explicit and coherent definition of the two different business practices: e-mail marketing and spam, and I believe the European legislator should not refrain from “calling things for what they are”, instead of using the unclear term of “unsolicited commercial communications”.

At the same time, if the provisions of both E-Commerce Directive (art.6 and 7) and 2002 Privacy Directive (art.13) are to be considered in force, than it should be made more clear that they address different business realities. Several arguments have been presented in Chapter 3 in order to justify that article 13 of the 2002 Privacy Directive is a norm designed to address spam, whereas the E—Commerce Directive ones may only be seen as a general framework setting the rules for the unsolicited commercial communications that cannot be qualified as spam. Therefore, the soft opt-in rule would be better placed in the E-Commerce Directive than in the 2000 Privacy Directive, as spam appears only exceptionally in already existing businesses relations. Moreover, the privacy legislation in general does not instantiate different principles and levels of protection based on the existence of a business relation between data subject and the data

controller. The result achieved by the inclusion of this rule in the legal text establishing a general framework for the unsolicited commercial communications would send a signal to the e-mail marketers that they cannot abuse existing business relations and would make sure that the customer has a viable alternative to the aggressive practice of the spammers.

Similarly, unifying the legal anti-spam provisions applicable to both natural and legal persons would first of all reflect better the business reality that spam does not discern between the e-mail addresses of the individuals and those of businesses, and secondly would relate the banning of spam not only to the emotional distress caused to the individuals but to the overall costs and negative consequences that impinge on the Internet communications in general.

I do believe that legislation is a powerful mechanism and a guarantee that non-pecuniary values such as equity, autonomy, privacy, non-discrimination are protected. In fact, since data protection in itself, separate from the right to privacy is starting to be recognized in Europe as a basic human right²³⁴, the argument that “spammers don’t care about the law anyway” should be accepted with care. I can see several reasons why the market should not be permitted to set alone the “price” of personal information, absent all regulatory constraints. First of all, there will always be an information asymmetry between customers and marketers, which will prevent the formers to perceive the real level of privacy intrusion made possible by the current technology as well all the uses to which different pieces of personal information could be put – rational factors that can contribute to identifying the true value of the personal data disclosed. Secondly, privacy is threatened by the aggregated effect of small violations, therefore the privacy preferences of the individual might be different for a particular intrusion and for privacy as a whole. Thirdly, most individuals view privacy as a long term, abstract gain, whereas the benefit resulted from personal data disclosure is usually tangible and immediate. This again prevents an equitable remuneration for the disclosure, and only an illusion of informational self determination.

²³⁴ see for example the Charter of Fundamental Rights of the European Union, adopted 7.12.2000 (OJ C364, 18.12.2000 p.1) in article 8 and also art I-51 of the Treaty establishing a Constitution for Europe (providing a right to protection of personal data)

Quite normally, the legislation is only part and parcel of a broader range of measures targeted against spam. Co-regulation, the use of self-regulatory mechanisms in order to translate the general normative rules into more detailed codes of conduct, may respond better to the complexities of spam than if only laws would be relied on. However, even the most detailed rules of conduct cannot supplement the pro-active involvement of the end-user himself. No one would argue that being a part of the “off-line” society means learning a series of preventive conducts and not relying only on laws guaranteeing the protection from various wrongs caused by the others. Similarly, actions aimed at raising awareness about the threats and the reasonable behaviour when exploring the “on-line world” can only be in the interest of the users. This is probably where future efforts of the international and national bodies alike should be directed more in the future, especially considering the increasing number of Internet users worldwide.

Selective bibliography:

A. Statutes and legislation referred to in this thesis:

- “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 L 281 , 23/11/1995 P. 0031 – 0050.
- “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*”, Official Journal L.178 of 17 July 2000.
- “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*”, Official Journal L 201, 31/07/2002, P. 0037-0047
- “Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 *concerning unfair business-to-consumer commercial practices in the internal market*” O.J. L 149/22 11.6.2005
- “Directive 92/28/EEC of the European Parliament and of the Council of 31 March 1992 *on the advertising of medicinal products for human use*” Official Journal No L 113 of 30. 4. 1992, p. 13
- “Directive 97/55/EC of the European Parliament and of the Council of 6 October 1997 amending Directive 84/450/EEC *concerning misleading advertising so as to include comparative advertising*” Official Journal L 290, 23.10.1997
- “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 L 24/1 30.1.98
- “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*”, Official Journal L 144, 04/06/1997 P. 0019 – 0027

“Directive 98/43/ EC of the European Parliament and of the Council of 6 July 1998 on the *approximation of the laws, regulations and administrative provisions of the Member States relating to the advertising and sponsorship of tobacco products*” Official Journal L 213 , 30/07/1998 P. 0009 - 0012

Argentinean Law (2000): “Personal Data Protection Act”, available at: <http://infoleg.mecon.gov.ar/infolegInternet/anexos/60000-64999/64790/norma.htm>.

Australian Spam Act (2003): “An Act about spam, and for related purposes” Australia (2003), available at <http://scaleplus.law.gov.au/html/pasteact/3/3628/top.htm>.

Belgian Law(2003): “Arrêté royal visant à réglementer l’envoi de publicités par courrier électronique”, 4.04.2003, published in the Moniteur Belge- Belgisch Staatsblaad on 28.05.2003, page 29292, available at: <http://www.iab-belgium.be/Media/pdf/kb040403.pdf>.

Canadian Law (2000) “Personal Information Protection and Electronic Documents Act (PIPEDA)” available at: <http://laws.justice.gc.ca/en/p-8.6/93196.html>.

CAN-Spam Act, USA- “Controlling the Assault of Non- Solicited Pornography and Marketing Act of 2003”, available at: <http://news.com.com/pdf/ne/2003/FINALSPAM.pdf>.

French Law: “Loi du 6 janvier 1978 relative à l’informatique, aux fichiers et aux libertés (modifiée par la loi relative à la protection des personnes physiques à l’égard des traitements de données à caractère personnel du 6 août 2004)”

Japanese Spam Law (2004): “Law on Regulation of transmission of Specified Electronic Mail available at: http://www.soumu.go.jp/joho_tsusin/eng/Releases/Telecommunications/news041227_8.html.

S-Korean Law (2001): “Act on Promotion of Information and Communication and Communications Network Utilization and Information Protection of 2001”, available at:http://www.mic.go.kr/eng/res/res_pub_db/res_pub_mic_wp/2003/whitepaper2003/in3_7_5.htm.

Regulation (EC) No 2006/2004 the European Parliament and of the Council of 27 October 2004 *on cooperation between national authorities responsible for the*

enforcement of consumer protection laws (the Regulation on consumer protection cooperation) L 364/1, 9.12.2004

Consult further <http://www.itu.int/osg/spu/spam/law.html> for all the existing anti-spam laws and anti-spam statutory provisions in the world at present.

B. Books:

- Acquisti, Alessandro & Grossklags: '*Privacy and Security of Personal Information- Economic incentives and technological solutions*' in J. Camp and R. Lewis (eds), '*The Economics of Information Security*' (Kluwer, 2004)
- Acquisti, Alessandro & Grossklags: '*Privacy Attitudes and Privacy Behavior- Losses, gains and hyperbolic discounting*' in J. Camp and R. Lewis (eds), '*The Economics of Information Security*' (Kluwer, 2004)
- Beverly-Smith, Huw: '*The commercial appropriation of personality*' (Cambridge University Press, 2002)
- Blok, Peter: '*The limits of informational self-determination*' in Anton Vedder (ed.) "*Ethics and the Internet*" (Intersentia 2001)
- Bygrave, L.A.: '*Data Protection Law- Approaching its Rationale, Logic and Limits*' (Kluwer Law International, 2002)
- Couser, James: '*Cyber Property*' in Mathias Klang and Andrew Murray (eds.), '*Human rights in the digital age*' (London: GlassHouse Press, 2005)
- Culnan, Mary J. & Bies, Robert J.: '*Managing Privacy Concerns Strategically: The Implications of Fair Information Practices for Marketing in the Twenty first Century*', in Collin J Bennett & Rebecca Grant (eds.) "*Visions of Privacy. Policy Choices for the Digital Age*" (University of Toronto Press, 1999)
- Custers, Bart: '*Data mining and group profiling on the Internet*' in Anton Vedder (ed.) "*Ethics and the Internet*" (Intersentia 2001)
- Godin, Seth: "*Permission Marketing: Turning strangers into friends, and friends into customers*" (Simon & Schuster –New York 1999)
- Johnson, Jeffery L.: '*Immunity from the illegitimate focused attention of others: an explanation of our thinking and talking about privacy*' in Anton Vedder (ed.) "*Ethics and the Internet*" (Intersentia 2001)

- Moor, James H.: '*Towards a Theory of Privacy in the Information Age*' in Terrell Ward Bynum & Simon Rogerson (eds.) "Computer Ethics and Professional Responsibility" (Blackwell Publishing, 2004)
- Rubin, Paul H. and Lenard, Thomas M.: '*Privacy and the Commercial Use of Personal Information*' (Boston: Kluwer Academic Publishers, 2002)
- Rule, James & Hunter, Lawrence: '*Towards property rights in Personal Data*' in Collin J Bennett & Rebecca Grant (eds.) "Visions of Privacy. Policy Choices for the Digital Age" (University of Toronto Press, 1999)
- Wong, Rebecca: '*Privacy: Charting its Developments and Prospects*' in Mathias Klang and Andrew Murray (eds.), 'Human rights in the digital age' (London: GlassHouse Press, 2005)

C. Journal articles

-off line journals

- Cheng, Tania S.L. '*Spam regulation- Recent international attempts to CAN- Spam*' in Computer Law and Security Report, vol.20, no.6, 2004, pp 472 – 479.
- Chetwin, Maree & Clarke, Bevan '*The Relative Effectiveness of Technology v. Legislation in Curtailing Spam*' Directive The Journal of E-commerce, Technology and Communications, December 2004, pp. 192-197.
- Davidson, Steve & Kapsner-Griffin, Miki: '*The US tackles Spam*' in The Journal of E-commerce, Technology and Communications, January 2005, pp. 1-3.
- Funk, Axel, Zeifang, Gregor et al. '*Unsolicited commercial emails in the jurisdictions of Germany and the USA*' in Computer Law Review International, issue 5, August 2004, pp. 138- 144.
- Goodman, Cathy: '*Privacy: Recognition of a consumer right*' in Journal of Public Policy and Marketing vol.10, 1 (spring 1991)
- Kam, Steven: '*Intel Corp. v. Hamidi: trespass to chattels and a doctrine of cyber-nuisance*', in Berkley Technology Law Journal no.1, 2004, pp 427-453.
- Kasprzycki, Dariusz: '*Trends in regulating unsolicited commercial communications*' in Computer Law Review International, issue 3, June 2004, pp. 76- 81.

- Mayer et al.: *'An integrative Model of Organizational Trust'* Academy of management review 20(3), 1995, pp. 709-734
- Milne, G.R. & Bloom, P.N.& Adler, R.: *'Avoiding misuse of New Information Technologies: legal and societal considerations'*, Journal of Marketing, vol.58, January 1994, pp.98- 110.
- Milne, G.R. & Boza, Maria-Eugenia: *'Trust and concern in consumer's perceptions of marketing information and management practices'*, Journal of interactive marketing, vol.13, no.1, winter 1999, pp.5- 24
- Milne, G.R. & Rohm, A. J.& Bahl, S.: *'Consumers' Protection of Online Privacy and Identity'* The Journal of Consumer Affairs, vol. 38, no. 2, 2004
- Milne, G.R. & Rohm, A. J: *'Consumer privacy and name removal across direct marketing channels: Exploring opt-in and opt-out alternatives'* Journal of Public Policy and Marketing, vol.19(2), fall 2000, pp. 238-249
- Milne, G.R: *'Consumer Participation in mailing lists: a field experiment'*, Journal of Public Policy and Marketing, vol.16(2), fall 1997, pp.98- 110
- Milne, George R.: *'Privacy and ethical issues in database/ interactive marketing and public policy: a research framework and overview of the special issue'* in Journal of public policy and marketing, vol. 19(1), spring 2000, pp.1-6
- Mossoff, Adam: *'Spam- Oy, What a Nuisance!'* in Berkley Technology Law Journal , spring 2004, pp. 626-666
- Motion, Paul: *'Spam Banned?'* The Journal of E-commerce, Technology and Communications, June 2004, pp. 77- 78.
- Munir, Abu Bakar: *'Unsolicited commercial email: Implementing the EU Directive '* , Journal of E-commerce, Technology and Communications, August 2004, pp. 105-108
- Petty, Ross D *"Marketing without consent: consumer choice and costs, privacy and public policy"*, Journal of Public Policy and Marketing, no.19 (spring) 2000, pp.42-53
- Phelps, Joseph & Nowak, Glen & Ferrell, Elizabeth: *'Privacy Concerns and Consumer Willingness to Provide Personal Information'* Journal of Public Policy and Marketing, no.19 (spring) 2000, pp.27- 41

Sheehan, Kim Bartel and Hoy, Mariea Grubbs: '*Dimensions of privacy concerns among online consumers*' Journal of Public Policy and Marketing, vol.19, spring 2000, pp. 62-73

Spinello, R.A.: '*Ethical reflections in the problem of spam*', Ethics and Information Technology vol. 1 no 3 pp.185-191 (1999).

- on-line articles and journals

- Acquisti, Alessandro & Grossklags: '*Privacy and Rationality in Individual Decision Making*' in IEEE Security & Privacy, January/ February 2005, pp 24-30, available at: <http://csdl2.computer.org/persagen/DLAbsToc.jsp?resourcePath=/dl/mags/sp/&toc=c omp/mags/sp/2005/01/j1toc.xml&DOI=10.1109/MSP.2005.22>
- Austria, Stephanie: '*Forgery in Cyberspace: The Spoof could be on you!*' in Journal of Technology Law and Policy, University of Pittsburg School of Law, vol. I, 2, spring 2004, available at <http://tlp.law.pitt.edu/articles.html>
- Ayres, Ian & Funk, Matthew: '*Marketing Privacy: A Solution for the Blight of Telemarketing (and Spam and Junk Mail)*', 2002, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=303303
- Chang, Susan & Morimoto, Mariko '*An Assessment of Consumer Attitudes toward Direct Marketing Channels: A Comparison between Unsolicited E-Mail and Postal Direct Mail*', Michigan State University April 1, 2003 available at: <http://www.inma.org/subscribers/papers/2003-Chang-Morimoto.doc>
- Cisneros, Danielle: '*Do not advertise: the current fight against unsolicited advertisements*', in Duke Law and Technology Review, 0010, 2003, available at: <http://www.law.duke.edu/journals/dltr/articles/2003dltr0010.html>
- Cranor, Lorrie Faith & Reagle, Joseph & Ackerman, Mark S.: '*Beyond Concern: Understanding Net Users' Attitudes About Online Privacy*' AT&T Labs-Research Technical Report TR 99.4.3, available at :
- De Boni, Marco & Prigmore, Martyn: '*Privacy and the information economy*' in Proceedings of the IADIS International e-Society 2003 Conference, Lisbon 2003 available at: <http://www-users.cs.york.ac.uk/~mdeboni/papers/IADIS2003-DeBoniPrigmore-1v1.pdf>
- Dinev, Tamara & Hart, Paul: '*Privacy Concerns And Internet Use – A Model Of Trade-Off Factors*' (2004) available at :

http://www.ebusinessforum.gr/content/downloads/Privacy%20Concerns%20And%20Internet%20Use%20_A%20Model%20Of%20Trade-Off%20Factors.pdf

Gomes, L.H., Cazita, C. et.al.: 'Characterizing a Spam traffic', available at:
<http://www.imconf.net/imc-2004/papers/p356-gomes.pdf>

Laudon, Kenneth C.: 'Extensions to the Theory of Markets and Privacy: Mechanisms of Pricing Information', available at:
<http://www.ntia.doc.gov/reports/privacy/selfreg1.htm#1D>

Laudon, Kenneth C.: 'Markets and privacy' in Communications of the ACM, vol.39, no.9, September 1996, available on-line at:
<http://delivery.acm.org/10.1145/240000/234476/p92-laudon.pdf?key1=234476&key2=6581035211&coll=GUIDE&dl=ACM&CFID=51736431&CFTOKEN=91883192>

Lueg, Christopher: 'Spam and Anti-Spam Measures: Look at Potential Impacts', June 2003 available at:
<http://proceedings.informingscience.org/IS2003Proceedings/docs/206Lueg.pdf>.

Margulis, Stephen T.: 'Privacy as a Social Issue and Behavioral Concept' in Journal of Social Issues, vol.59, no 2, 2003, pp.243-261 available at <http://www.blackwell-synergy.com/doi/abs/10.1111/1540-4560.00063> .

Nicola Lugaresi "European Union vs. Spam: A Legal Response" available at:
<http://www.ceas.cc/papers-2004/145.pdf>.

Ravine, Laura D.: 'Footprints in Cyberspace. Using Transactional Data to Target Advertising', in UCLA Journal of Law and Technology, no. 4, 1998, available at
<http://www.lawtechjournal.com/archives/blt/i4-ldr.html>

Rice, Cindy M. : 'Comment: The TCPA: A Justification for the Prohibition of Spam in 2002?' in North Carolina Journal of Law & Technology, volume 3, issue 2: spring 2002, available at: <http://www.jolt.unc.edu/vol3/Rice-V3I2.pdf>

Volkman, Richard: 'Privacy as life, liberty, property' in Ethics and Information Technology 5/2003, 199–210, available at:
<http://portal.acm.org/citation.cfm?id=972561.972577&coll=GUIDE&dl=guide>.

D. Reports and other documents:

D.1. from the European Commission

“Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee of the Regions *on unsolicited commercial communications or ‘spam’*” Brussels, 22.01.2004, COM (2004) 28 final.

“*Seventh report on the situation regarding the protection of individuals with regard to the processing of personal data and privacy in the European Union and in third countries covering the years 2002 and 2003*”, 21 June 2004

CNSA: “*Cooperation procedure concerning the transmission of complaint information and intelligence relevant to the enforcement of article 13 of the Privacy and Electronic Communication Directive 2002/58/EC, or any other applicable national law pertaining to the use of unsolicited electronic communications*”, available at: http://europa.eu.int/information_society/policy/ecommm/doc/todays_framework/privacy_protection/spam/cooperation_procedure_cnsa_final_version_20041201.pdf.

Commission of the European Communities: “*Study on the protection of the rights and interests of legal persons with regard to the processing of personal data relating to such persons*” (Study Contract ETD/97/B5-9500/78), 1998 (Douwe Korff)

Commission of the European Communities: “*Unsolicited Commercial Communications and Data Protection*” (Internal Market DG – Contract n° ETD/99/B5-3000/E/96), January 2001 (Serge Gauthronet and Etienne Drouard)

Commission of the European Communities: “*Unsolicited Commercial Communications and Data Protection*” (Internal Market DG – Contract n° ETD/99/B5-3000/E/96), January 2001 (Serge Gauthronet and Etienne Drouard) - summary of study findings.

Committee on Legal Affairs and the Internal Market: “*Report on the proposal for a European Parliament and Council directive concerning unfair business-to-consumer commercial practices in the Internal Market and amending Directives 84/450/EEC, 97/7/EC and 98/27/EC (the Unfair Commercial Practices Directive)*”, (COM (2003) 356 – C5-0288/2003 – 2003/0134(COD)), Final A5-0188/2004

Communication from the Commission: “*European Governance: Better lawmaking*”, COM (2002) 275 final, Brussels, 5.6.2002

Presidency Paper, “*Unsolicited communications for direct marketing purposes or spam*”, Council of the European Union, Brussels, 24 November 2004, 15148/04.

Report from the Commission to the European Parliament, the Council, the European Economic and Social Committee: “*First Report on the application 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)*” COM (2003) 702 final.

D.2. from the Art. 29 Data Protection Working Party

“*Opinion 1/2000 on certain data protection aspects of electronic commerce*”
5007/00/EN/final WP 28

“*Opinion 7/2000 on the European Commission 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 of 12 July 2000*”
5042/00/EN/FINAL WP36

“*Opinion 3/2003 on the European code of conduct of FEDMA for the use of personal data in direct marketing*” 10066/03/EN final WP 77

“*Opinion 5/2004 on unsolicited communications for marketing purposes under article 13 of Directive 2002/58/EC*”, 11601/EN WP90

“*Recommendation 2/2001 on certain minimum requirements for collecting personal data on-line in the European Union*”, 5020/01/EN/ Final, WP 43.

“*Working Document Privacy on the Internet - An integrated EU Approach to On-line Data Protection-*” 21st November 2000, 5063/00/EN/FINAL WP 37.

“*Working Document on Blacklists*”, 3 October 2002, 11118/02/EN/final WP 65

D.3. from other sources

“*Antispam- A Guideline from the Confederation of Danish Industries and ITEK*” (2003)
available at <http://billed.di.dk/wimpfiles/lores/image.asp?objno=/298860.pdf>.

“*EuroISPA presentation to European Commission Press Briefing*”, 15 July 2003, Brussels, available at: http://www.euroispa.org/docs/030715_spampresentation.pdf.

“FEDMA comments *regarding the Working Document on the processing of personal data and the protection of privacy in the electronic communication sector*, 18 may 2000”, available at:
<http://europa.eu.int/ISPO/infosoc/telecompolicy/review99/nrfwd/FEDMA22e.htm>.

“FEDMA European code of practice for the use of personal data in direct marketing”(2003), available at <http://www.fedma.org/img/db/FEDMACodeEN.pdf>

“FEDMA's Code of Conduct on e-Commerce & Interactive Marketing” (2000), available at: http://www.fedma.org/img/db/Code_of_conduct_for_e-commerce.pdf

“FPS Economy, SMEs, Self-Employed and Energy – Belgium « Spamming » 24 questions & answers” – January 2005 available at:
http://mineco.fgov.be/information_society/spamming/spamming_note_en.pdf

“Position de la CNIL sur la prospection par courrier électronique dans le cadre professionnel” (02.03.2005), available at:
[http://www.cnil.fr/index.php?id=1780&news\[uid\]=238&cHash=6dd2646505](http://www.cnil.fr/index.php?id=1780&news[uid]=238&cHash=6dd2646505)

“Significant Developments in Global Internet Law in 2003” Covington & Burling (2004)
www.cov.com/publications/GlobalInternetLaw.html

“Significant Developments in Global Internet Law in 2004” Covington & Burling (2005)
http://www.cov.com/download/content/brochures/Internet_2004.pdf

“The Direct Marketing Association (UK)'s comments on the Working Document on the processing of personal data and the protection of privacy in the electronic communication sector”, available at:
<http://europa.eu.int/ISPO/infosoc/telecompolicy/review99/nrfwd/DMA22e.htm>

Ann Cavoukian, Information and Privacy Commissioner Ontario, “*Privacy as a fundamental human right vs. an economic right: an attempt to conciliation*” 1999 available at http://www.ipc.on.ca/userfiles/page_attachments/pr-right.pdf

AT&T Labs-Research Technical Report: “*Beyond Concern: Understanding Net Users' Attitudes about Online Privacy*” TR 99.4.3, available at:
<http://www.research.att.com/resources/trs/TRs/99/99.4/99.4.3/report.htm>.

Centre for Democracy & Technology: “*Why Am I Getting All This Spam? Unsolicited Commercial E-mail Research Six Month Report*” March 2003, available at:
<http://www.cdt.org/speech/spam/030319spamreport.shtml>.

- European Advertising Standards Alliance, “*Recommendations for the issue paper for the EU Workshop on unsolicited commercial communications or spam*”, November 4th 2003, available at: http://www.easa-alliance.org/news_views/en/position_spam%20issue.pdf.
- FTC – “*False claims in spam*” (30 April 2003), available at: <http://www.ftc.gov/reports/spam/030429spamreport.pdf>
- ICC- “*ICC Guidelines on Marketing and Advertising using Electronic Media*” 2003, available at: http://www.iccwbo.org/home/statements_rules/rules/2004/Guidelines-on-Marketing-and-Advertising-using-Electronic-Media.asp
- ICC- “*ICC policy statement on 'spam' and unsolicited commercial electronic messages*” 2004, available at http://www.camara-e.net/_upload%5C373-22_114_spam1.pdf
- ITU- Cristina Bueti: “ITU Survey on anti-spam legislation worldwide” (July 2005), available at: http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_ITU_Bueti_Survey.pdf.
- ITU- Derek E.Bambauer et.al: “A comparative analysis of spam laws: the quest for a model law” (July 2005), available at: http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Comparative_Analysis_of_Spam_Laws.pdf.
- ITU- Matthew B. Prince: “*Countering spam: how to craft an effective anti-spam law*” (2004), available at: http://www.itu.int/osg/spu/spam/contributions/Background%20Paper_How%20to%20craft%20and%20effective%20anti-spam%20law.pdf.
- Nucleus Research Report: “SPAM-The serial ROI killer” (2004), available at: <http://www.nucleusresearch.com/research/e50.pdf>.
- OECD- “*Anti-Spam Law Enforcement Report*” (May 2005), available at: <http://www.oecd.org/dataoecd/18/43/34886680.pdf>
- OECD- “*Background paper for the OECD workshop on spam*”, DSTI/ICCP (2003)10/FINAL, available at: [http://www.oilis.oecd.org/oilis/2003doc.nsf/43bb6130e5e86e5fc12569fa005d004c/edfc2255d6a8a51ac1256e240030f5b6/\\$FILE/JT00157096.PDF](http://www.oilis.oecd.org/oilis/2003doc.nsf/43bb6130e5e86e5fc12569fa005d004c/edfc2255d6a8a51ac1256e240030f5b6/$FILE/JT00157096.PDF).

“Operation ‘Boite a Spams’: Les Enseignements et les actions de la CNIL en matiere de communications electroniques non sollicitées” 24 octobre 2002.

UK Code of practice for direct marketing (3rd edition), available at www.dma.org.uk.

UK Information Commissioner: “The ‘Durant’ Case and its impact on the interpretation of the Data Protection Act 1998”, available at: <http://www.informationcommissioner.gov.uk/cms/DocumentUploads/webversion%204%2004.10.042.pdf>

UK Information Commissioner: “*Guidance to the Privacy and Electronic Communications (EC Directive) Regulations 2003*”, available at: <http://www.informationcommissioner.gov.uk/cms/DocumentUploads/Electronic%20Communications%20Part%201%20Version%203.pdf> .

WSIS- “*Background Report of the Working Group on Internet Governance*” (June 2005), available at: <http://www.wgig.org/docs/BackgroundReport.doc>.

WSIS- “*Internet Governance: Quo Vadis? A Response to the WGIG Report*” (July 2005) (J. Mathiason & M. Mueller), available at: <http://dcc.syr.edu/miscarticles/IGP-quovadis.pdf>

WSIS- “*Report of the Working Group on Internet Governance*”, Château de Bossey, June 2005, available at: <http://www.wgig.org/docs/WGIGREPORT.pdf>

Union Francaise du Marketing Direct: “Code relatif à l’utilisation de coordonnées électroniques à des fins de prospection directe” (2005), available at: http://www.fevad.com/fr/gre_page/affiche_page.asp?categorie=7&id_page=150

ABBREVIATIONS:

CNSA- Contact Network of Spam Authorities

DPWP- Article 29 Data Protection Working Party

EASA- European Advertising Standards Alliance

FEDMA- Federation of European Direct Marketing Association

FTC- Federal Trade Commission

ICC- International Chamber of Commerce

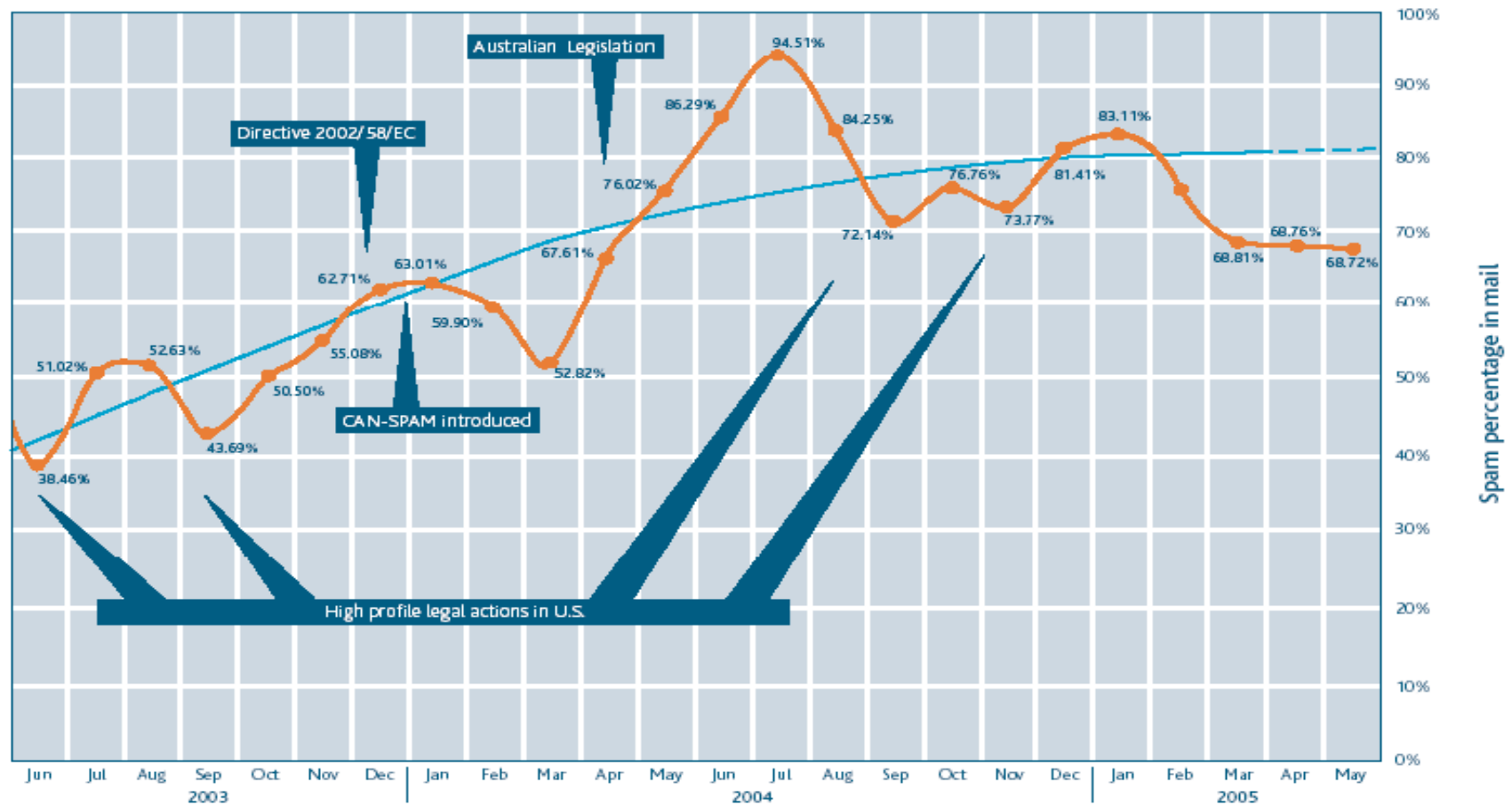
OECD- Organization for Economic Co-operation and Development

OJ- Official Journal of the European Communities

WGIG- Working Group on Internet Governance

WSIS- World Summit on the Information Society




Op.cit.- “*opus citatum*”, the work quoted.



Source: MessageLabs , taken from the “ITU SURVEY ON ANTI-SPAM LEGISLATION WORLDWIDE 2005, available at http://www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf”

Annex 1 Percentage of worldwide internet e-mail identified as spam

Annex 2 E-mail spam examples:

Date:	Sat, 16 Jul 2005 00:56:26 +0500
From:	 "Lynn Willis" <bthnnggvsejagb@yahoo.com>  Add to Address Book
To:	 dancointl@yahoo.com
Subject:	Re [11]:

DEAR CUSTOMER!

NEW BRAND SOFTWARE **RELEASES** IN OUR SHOP!
AS USUAL: **BEST PRICES** ON THE MARKET – JUST FOR YOU!

Just some examples:






Adobe PhotoShop 9.0 CS2 (1 cd) TOP!	\$45
Microsoft Windows XP Professional with SP2 (1 cd) TOP!	\$50
Corel Draw 12 Graphic Suite (3 cds) TOP!	\$65
AutoCAD 2006 (1 cd) TOP!	\$40
Microsoft Office 2003 System Professional with SP1 (5 cds) TOP!	\$55
DVDXCopy Platinum 4.0.38 for	\$20
Roxio Easy Media Creator 7.0 for	\$20

+ 1000s positions in categories:

- Audio (Music)
- Internet
- Games
- Business
- IS/IT
- Mobile, Palm, Pocket
- Design, Photo, Flash, Media, Illustration
- Web Developer
- Software Developer
- Utilities, Drivers, Antivirus, Security
- Desktop Enhancements
- Home & Education
- 3D Studio, Adobe, Maya... Plugins
- Video
- CAD/CAM
- Macintosh software

[CLICK HERE TO VISIT OUR SHOP](#)

Example 1: False header information

Date:	Mon, 04 Jul 2005 07:24:41 -0500
From:	"Steve Dauman P.manager" <seabird@infinito.it>  Add to Address Book
To:	 dancohen58@yahoo.com
CC:	 dancohn1@yahoo.com,  dancoi2000@yahoo.com,  dancointl@yahoo.com, dancoj2000@yahoo.com
Subject:	The unique possibility to increase your income. Protection code:GE-4177

You are invited to work in world-wide enterprise.

Would You Rather Have
Financial independence or Time Freedom?

How about both?

Everyday People Living Extraordinary Lives Their
Very First Year!
Your success will be achieved with personal
mentoring by a group of
individuals that have already achieved a multiple
six-figure income. The
system that is in place works perfectly. If you
are not satisfied with
unfairly low salary and ready to earn much more,
YOU have come to the RIGHT
place. ANYONE that is coachable and trainable
will succeed. This opportunity
requires no personal selling or explaining. Here
are just a few of YOUR
benefits.
--[...]

Example 2 : One form of dictionary attack

Box 7.1: The ten worst spam countries as at 21 June 2005

Top 10 Worst Spam Countries		Number of Current Listed Spam Issues
1	United States	2470
2	China	399
3	South Korea	288
4	Russia	191
5	Taiwan	171
6	Japan	136
7	Canada	135
8	Brazil	117
9	Argentina	95
10	Hong Kong	93

Many critics have been raised to the opt-in approach and one year after the passage of a national anti-spam law in the United States, known as the CAN-SPAM Act, only a low percentage of spam messages complied with its requirements in fact according to Spamhouse the United States continues to be the world's worst spam country, accounting for 2470 number of current listed spam issues.

Source: Spamhouse

Source: MessageLabs , taken from the “ITU SURVEY ON ANTI-SPAM LEGISLATION WORLDWIDE 2005, available at http://www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf”

Annex 3 Top ten spam countries

TABLE OF CONTENTS

INTRODUCTION.....	1
1. Spamming as an advertising practice.....	6
1.1 The role of personal information in the advertising practice today.....	7
1.1.1 Personal data as an asset.....	8
1.1.2 Personal data as commodity.....	11
1.2 E-mail address as personal data	13
1.3 E-mail marketing and spam practices.....	18
2. Values and interests involved in spam practices.....	23
2.1 Different interests that need to be safeguarded by the anti-spam legal provisions	23
2.2 Unsolicited commercial communications- a concern for individual privacy?	27
2.3 Privacy and economic interest –anti-spam initiatives between two focal points of interest.....	30

3. Anti-spam legislation: a balance of interests.....	34
3.1 The response to “unsolicited commercial communications” in the e-commerce legislation	34
3.2 The data protection legislative response to spam practices.....	43
3.2.1 Principles and rules regarding the collection of e-mail addresses for direct marketing purposes.....	43
2.3.1.1 Collection of e-mail addresses belonging to natural persons...	43
2.3.1.2 Collection of e-mail addresses belonging to legal persons.....	46
3.2.2 Principles and rules regarding the use of personal data for direct marketing purposes.....	49
3.2.3 Principles and rules regarding the transfer of personal data to third parties for direct marketing purposes.....	52
3.3. The efficiency of the anti-spam solution provided by the European legislator.....	55
3.3.1 Different mechanisms – one solution?	55
3.3.2 Fitness for the purpose.....	62
3.3.3 Negative consequences?	65
3.4 Other legislative solutions.....	67
 CONCLUSIONS.....	 71
SELECTIVE BIBLIOGRAPHY	75
ABBREVIATION LIST	
Annex 1.....	I
Annex 2.....	II
Annex 3.....	IV