Commission of the European Communities

Unsolicited Commercial Communications and Data Protection

(Internal Market DG – Contract n° ETD/99/B5-3000/E/96)

Authors (ARETE): *Serge Gauthronet*
Etienne Drouard

January 2001

Table of contents

Introduction

Within the last four years, the European Parliament and the Council have adopted two major directives establishing a high level of privacy safeguards in relation to the electronic processing of personal data: Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data and Directive 97/66/EC concerning the processing of personal data and the protection of privacy in the telecommunications sector. The Member States are currently completing the transposition of these directives into national law. However, with the rise of the Internet and electronic commerce, there is a growing concern in our modern society over the unlimited harvesting and uncontrolled trading of personal data, the creation of vast databases of personal profiles, aggressive advertising, increasing use of unfair practices and serious breaches of privacy.

The Commission has been looking at these issues for a number of years and has now commissioned ARETE to report specifically on the phenomenon of unsolicited commercial e-mail, also known as "spam".

There are at present some **569 million electronic mailboxes** worldwide, 153 million of them in Europe (1), or an average of 1.8 mailboxes per Internet user. Every day these inboxes are inundated with hundreds of million of commercial messages, underlining the fact that e-mail is not only a means of interpersonal communication but also a powerful and cost effective **business tool**. Like advertising and direct marketing, both mass-oriented and one-to-one, many of these messages have not been solicited by their recipients. Thus a whole new sector has developed on the basis of a sophisticated technology, a set of clever techniques for collecting e-mail addresses and a comparatively inexpensive cost structure.

In the terms of reference given to ARETE by the Commission, the first task is to analyse this activity of e-mail marketing and spam. This analysis is the subject of the first part of the study .

This part is divided into two chapters: the first is devoted to an analysis of the general situation and the history of the phenomenon in the US. One of the findings of this chapter is that spam is in a sense a teething trouble of e-mail marketing: now, led by the online industry and the gurus of modern marketing, the

1) Source: Messaging Online - March 2000.

consent-based approach is beginning to supplant the more cavalier forms of unsolicited commercial communication.

The second chapter analyses the world of spam and e-mail marketing. It contains a detailed discussion of spamware – software packages that can be used to harvest e-mail addresses in the Internet's public areas – and the legal and financial risks now facing those who use them. It includes an in-depth study of the new model which is set to dominate the marketing industry and which is based on the concepts of permission and opt-in. The implementation of this model is discussed by reference to a number of market-leading American companies which were analysed in the US or in Europe specifically for the purposes of this study. The chapter ends with a discussion of what opt-in really means.

The second part of the study first surveys the legislative, administrative, regulatory, judicial, doctrinal and ethical backdrop against which the phenomenon of unsolicited e-mail marketing is developing or is being shaped in the Member States of the European Union in the current state of Community law. This is followed by a discussion of the similarities and differences between the various national approaches, both public and private. Finally, on the basis of the preceding analysis the conclusions and recommendations are set out as to the legal framework which can best provide legal certainty for Europe's e-commerce industry while protecting the recognised rights of Europe's web surfers.

This part of the study was initially restricted to four Member States but was subsequently extended to all fifteen.

The working method initially adopted when the scope of this study was being defined was to examine in detail the situation in four Member States (Italy, UK, Germany and France). These were chosen because of their large numbers of web surfers and servers online, the contrasts between them, their perceived active involvement in the issue and because some of them had long-standing and some recent data protection laws, which in the latter case might make it easier to introduce legislation specific to electronic marketing.

The initial inquiries carried out in all the Member States in relation to data privacy legislation in general and unsolicited commercial e-mail in particular quickly revealed that the national situations were not those originally expected and that a study confined to four countries would not provide a complete picture of the differences or similarities existing in Europe.

It soon became apparent that the only way of providing a reliable account of the situation in Europe was to conduct an exhaustive study of the legal framework and industry practices in each of the fifteen Member States. This method entailed surveying some 170 public agencies and industry representatives (2) throughout the entire Community, as well as interviewing particular e-commerce merchants where specific national circumstances so required. This operation was carried out between the end of 1999 and the summer of 2000.

2) For a complete list of those consulted see Annex 2 - page 147.

The second part of this report is divided into 5 chapters. Chapters III and IV consider the apparently low incidence of unsolicited commercial e-mail in Europe, as evidenced by the responses to the survey, analyse the work of the national data protection authorities and look at industry practices and the attitude of the courts in the Member States.

Next, the study focuses on the confusion within the industry as to both the meaning of some key expressions and the scope of the relevant directives (Chapter V). In Chapter VI, finally, the authors argue that a clarification of the Community legislation is necessary in the wake of the adoption of Directive 2000/31/EC of 8 June 2000 on electronic commerce and that the balance must be redressed in favour of the protection of Europe's web surfers. Directive 2000/31/EC, in failing to re-affirm explicitly the rules governing collection of e-mail addresses by online merchants, has engendered widespread confusion that benefits nobody. This confusion must be dispelled in order to give Europe the legal certainty necessary for e-commerce to flourish, while respecting individual rights and the applicable laws.

We would like to express our sincere thanks to all those who contributed for their time and helpfulness.

Part One:
E-mail marketing and spamming: general situation, practices and services offered

Chapter I: E-mail marketing and unsolicited commercial communication: general situation

Interactive marketing has found an obvious growth medium in the Internet evidenced, as the first part of this chapter will seek to show, by the shift in advertiser's spending patterns in the United States. It was only to be expected, however, in the early years of this market that the ease with which e-mail addresses could be collected for nothing and the low overall cost of operating would attract unprofessional operators who cared nothing for the Internet's etiquette and the privacy of its users. Thus the second half of the 90s was marked by an explosion in the phenomenon known by that ugly word "spam". This chapter examines the origins of the phenomenon and how gradually the Internet community, led by the network administrators and access providers, succeeded in containing if not overcoming it. It also examines how US legislators gradually responded to pressure from privacy advocates to enact anti-spam legislation. Lastly, it looks at the current theory of e-marketing as seen through the eyes of the legitimate e-marketing industry.

I.1) - Some economic data on the Internet, marketing and commercial communications

Overall, direct marketing now accounts for the lion's share of commercial communications. The statistics show that it has overtaken traditional advertising: according to the DMA (Direct Marketing Association), direct marketing expenditure in the US in 1999 came to $176 billion, or 57% of total spending on commercial communications ($308.9 billion), and is forecast to reach $221.5 billion in 2003. The following table shows a breakdown of this figure by medium (note that direct marketing in print media, radio and television refers to advertising campaigns using coupons or toll-free telephone numbers to generate business or attract consumers to retail outlets).

Spending on direct marketing compared to overall advertising spending in the US market (source: Direct Marketing Association)			
(US $billion)	**Direct marketing expenditure**	**Total of advertising and direct marketing expenditure**	**% of total spent on direct marketing**
1994			
Direct mail	29.6	29.6	100.0
Telephone marketing	46.8	76.8	60.9
Newspapers	12.2	34.4	35.6
Magazines	6.2	11.5	53.7
Television	12.9	35.4	36.5
Radio	3.8	10.5	36.5
Other media	9.7	20.4	47.5
Total	**$121.3**	**$218.7**	**55.5%**
1999			
Direct mail	42.2	42.2	100.0
Telephone marketing	66.9	110.5	60.5
Newspapers	17.4	47.0	37.1
Magazines	8.9	15.9	56.3
Television	20.4	51.4	39.6
Radio	6.5	15.5	42.0
Other media	14.2	26.4	53.7
Total	**$176.5**	**$308.9**	**57.1%**

Spending by advertisers in 1999 in the Other Media category, which essentially means online networks and services, came to a total of over $26 billion, of which the greater part, $14.2 billion, was spent on direct marketing campaigns rather than advertising.

Within this spending category, interactive direct marketing accounted for a total of $1.3 billion in 1999. This figure is still relatively low but the DMA is forecasting very high growth rates through to the year 2004 when it is expected to reach $8.6 billion. The table below shows a breakdown of the figures as between business-to-business and business-to-consumer

marketing. It reveals exceptionally high growth rates over the last 5 years, entirely in keeping with the phenomenal upsurge of the net economy.

Growth in direct marketing expenditure on interactive media in the US

(source: Direct Marketing Association)

(in US$ million)	1994	1998	1999	2000	2004	94-99
Total	**$11.0**	**$742.0**	**$1,311.0**	**$2,135.0**	**$8,614.0**	**160.2%**
Business-to-business	7.5	469.7	824.6	1,338.6	5,418.2	156.0%
Consumer	3.5	272.3	486.4	796.4	3,195.8	168.3%

All the signs are that over the next few years we will witness a growing shift in expenditure in the direction of direct marketing over the Internet and e-mail marketing in particular. There are three main reasons for this: the first is the fact that the cost of mounting an advertising campaign on the Internet represents a fraction of the cost using traditional media: the average unit price for an e-mail marketing campaign in the United States is about 10 cents compared to a cost of between 50 cents and $1 for a direct mail campaign. The second reason is that sales conversion ratios for e-mail marketing are 5 - 15% as compared to 0.5 - 2% for conventional mailings (3). Lastly, there is competition too between the different methods of advertising on the Internet and it is highly likely that advertisers will opt increasingly for e-mail marketing at the expense of banner advertising: several studies show a significant differential in response rates between e-mail marketing, which achieves click-through rates (4) in the region of 18%, and banner advertising, where rates have fallen steadily before levelling off at 0.65%, according to Forrester Research (5);other sources (Nielsen Netratings – March 2000) report a drop from 2.5%, in the mid-90s, to 0.36% in March 2000.

---

3) Source: Forrester Research.

4) In the jargon of online marketing, a click-through occurs when a user clicks on a hyperlink to be taken directly to the advertiser's website and details of the advertised product. When the user actually makes a purchase this is called a click-order.

5) Source: Forrester Research – March 1999. These figures are confirmed in a recent article: **Saul Hansell**: "*So Far Big Brother Isn't Big Business* "– The New York Times On the Web – May 7, 2000.

I.2) - Spam: the teething trouble of e-mail marketing

Over the last five or six years, e-mail marketing has been characterised by some rather crude practices, almost as basic as stuffing brochures into letter-boxes or under the windscreen-wipers of parked cars. This is what is known as spam. According to the definition given in a recent report by the CNIL, spam "(...) is the bulk-mailing, sometimes repeatedly, of unsolicited e-mail messages, usually of a commercial nature, to individuals with whom the mailer has had no previous contact and whose e-mail addresses the mailer collected from the public spaces of the Internet: newsgroups, mailing lists, directories, web sites etc." (6). Spam has gone through a number of stages, but thanks to a powerful backlash by Internet activists opposed to the commercialisation of the Internet, pressure from privacy advocates and action by legislators, it is now in retreat or at least evolving into less unacceptable forms.

I.2.1) - The three ages of spam

It is likely that spam, like many other Internet phenomena, will turn out to have had a short life-cycle, of 4 to 5 years, during which things moved very fast. Two US authors, Alan Schwartz, a university professor, and Simson Garfinkel, an IT consultant, provide a good account of the rise and fall of spam (7). In broad outline, there are three major milestones in this short history.

- April 1994: Canter & Siegel and the Green Card Lottery spam

  Laurence Canter and Martha Siegel are two Arizona lawyers who thought up a scheme to offer advice to anybody wishing to take part in the Green Card Lottery. This is a special procedure organised by the US government agency in charge of issuing immigration visas; all those eligible i.e. men and women from any continent having completed secondary education or having at least 2 years work experience during the previous 5 years are invited to lodge a visa application form with the United States National Visa Center in Portsmouth, New Hampshire. These applications, which greatly outnumber the annual quota of visas issued (between 4 and 5 million applications on average for 50,000 visas), are then processed by computer and drawn by lots. Lodging a Green Card application is free of charge. In view of the fact that between 30 and 40% of applications are normally rejected as invalid, many law

---

6) **Commission Nationale de l'Informatique et des Libertés**: *"Le publipostage électronique et la protection des données personnelles"* - Report presented by Madame Cécile Alvergnat and adopted on 14 October 1999.

7) **Alan Schwartz & Simson Garfinkel**: *"Stopping Spam – Stamping out Unwanted E-mail & News Posting"* - O'Reilly – Oct. 1998.

firms provide an advisory service and guarantee clients that they will be included in the lottery. One such firm, Canter & Siegel, posted an advertisement on over 6,000 Usenet newsgroups in April 1994 offering to help applicants complete the forms for a fee of $100. Unwittingly, Canter & Siegel had just invented what would later be termed EMP (Excessive Multi-posting) (8). Tens of thousands of individuals who received the message protested by bombarding the senders with reply e-mails. The senders' ISP was unable to handle the volume of protest responses and ended up terminating their account. After a number of attempts to resume their activity using other access providers, Canter & Siegel decided to spawn some imitators by publishing "*How to Make a Fortune on the Information Superhighway*", in which they explain how to collect addresses from newsgroups and how to inundate mailboxes with advertising messages. Canter & Siegel spammed the newsgroups for the last time in March 1995, apparently to promote their book.

- July 1995: Jeff Slaton, the "Spam King"

Jeff Slaton, a sales executive based in Albuquerque who sold advertising space in the yellow pages directory of US West, got the idea – apparently after reading Canter & Siegel's book – of sending bulk e-mails to science newsgroups. By way of example, in one of these he claimed to be in contact with a researcher recently retired from the laboratories in Los Alamos (New Mexico) and as a result to be able to offer the plans for the atom bomb for the bargain price of $18, postage not included. Jeff Slaton later recounted having sold thousands of these plans all around the world. Heartened by this experience, Jeff Slaton shortly afterwards began offering his services as a spammer, charging $495 per campaign. Hundreds of small-time advertisers – at the rate of 15 a week it is claimed – took up the offer, some of them to promote schemes or services which are subject to strict regulation or even prohibition, such as pyramid-selling scams (9). Jeff Slaton is a true pioneer: it was he who invented the fake e-mail address and the forged domain name to avoid detection; he was also quick to grasp the need to give spam recipients a means of contacting him and he was careful to include telephone numbers (voicemail) in his adver-

8) So called because a single advertisement is transmitted and stored as many times as the number of Usenet Groups to which it is addressed.

9) Pyramid selling is a product distribution technique in which those taking part earn income by selling the products to other recruits who, in turn, earn income by selling to others, and so on. It is a form of what is known as multi-level marketing, which is based on various unscrupulous sales practices such as: the payment of a sum of money in return for the right to be paid for recruiting new participants; the purchase of a stock of particular products as a precondition for taking part; the sale to participants of unreasonable quantities of product; no means for participants to return the products on fair terms. Because of all this, pyramid selling is banned in many countries.

tising messages. He even offered an unsubscribe option. In fact it appears that no opt-out list ever actually existed, although Slaton tried, at the end of 1995, to market a full-blown opt-out service for $5 per registration. A guerrilla war ensued between Slaton and the defenders of the Net, mostly students, which led to the publication on specialist newsgroups (10), dedicated web sites (11) and the first of the blacklists (Black-Hole List) (12) of Slaton's home telephone number, his age, a photograph of him, his address, his social security number, his direct line at work and even the direct line of his boss at US West.

- 1996: Sanford Wallace and Cyber Promotions, Inc.

Sanford Wallace, the owner of Cyber Promotions, a Philadelphia-based company, took spam into the industrial age by leasing his own T1 connection and operating under his own domain name (cyberpromo.com). From the outset, Cyber Promotions' prime targets were AOL members, whose e-mail addresses it collected in bulk using a harvesting tool it had developed itself. Everyone on its list received between two and five spams a day, all of a similarly dubious nature such as get-rich-quick schemes or weight-loss methods. At its peak, Cyber Promotions was sending a total of up to 30 million e-mails per day. Like Slaton, Wallace mounted these campaigns on behalf of advertisers who were not terribly bothered about the methods used. AOL responded by developing its own defence system which systematically blocked all messages originating from the three different addresses of Cyber Promotions. Wallace then sued AOL claiming violation of his right of free speech under the First Amendment to the United States Constitution. The court proceedings continued until 1997. Eventually Wallace lost the case on appeal. A few weeks later, Cyber Promotions was back in court, this time as defendant, in a lawsuit brought by three online service providers, CompuServe, Prodigy and Concentric Network. Compuserve alleged fraud and trademark infringement by Cyber Promotions consisting in using the domain names of the three service providers in the return addresses for its spams ("From:"). This was a technique used by Wallace to get past the anti-spam filters put in place by AOL. Cyber Promotions signed agreements with the plaintiffs undertaking to cease the practices complained of. While this was going on, however, Wallace had already thought up a new way of spamming AOL's membership – by leasing several T1 connections from different access providers for $1,000 a month.

---

10) news.admin.net-abuse, news.admin.net-abuse.bulletins, news.admin.net-abuse.policy, news.admin.net-abuse.sightings, news.admin.net-abuse.e-mail, news.admin.net-abuse.usenet.
11) http://com.primenet.com/spamking/
12) The Realtime Blackhole List at the Mail Abuse Protection System, http://maps.vix.com – Cf. pages 18 & 19

At the beginning of 1997, Cyber Promotions registered a new domain name, cheekily called spamford.com. By now the company had 7 employees. However, it was finding it increasingly difficult to find a compliant ISP, for the very good reason that Wallace had become the Internet's public enemy number one and any ISP doing business with him would have been taking a commercial risk. AGIS (Apex Global Information Services), a Michigan ISP, terminated the Cyber Promotions account in August 1997 (13). Two months previously, WorldCom had done likewise. In March 1998, a lawsuit filed by another ISP (EarthLink Network Inc.) spelled the end of Sanford Wallace's spamming career: he was forced to agree a $2 million settlement for having spammed EarthLink's subscribers. The poacher has since turned gamekeeper and Wallace now operates a spam consultancy service. Among his clients is the Atlanta law firm (Hunton & Williams) which acted for Earthlink in the case that put him out of business. According to Wallace "(...)Spam is no longer going to work, spammers of today are almost exclusively hiding behind forgery and using the resources of others. People on the Internet are not going to stand for it. I will give back to the Internet by spending time and effort to help clean up the streets" (14).

I.2.2) - The factors against spam

It is safe to say that spam phenomenon as it existed in the US in the mid-1990s is now in decline. This is borne out by the various blacklists posted on the Internet which reveal that the phenomenon had its heyday between 1995 and 1998. Since then the number of blacklist entries has been falling, thanks in particular to the fact that the ISPs have acquired more control over traffic passing through their mail and news servers. One database, for example, Spamhaus.org, which is updated on a daily basis, currently lists 68 marketing agencies still spamming on the Internet or on Usenet compared to the 168 which have vanished from the scene over the last two or three years.

There are two factors which have a quasi-mechanical effect on the spam phenomenon: the combative stance taken by the ISP community on the Internet and on Usenet and the enactment of anti-spam legislation by an increasing number of US states and perhaps in the near future at Federal level also.

---

13) AGIS began business in 1994. It is one of the oldest Internet backbone providers. The company has been notable for its willingness to do business with spammers and is something of an Internet pariah as a result. This may explain why it failed to complete a second round of financing and has been in Chapter 11 protection since February last.

14) Cf. **Deborah Scoblionkov**: "*Spam King Forges Unholy Alliance*" - Wired – 11 May 98

➢ The Mail Abuse Prevention System and the Realtime Blackhole List (RBL)

Nowadays, the vast majority of ISPs hound the spammers remorselessly. One of their responses to spam has been to organise a network of voluntary administrators (founded by Paul Vixie, a militant anti-spam activist) known as The Mail Abuse Prevention System (MAPS – Redwood City, Calif.) which operates the Realtime Blackhole List (RBL). This list is an instrument of mass boycott used by the ISPs' system administrators – who together control thousands of routers and mail servers – to share information on spam attacks and to ostracise IP addresses and domain names that are known sources of UCE. The details of every spammer whose account is terminated by an ISP are posted to the list so that the 2,000 other ISPs around the world who subscribe to the RBL – about 1/3 of all ISPs – can refuse to provide service if approached by that spammer. This is a basic information-pooling system of the sort that is widely used in the information society to keep ahead of fraudsters. But the MAPS system also acts as a filter which uses algorithms (15) to automatically block messages from known spammers – and from their ISPs, which are deemed to have failed in their duty to the online community as a whole to help keep the network free of junk. Thus AOL, MSN and Real Networks have all at one time or another found themselves in the RBL. The problem is that, being an automatic filter and now a very powerful one, the MAPS system, sometimes gets it wrong, with the result that some innocent ISPs operating genuine anti-spam policies end up on the RBL. Moreover, the suspension of an ISP has the effect of blocking the entire mail server, thereby preventing bona fide users from accessing it. Such cases are frequently reported in the press and the MAPS community is sometimes accused of McCarthyism and of acting like a vigilante group whose only legitimacy derives from the growing number of its members. The fact of the matter is that fewer and fewer ISPs are going to run the risk of winding up blacklisted in the RBL for having hosted or even allowed through a spamming operation. John Mozena, founder of CAUCE (of which MAPS is a member), agrees, albeit with a qualification: "(...) It's not a solution to spam, but it is a valuable tool - both in technical and public relations terms - for domains that want to protect themselves against spam. **No one wants to be stigmatized by being on the RBL list**" (16).

---

15) Matching algorithms which construct a DNS tree diagram consisting of the IP addresses of domains hosting or relaying spam. If a connection comes from a machine with the address a.b.c.d, the software will check if the ressource record d.c.b.a.rbl.maps.vix.com exists in the DNS.

16) **Jon Swartz**: *"Anti-Spam Service or McCarthyism? - Internet group puts some ISPs On a blacklist"* - Monday, May 10, 1999 - ©2000 San Francisco Chronicle.

- The Usenet Death Penalty (UDP)

  Usenet is a group of computers linked to different networks, including the Internet, which carries articles posted to newsgroups. It is governed by unwritten rules of cooperation between the administrators. The articles posted must comply with a standard transmission format (RFC-1036) which is accepted by all the networks. By extension, "Usenet" also means the community of individuals who read and write articles in newsgroups. Usenet has long been the favourite hunting-ground of the spammers who use it both to harvest e-mail addresses and to inundate the newsgroups with spam, often of an unsavoury nature (pornography, MMF – Make Money Fast, pyramid schemes, terrorism). The Usenet Death Penalty is a "death sentence" issued against the authors of such messages who ignore complaints by other users and warnings by Usenet administrators. The main driving force behind the system is Ken Lucke, the creator of stopspam.org. The UDP is activated after a probation period of 5 business days and has the effect of deleting all messages posted by the site in question. Online service providers such as CompuServe and UUNET received the UDP in 1997, while Netcom was threatened with it in 1998. 1997 was probably the worst year for spam on Usenet with an estimated 60% of all messages posted being deleted. Like the RBL, the UDP does not operate with surgical precision. Technically speaking, it is a filter and it makes no exceptions: all messages originating from a blacklisted site or ISP are systematically deleted without being delivered. It gives ISPs a very strong incentive to be vigilant themselves and not to harbour spam or offensive content.

- The regulatory response in the US

  There is as yet no federal legislation explicitly outlawing UCE. Seven anti-spam bills were introduced in 1997 and 1998 and the following table summarises their main provisions. All seven bills fell during the105th session of Congress:

Federal Bills pending in 1998
(Sources: The John Marshall Law School – **1998/07/17)** (17)

Bill no./ sponsor	Introduced	Status	Prohibit unsolicited e-mail	Enforce ISPs' policies	Universal exclusion list	Honor opt-out requests	Sender ID/false headers	Require labels
H.R. 1748 (C. Smith)	5/22/98	pending in House	prohibit UCE	no	No	no	Yes	no
H.R. 2368 (Tauzin)	7/31/97	pending in House	no	no	no	no	no	no
H.R. 4124 (Cook)	6/24/98	pending in House	no	yes	possibly[1]	yes	yes	no
H.R. 4176 (Markey)	6/25/98	pending in House	no	sender's ISP only	yes	yes	yes	no
S. 771 (Murkowski)	5/21/97	pending in Senate	no	no	no	yes	yes	yes
S. 875 (Torricelli)	6/11/97	pending in Senate	no	possibly[1]	possibly[1]	yes	yes	no
S. 1618 (McCain) (amendments by Murkowski & Torricelli)	2/9/98 (amended 5/12/98)	passed Senate	no	no	no	yes	yes	no

[1] H.R. 4124 and S. 771 both refer to Internet standards not yet adopted, which could provide for a universal exclusion list or other method for individuals or ISPs to notify prospective senders of unsolicited e-mail of their preferences or policies.

Nine further bills were introduced during 1999:

- ⇨ *Can Spam Act* (June 1999)
- ⇨ *E-Mail User Protection Act* (May 1999)
- ⇨ *Inbox Privacy Act of 1999* (March 1999)
- ⇨ *Internet Freedom Act* (May 1999)
- ⇨ *Internet Growth and Development Act of 1999* (May 1999)
- ⇨ *Netizens Protection Act of 1999* (October 1999)
- ⇨ *Protection Against Scams on Seniors Act of 1999* (February 1999)
- ⇨ *Telemarketing Fraud and Seniors Protection Act* (March 1999)
- ⇨ *Unsolicited Electronic Mail Act of 2000* (October 1999 and amended in March 2000)

None of these bills has been passed but there is a strong possibility that the most recent of them, the Unsolicited Electronic Mail Act of 2000, will soon become law. This is the bill which appears to be the most strongly in favour of strict spam controls. Broadly speaking, all the proposals contain three core provisions: prohibiting

17) Source: **The John Marshall Law School**, 315 S. Plymouth Court Chicago, Illinois 60604 – whose website can be found at: http://www.jmls.edu/cyber/statutes/e-mail/

false sender ID and unauthorised access and requiring opt-out systems to be put in place.

Without waiting for Congress to act, several US states have gone ahead and enacted anti-spam legislation. These statutes have already been used to bring a number of lawsuits against spammers. Many of them also apply to unsolicited faxes. The following table (18) summarises the first 15 anti-spam statutes enacted by US state legislatures. Since then, five other states have followed suit or are about to do so: Colorado (statute passed in February 2000), Hawaii (3 statutes pending, one already passed by the state senate), Maryland, Vermont and Wisconsin. In essence, these statutes require opt-out registries to be set up and opt-out requests to be honoured and they prohibit the intrinsic features of spam – the forging of addresses and the doctoring of message headers and subject lines. Some states require the inclusion in the header of a label indicating that the message is an advertisement (ADV) or concerns an adults-only website (ADLT). In one third of these statutes, spam is defined as the sending of messages to Internet users without an express prior request on their part. All of these statutes have shortcomings, no doubt, and they have been criticised by privacy advocates in particular for not going far enough and for offering little redress to the actual victims of spam.

However, what all these statutes have in common is a pragmatic approach based on stiff penalties for spammers: the average being $10 per message up to a maximum of $25,000 per day. Given the fact that these days spammers tend to be small-scale operators with limited financial resources, these penalties may represent a serious or even a massive deterrent. As a *Wired* reporter commented upon returning from a meeting of Internet sex industry experts held last August in San Francisco: "(...) Porn sites are beginning to learn that the potential gains of spamming don't outweigh the risk" (19).

---

18) Source: **David E. Sorkin**, Spam Laws, <http://www.spamlaws.com/>

19) **Craig Bicknell**: "*Sites for Hardcore Eyes*" Wired News - Aug. 12, 1999.

STATE	Date legislation was passed	Main provisions										Penalties	Remarks
		Opt-out	Honour remove request	False sender address	Use of third party domain name	Falsification of routing information	Clear identification of sender	Misleading subject line	Label	Prior relationship / Consent	ISP Policy		
CALIFORNIA	Sep-98	x	x		x				x	x	x	from $5,000 to $10,000 + prison sentence according to seriousness of case	Law applies to both e-mail and fax.
CONNECTICUT	Jun-99			x	x	x			x		x	from $2,500 upwards	General statute covering various types of wrongdoing (hacking, virus spreading etc.).
DELAWARE	Jul-99	x	x			x				x			
IDAHO	Apr-00	x	x	x	x	x	x					from $100 to $1,000 / bulk mail	
ILLINOIS	Jul-99				x	x		x				$10 / bulk mail - maximum $25,000 / day	
IOWA	Mayi-99	x	x	x	x	x	x			x		from $10 to $500 / bulk mail	
LOUISIANA	Jul-99			x	x	x					x		Quantitative definition of bulk mail (>1,000)
NEVADA	Jul-97	x	x	x			x			x			
NORTH CAROLINA	Jun-99			x		x					x	$10 / bulk mail up to a maximum of $25,000 / day	
OKLAHOMA	Jun-99			x	x	x						$10 / bulk mail up to a maximum de $25.000 / jour	
RHODE ISLAND	Jul-99	x	x	x	x	x				x	x	from $10 to $100 / bulk mail up to a maximum of $25,000 / day	Probably the most technical of the state statutes from a legal viewpoint
TENNESSEE	Jul-99	x	x				x		x		x		
VIRGINIA	Apr-00	x	x				x				x	$10 / bulk mail up to a maximum of $25,000 / day	
WASHINGTON	**Mar-98**			x	x	x		x					Refers to the Consumer Protection Act.
WEST VIRGINIA	**Mar-99**			x	x	x	x	x			x		Quantitative definition of bulk mail

I. 3) - From spamming to permission marketing

Meanwhile, more and more e-marketers and e-commerce merchants are starting to see the potential of permission marketing and discovering this new concept of advertising campaigns targeted at willing, consenting audiences. ***Opt-in e-mail marketing*** is the new talk of the trade and the direct marketing industry federations are beginning to embrace this new approach, albeit slowly.

I.3.1) - The theories of Seth Godin

The whole approach to marketing and advertising is going through a process of change with the advent of the theory of "permission marketing". Following on from Don Peppers and Martha Rogers and the concept of one-to-one marketing, the leading thinker behind this approach is Seth Godin, a computer scientist and marketing graduate who founded Yoyodyne Entertainment Inc., the first online marketing company in the US to take e-mail marketing seriously. Seth Godin sold Yoyodyne to Yahoo in 1998 for $30 million in shares and the job of vice-president in charge of direct marketing. The term "permission marketing" has been copyrighted by Yahoo.

In a recent book (20), Godin sets out a number of key ideas which are now summarised. With the average American today seeing an average of 3,000 advertisements a day, the market is completely saturated. The public's time and attention has been exhausted. Ironically, the more advertisers attempt to stand out from the crowd the more they succeed simply in creating apathy and confusion. This is what Seth Godin calls "interruption marketing", advertising which interrupts whatever people are doing – watching a film on television, reading a magazine, or simply walking down the street and seeing a passer-by wearing a "Banana Republic" T-shirt. Seth Godin warns advertisers that their mass advertising methods are not working and that they are wasting their money. He appeals to them to turn to permission-based direct marketing, in other words, to communicate with customers and prospects on a voluntary basis, slowly building from interest to trust: "(...) Take your time, build trust through frequency. Tell your story patiently to each consumer who is willing to participate in **the exchange**" (21). This process of "exchange" revolves around the communication of personal information: as trust is built up, the consumer is persuaded by custom-tailored, genuine offers (incentive marketing) to give permission for an ever-wider range of marketing activities: permission to collect more information on his lifestyle, hobbies and interests, per-

---

20) **Seth Godin**: *"Permission Marketing: Turning strangers into Friends, and Friends into Customers"* - Simon & Schuster – New York – 1999.
21) Ibid. p. 75

mission to be sent messages advertising new products or services, permission to receive loyalty points, miles, free samples, trial subscriptions, etc. (22). As this process takes its course, the stranger becomes first a contact, then a prospect, then one day a customer and finally a loyal customer. This is the culmination of the exchange and the stage which Godin calls the intravenous stage, meaning the kind of trust displayed by a patient on a drip to the medical team treating him.

To create a relationship of this kind requires time and frequency of contact while keeping costs to a acceptable level if possible. What medium other than the Internet offers the same scope for interaction and graduated development? What better permission basis is there than one based on voluntary registration in opt-in lists? Mailing costs are tiny, the results of test campaigns are virtually instantaneous, response rates are fifteen times higher than for other media, continuous contact can be maintained with prospects without over-stretching advertising or consumer relations budgets (provided the process can be sufficiently automated) and printing costs are nil. In the Internet, permission marketing has found the perfect medium in which to grow and flourish. On the other hand, Seth Godin is critical of advertisers and marketers who replicate on the Internet the only advertising model they know – interruption marketing – which at best takes the form of banner advertisements or pop-ups and, at worst – because it is coupled with shoplifter-type behaviour (sic) – takes the form of spam. Both these marketing methods are doomed to failure as all they do is increase the clutter. As for spam, it is clear that its days are numbered, now that it is shunned by the marketing industry itself as well as by the network operators and by a public which will never be inclined to enter into a relationship of trust with a spammer.

I.3.2) - Opt-in e-mail marketing: the difficult transition to a new professional standard

Most US advertising and direct marketing industry organisations now condemn UCE explicitly. Some are beginning to espouse permission-based marketing and opt-in e-mail, although not without a number of contradictions which will probably take time to resolve.

The AIM (Association for Interactive Media) is an independent subsidiary of the DMA, founded in 1993. Its raison d'être is to represent and defend the Internet industry in Washington and to promote consumer confidence. Its 350 members include some of the highest-profile website operators (including Yahoo!, Citibank, Internet Shopping Network, New York Times). At the meeting of its Council for Responsible E-mail in Seattle in February 2000, the AIM adopted a set of

22) Ibid. p. 47

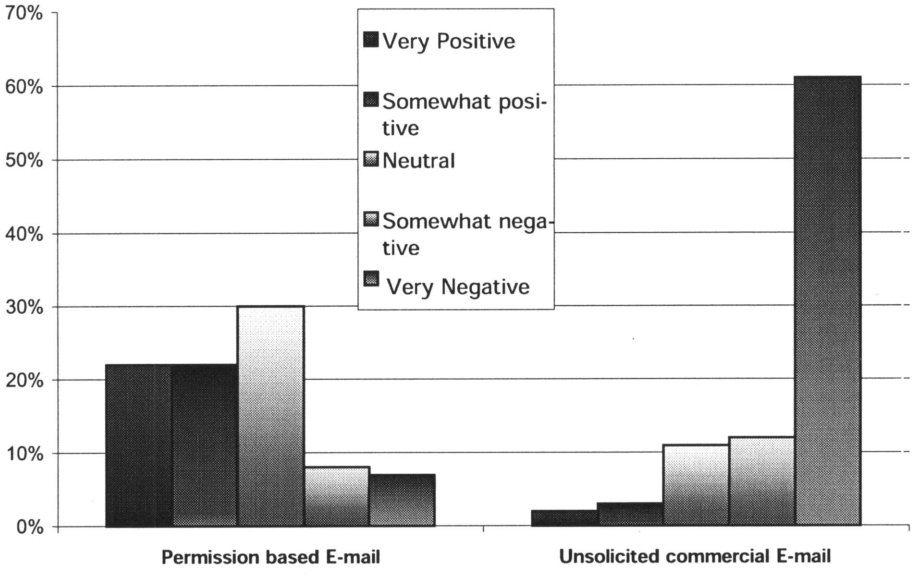
guidelines which are unequivocal on the subject of spam and which lay down the principle that there should be a prior business relationship with the addressees of a marketing campaign:

- ⇨ Commercial operators, that is, online marketers and retailers, must not falsify the sender's domain name or use an IP address without the prior agreement of the parties
- ⇨ Commercial operators must not falsify the subject line to deviate and mislead readers from the content of the e-mail message
- ⇨ All e-mail marketing messages must either include an option for the recipient to be removed from the database of the sender or intermediary and contact information of the sender or intermediary
- ⇨ Commercial operators must inform the respondent upon online collection of the e-mail address for what marketing purpose the respondent's e-mail address will be used. (Inform either online or via e-mail)
- ⇨ Commercial operators must not harvest e-mail addresses with the intent to send bulk unsolicited commercial e-mail without consumers' knowledge or consent
- ⇨ Bulk unsolicited commercial e-mail must not be sent to an e-mail address without a prior commercial relationship, which includes any previous correspondence, transaction activity, customer service activity or third party permission use.

The AIM has also published a strategic study on permission e-mail commissioned from the consultancy firm IMT (Integrating Marketing & Technology) (23). This study is based on interviews conducted with 400 e-mail users and 200 marketers. It highlights the difference in terms of attitudes and impact between UCE and permission marketing. Spam is not popular with the public, as is illustrated in the following chart:

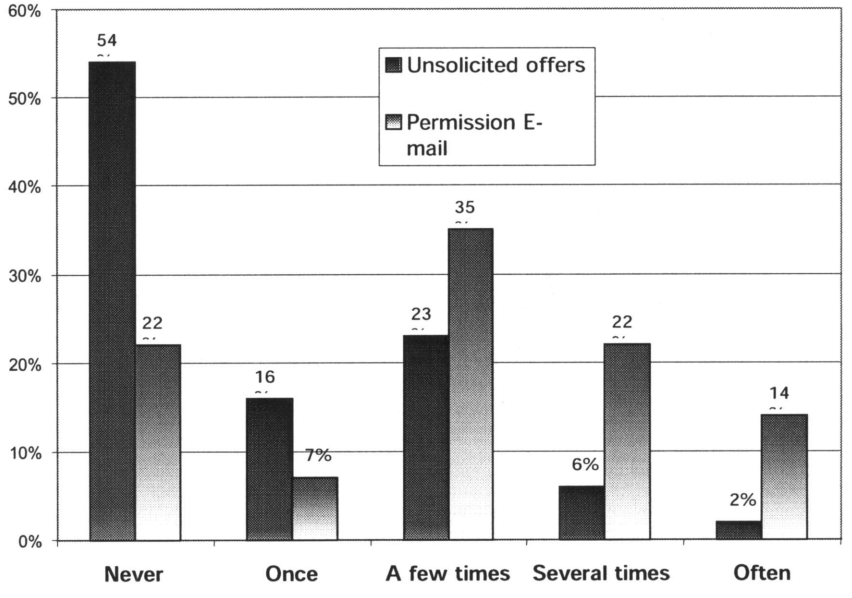
23) **IMT**: *"Permission E-mail: The Future of Direct Marketing"*. http://www.imtstrategies.com/aim_dma/index.html.

Attitudes about Commercial E-mail
Permission vs. UCE
Source : IMT Strategies 2000



Not surprisingly, consumers are vastly more responsive to permission e-mail. As the following graph shows, 70% of Internet users have clicked either a few times, several times or often on advertising messages sent by permission e-mail, compared to just 30% in the case of UCE.

Frequency of E-mail response



The NAI (Network Advertising Initiative) is a group representing various online marketing service providers, including the leading players (24/7 Media, AdKnowledge, DoubleClick, Flycast, Engage, Real Media etc.), and whose purpose, like that of the AIM, is to promote confidence in e-commerce. It has a clear policy – as stated most recently at the FTC hearings – requiring its members to inform Internet users prior to collection of personal data.

The DMA (The Direct Marketing Association) has for many years operated guidelines for ethical business practice in direct marketing and in particular in direct mailing. The main ones are shown on the following page. Naturally, these guidelines have had to be updated regularly to keep in step with advances in direct marketing techniques and to reflect changes in consumer law and the growing privacy awareness of US society. They were most recently revised (in August 1999) to incorporate new guidelines on e-mail marketing and in response to the Children Online Privacy Protection Act (COPPA).

Main DMA guidelines on direct marketing

(Source: DMA - The DMA Guidelines for Ethical Business Practice Revised August 1999)

- **HONESTY AND CLARITY OF OFFER:** All offers should be clear, honest and complete so that the consumer may know the exact nature of what is being offered, the price, the terms of payment (including all extra charges) and the commitment involved in the placing of an order.
- **ACCURACY AND CONSISTENCY**: Simple and consistent statements or representations of all the essential points of the offer should appear in the promotional material.
- **ACTUAL CONDITIONS**: All descriptions, promises and claims of limitation should be in accordance with actual conditions, situations and circumstances existing at the time of the promotion.
- **DISPARAGEMENT**: Disparagement of any person or group on grounds addressed by federal or state laws that prohibit discrimination is unacceptable.
- **DECENCY**: Solicitations should not be sent to consumers who have indicated to the marketer that they consider those solicitations to be vulgar, immoral, profane, pornographic or offensive in any way and who do not want to receive them.
- **DISCLOSURE OF SPONSOR AND INTENT**: All marketing contacts should disclose the name of the sponsor and each purpose of the contact. No one should make offers or solicitations in the guise of one purpose when the intent is a different purpose.
- **ACCESSIBILITY**: Every offer and shipment should clearly identify the marketer's name and postal address or telephone number, or both, at which the consumer may obtain service. If an offer is made online, an e-mail address should also be identified.
- **MARKETING TO CHILDREN**: Offers and the manner in which they are presented that are suitable for adults only should not be made to children. In determining the suitability of a communication with children online or in any other medium, marketers should address the age range, knowledge, sophistication and maturity of their intended audience. Marketers should not collect personally identifiable information online from a child under 13 without prior parental consent or direct parental notification of the nature and intended use of such information online and an opportunity for the parent to prevent such use and participation in the activity.
- **USE OF THE WORD "FREE" AND OTHER SIMILAR REPRESENTATIONS**: A product or service that is offered without cost or obligation to the recipient may be unqualifiedly described as "free."
- **PRICE COMPARISONS**: Price comparisons including those between a marketer's current price and a former, future or suggested price, or between a marketer's price and the price of a competitor's comparable product should be fair and accurate.
- **USE OF TEST OR SURVEY DATA**: All test or survey data referred to in advertising should be valid and reliable as to source and methodology, and should support the specific claim for which it is cited. Advertising claims should not distort test or survey results or take them out of context.
- **TESTIMONIALS AND ENDORSEMENTS**: Testimonials and endorsements should be used only if they are: Authorized by the person quoted; Genuine and related to the experience of the person giving them both at the time made and at the time of the promotion; and not taken out of context so as to distort the endorser's opinion or experience with the product.
- **USE OF THE TERM "SWEEPSTAKES"**: Sweepstakes are promotional devices by which items of value (prizes) are awarded to participants by chance without the promoter's requiring the participants to render something of value (consideration) to be eligible to participate. The co-existence of all three elements - prize, chance and consideration - in the same promotion constitutes a lottery. It is illegal for any private enterprise to run a lottery without specific governmental authorization. When skill replaces chance, the promotion becomes a skill contest.
- **PERSONAL DATA**: Marketers should be sensitive to the issue of consumer privacy and should only collect, combine, rent, sell, exchange or use marketing data. Marketing data should be used only for marketing purposes.

The DMA is a fervent advocate of self-regulation and the marketing and mail order companies who are members of the association are expected to abide by these guidelines in letter and spirit: "These self-regulatory guidelines are intended to be honored in light of their aims and principles. All marketers should support the guidelines in spirit and not treat their provisions as obstacles to be circumvented by legal ingenuity".

The DMA's latest initiative to protect Internet users' privacy is an opt-out scheme to be operated by the association itself. This service is called **e-MPS (*Electronic Mail Preference Service*)**. It was announced in December 1999 and officially launched on 10 January 2000. This free service allows users to register their e-mail addresses stating the categories of messages from which they wish to opt-out (business-to-consumer, business-to-business, or both). Direct marketers, for their part, can use the e-MPS system to clean their e-mail address lists (non-members of the DMA are charged a fee of $100 for this service). This process is carried out online and takes only a few hours to complete.

The scheme has been fiercely attacked by American anti-spam campaigners, including representatives of MAPS, Junkbusters Corp. and CAUCE. Some of the DMA's own members are also strongly opposed to the idea. Three main criticisms have been levelled at the e-MPS scheme:

- This opt-out list is based on the principle that the onus is on the Internet user to ask for relief and that marketers have the right to send UCE or UBE (Unsolicited Bulk E-mail) until told to stop. This has led to charges that the DMA's approach is profoundly hostile to consumers as well as to the Internet infrastructure. Nick Nicholas, current Executive Director of MAPS has warned marketers who rely on the e-MPS list that they could find themselves added to the Realtime Blackhole List.

- The DMA refused to allow ISPs to opt-out their entire domain on the e-MPS system. The DMA has defended its approach arguing that the scheme is based on the individual's right to opt out. In addition, the DMA maintains that the ISPs do not need the e-MPS since they already have tools to detect and filter UCE.

- On a more general note, this initiative betrays a reluctance on the part of the DMA to accept the concept of permission marketing. The DMA has been ambivalent and has even contradicted itself on this issue. While it has ostensibly espoused the opt-in approach, the public statements of its leadership have been fairly ambiguous, to say the least. The following is an extract from the keynote address delivered by Robert Wientzen, President and CEO of the

DMA, at its recent annual conference: "A relatively new Internet-related issue that impacts our industry and its image is unsolicited commercial e-mail. Well, let me begin by recognizing that bulk unsolicited commercial e-mail is not real popular with consumers. And to date, very few of you are employing it. However, **we also feel that most of those who push for an opt-in-only regime have very little understanding of the incredibly negative impact it would have on the future use of e-mail as a marketing tool.** So in the end, we cannot let the unsavory, dubiously employed bulk e-mail out there destroy the opportunities of targeted, sophisticated, responsibly used commercial e-mail, which, without doubt, holds promise as a powerful marketing tool. So, the DMA is endeavoring to do just that: preserve unsolicited commercial e-mail as a business communications tool, while also supporting the development of various permission marketing models" (24).

---

24) **H. Robert Wientzen:** *The DMA 82nd Annual Conference & Exhibition*, Toronto - Monday, October 25, 1999

Chapter II: E-mail marketing: services offered and practices

Technological and structural change in society is necessarily diachronic in nature. In relation to online marketing, this is manifested in the concurrent existence of two types of operator: those who still continue to engage in spamming using all the tools available and undeterred by the legal and financial risks involved, as we will be seeing in the first part of this chapter, and those who oppose spam and are developing a radically different business model based on the theories of permission-based marketing. We will be analysing these companies in terms of market data, growth model, product offerings, business methods and technology. We will also be discussing the issues of opt-in and data privacy.

II.1) - Spam today: technology, services and risks

II.1.1) - Spamware

Spammers use two main tools: one to harvest e-mail addresses and the other to bulk-mail their advertisements. These software tools are collectively referred to as spamware.

- *Harvesting tools*

  There are very few harvesting programs on the market: On Target 98, Post News 2000 and Atomic Harvester 2000. All work both on the web and on newsgroups. Atomic Harvester 2000 is indisputably the market leader although one cannot really speak of a standard in this new and highly unstable market. It is very attractively priced at $179. It is sometimes bundled with the mailing package Desktop Server 2000. We should also mention E-mail Marketing 98, an "integrated system" of sorts, which performs both functions: extraction of e-mail addresses from newsgroups (collection of addresses filtered by keywords, first names or surnames) as well as bulk-mailing.

The main reason for collecting e-mail addresses directly rather than buying them in is that bought-in lists contain a lot of invalid data and even those addresses that are live tend to belong to users already saturated by a multitude of previous campaigns based on the same lists.

These software products are noteworthy for their ease of use. They operate by automatically navigating websites and public spaces on Usenet, using a list of URLs either specified in advance or created by means of keywords entered into search engines. The software then systematically collects all the e-mail addresses found on those websites or newsgroups. For example, a reseller of golfing equipment wishing to compile a database of e-mail addresses of prospects will choose a list of keywords such as: "golf, golfers, putting, tee time, golf balls, 9 iron, club house, etc.". The software application will go to all the URLs referenced under these terms and then hoover up all the e-mail addresses it finds there.

To speed up the process, Atomic Harvester 2000 allows the user to connect to 15 sites at once and gather data from all of them in parallel. Harvesting programs can be set up to exclude sensitive TLDs (.mil or .gov, for example) or those unsuited to the subject matter of the spam campaign. It is also possible to avoid URLs identified by pre-defined keywords. These programs are also touted as being able to avoid pages containing spam traps, but no publisher provides precise information on the effectiveness of this function, since a spam trap can be an innocuous e-mail address behind which a site administrator or ISP lies in wait. Moreover, each of these programs has a specific signature which is masked behind the browser's signature but which the most highly-prized sites and service providers are able to detect. Finally, e-mail harvesting tools have features enabling the user to delete duplicate addresses, extract addresses (in many cases manually) and save the lists of addresses thus compiled.

- *The mailing tools*

Mailing tools are software applications capable of sending bulk e-mail without going through a specific mail server or a particular ISP. The most widely available products, such as Desktop Server 2000 and Stealth MassMailer v.3.2, turn the spammer's PC into a mail server in its own right, which avoids trouble with ISPs for hogging their bandwidth.

These applications are fast and simple to use, they perform reporting functions and they can circumvent the filters put in place by the ISPs. Stealth MassMailer is a complete product available on special offer at $200 (compared to a list-price of $399). Generally

speaking, these programs are not found in shops and can be bought only from online distributors such as Bulk E-mail Software Superstore.

Stealth MassMailer has an impressive output, capable of sending more than 250,000 messages an hour (using a 28.8K modem), although this level of performance can be achieved only by using the resources of an ISP. Sending capacity on a standard connection is of the order of 5,000 messages an hour. For a small company wishing to remain anonymous and to prevent its messages being traced, the software has the attraction of not requiring a valid mail account (POP). It also has a feature enabling the messages to be personalised ("Dear John ....") with a view to increasing positive response rates (25). Stealth MassMailer also enables random generation of the "From :...." field and falsification of the username and domain name during sending (as an option). This falsified information is carried through to the header of the received message which may also show a forged sender's name. It is also possible to add false information in the "Received from:", "Received by:" and "Date stamp and recipient" fields in the header. Stealth MassMailer claims the ability to bypass anti-bulk mail filters – including those of AOL, whose members are the prime target for spammers – by suppressing the message header. Finally, all these mailing packages include monitoring functions (progress, status, error log file, etc.).

It is rather anomalous to find such products on open sale, through what appear to be official distributors, given that their functionality includes features designed to divert Internet traffic, a practice now outlawed in an increasing number of US states. Moreover, it is not easy to obtain detailed information on the functionality of these products, as the publishers or resellers prefer to make them available by download only with online payment by credit card. Could this be a sign that the market is heading underground? Yet the suppliers make sure to comply with their legal obligations by warning their customers of the restrictions on spamming ("Is it legal?", "The Bulk E-mail Survival Guide" etc.), from which it is manifestly obvious that what these applications do is against the law.

II.1.2) - Spam consultants and service providers

The bulk e-mail services available on the market can be divided into two main categories: campaign hosting and brokering of e-mail addresses. In the market for spam services, one finds professional op-

25) This feature works if the addresses supplied are in the form firstname.surname@xxx.com. Harvesting applications have a feature enabling this type of address to be extracted.

erators side by side with what are clearly amateurs or opportunists trying to peddle their wares on the Web.

- *Spam campaign hosting*

  Companies operating in this domain offer the complete range of services required to organise a spamming campaign: there are many small operators openly carrying on this business on the Internet. Web Studios, for example, charges $5/1000 for a mailing and $20/1000 if the client wants to have the addresses as well. Some of these companies offer a "bullet-proof" service, which is supposed to circumvent the counter-measures taken by the ISPs. Marketing Masters is the main player in this niche with a service called *Bullet Proof Web Space*, in which campaigns are hosted on a dedicated site so as minimise complaints. The price is $200 for setting up the service and $200 per month for hosting.

  Elite Web Hosting offers the same service for $1,500 a month. This company aspires to an ethical stance by enjoining its customers to observe a code of good conduct: "Our Bulk Laws (...) clarify what our members can and cannot do in terms of direct marketing and will enable them to check that every unsolicited targeted direct marketing e-mail they send is commercially justified and in accordance with the legal requirements. We actively support the ethical provisions contained in the Senator Murkowski's anti-spam law and of course the efforts by CAUCE to free the Internet of fraud". It is rather unusual to find this type of service provider claiming to operate a no-spam policy. What it probably means is that operators are beginning to respond to the reduction in their room for manoeuvre and attempting to stay within the law. This exercise is not always free from ambiguity.

  A number of these operators, moreover, cannot be accused of failing in their legal obligations vis-à-vis their customers. Many of them explicitly draw their customers' attention to the risks entailed by misguided campaigns. These warnings serve both to disclaim liability and to recommend the use of a professional service provider: thus, for example, Rod Truit, creator of Rod's Networking Services attempts to temper the unrealistic expectations of his customers "(...) who think that everybody who receives an e-mail promoting their obscure product is going to buy it". He cautions them with the warning that "(...) no Bulk E-mail application can completely hide your identity or your use of an ISP. We shall not be liable for the closure of your account. We recommend all those who wish to engage in Bulk E-mail to use the services of a professional".

In the same vein, Net Achievers gives the following recommendations to aspiring spammers: "When sending bulk e-mail, always use a valid "from" and "reply to" e-mail address, otherwise the bulk e-mail will be blocked. When sending bulk e-mail, always keep your bulk e-mail sales letter very short. Always offer the recipient a way to be removed from your list. Never put your website address on the bulk e-mail letter. Only give people your URL after they have requested more information. When sending e-mail to your potential prospects, using your bulk e-mail software, be sure to pay attention to the local, state, and federal laws pertaining to bulk e-mail. The Internet is a constantly changing place and there are many forces at work to change, regulate, and restrict our rights on the Internet."

For Door Net "the best advice is to get a company specialising in bulk e-mail to do it for you. That way you don't have to worry that somebody will complain about you to your ISP."

➢ *The e-mail address brokers*

There are many lists of e-mail addresses available wholesale on the Internet. There are many suppliers, including Bulkbarndotcom, Web-Promoters and Bulkers.net, all offering basically the same range of services:

- A membership offer with three different subscription options. Option 1: 300,000 addresses a week for $19.95 a month; Option 2: 500,000 addresses a week for $29.95 a month, Option 3: 1 000,000 addresses a week for $39.95 a month. By way of comparison, Bizzmaker offers 300,000 addresses a week for $13.95 a month, 500,000 addresses a week for $22.95 a month and 1,000,000 addresses a week for $36.95 a month.

- Online lists of addresses for immediate downloading: from $19.95 for 300,000, for example, to $49.95 for 1,000,000 general Internet addresses and from $19.95 for 300,000 to $99.95 for 4,000,000 AOL addresses.

In response to the anti-spammers – "(...) bombers, blasters, flamers and just plain old complainers" – the Californian company ListGuy markets three varieties of lists which enable businesses to continue to operate even in an anti-spam environment: opt-in lists, lists of "harvested business owners and opportunity seekers" and remove lists, which enable customers to clean up their lists of prospects. Listguy.com offers a CD-ROM containing 11 million "fresh", "verified" and "filtered" addresses, i.e. purged of the addresses of known troublemakers (anti-spam activists) and of those

who have asked to be removed, and of the .gov, .mil and .edu domains. DB Networks, Door Net, Elite Webhosting also offer subscription options for updated version of their remove lists.

Not all suppliers in this sector share this concern for clean lists. The availability of so many lists of e-mail addresses inevitably raises the question as to the quality of the addresses and their validity, not to mention whether genuine permission was obtained prior to collection. Targeted lists are usually described in rather vague terms: the most common selection criteria are country, state, city, gender, interests, occupation and business sector. Interests are broken down into about fifty major categories which are rather reminiscent of the main Usenet domains:

Common selection criteria for e-mail addresses based on interests		
Adult Oriented	Business – Advertising	Business – Finance
Business - General	Business - Home Based	Business – Industry
Business - International	Business – Internet	Business – Marketing
Business - MLM	Business – Opportunity	Computer Software
Computer Software - Resellers	Computer Software – Shareware	Computer Software - Web Tools
Computers	Credit Cards	e-Commerce
Education	e-marketing	Entertainment
Entrepreneurs	E-Zines	Food & Drink
Games	Gardening	Health & Beauty
Insurance	Job	Law
Literature	Miscellaneous	Music
OnLine Banking	OnLine Auctions	OnLine Shopping
OnLine Stores & Malls	Personal	Programming
Real Estate	Religion	Science & Technology
Small Business - Home Business	Social Sciences	Software Development
Sports & Fitness	Travel	Webmasters
Website Owner - Business	WWW Technology	

II.1.3) - Spam today: practices and risks – An illustration

As was seen in the preceding chapter, spamming in the United States today entails risks. Spammers are disowned by the marketing profession and any business resorting to spam risks damaging its image and reputation. Now in addition, as we will be seeing in the two following cases, there is a very real threat of severe legal and financial consequences. So much so that one has to wonder whether the spammers really know what they are getting involved in, at least in the case of those spammers who are not entirely unscrupulous.

➢ The Benchmark Print Supply case

This recent case is an excellent illustration of the changing fortunes of the spammers and their victims.

Benchmark Print Supply is a company based in Atlanta, Georgia owned by Mr Sam Khuri. Its main business consists of selling laser printer toner cartridges online from a catalogue distributed by e-mail. It is a typical spam operation which uses forged sender's addresses and an inactive remove-list option. In August 1998 Benchmark Print Supply was identified and blacklisted. It then became the target of repeated attacks by irate Internet users who reported it to the FTC and bombarded its telephone and fax lines. Nor did the harassment stop at the office: several anti-spam sites published the owner's home address and telephone number (26). Sam Khuri turned a deaf ear to these protests and feigned complete ignorance. One newsgroup participant reported having spoken to Khuri's mother who had warned him very nicely that her son was very edgy, armed and driving a black Mercedes. Sam Khuri has a reputation of being a more persistent spammer than most. He has been sued many times in different states by various ISPs. One of the most recent lawsuits was filed in October 1999 by Visto Corp., an Internet company based in Mountain View (CA), which provides e-mail services to one million members . Visto accuses Sam Khuri of spamming its members using a forged identity, damaging its reputation and clogging up its mail servers (27). Ironically, however, the one lawsuit to have really made a difference was brought by a British ISP, BiblioTech, which sued this particular spammer in the US District Court for the Northern District of Georgia.

Established in 1995 in Fulham, London, BiblioTech was initially a cyber café which capitalised on the extraordinary upsurge in Internet use to become a full-blown ISP with a booming business. Like every other ISP of any size, it fell prey to the spammers who were very active in 1997 and 1998. Apart from the vexation caused to its customers, BiblioTech was faced with technical difficulties due to the massive volume of spam being received each day. According to Chris Verdin, the company's Financial Director, BiblioTech had to deal with hundreds of thousands of spam messages every hour (28). So much so that BiblioTech made it its policy to systematically track down the spammers and threaten them with litigation. In January 1999, BiblioTech brought its first legal actions in the US

26) http://www.darron.net/benchmarkprintsupply/ http://www.pglwebsdesigns.com/bps.html
27) **Carl S. Kaplan**: "*Company says Junk E-mailer stole its identity*" - Cyber Law Journal – New York Times – November 19, 1999
28) **Tim Richardson**: "*UK anti-spam minnow takes on US big fish*" - The Register – 20/04/99 http://www.theregister.co.uk/

courts against five American spammers. These resulted in out-of-court settlements with four of the spammers who agreed to stop their activities. If they refused, they would face a damages claim for $2 million. In order to track down the spammers, BiblioTech retained the services of Sanford Wallace, now embarked on his new career of anti-spam consultant and the Atlanta law firm of Arnall Golden & Gregory, with Pete Wellborn taking charge of the lawsuit against Benchmark Print Supply. This is a law firm with a strong track record in this sort of case, having represented CompuServe some years previously in its action against the self-same Sanford Wallace and his Cyber Promotions company, now on the other side of the legal fence.

In April 1999, BiblioTech rejected a proposal by Sam Khury for an out-of-court settlement, under which he would pay BiblioTech damages and undertake to refrain from spamming its subscribers but without promising not to resume his activities through other ISPs. This was not enough for BiblioTech which wanted him to cease spamming altogether. An out-of-court settlement was finally reached in March 2000. The great merit of this settlement was that it was not only financial: Sam Khuri did indeed pay BiblioTech an undisclosed sum in damages and agree to pay the costs of the action. But, most crucially, he has also bound himself to include in all his future campaigns without exception a valid return address and a genuine remove option. In the event of a breach of this undertaking, he will be liable to pay $1,000 for each single act of breach, whether committed against BiblioTech itself or any other ISP whatsoever. What is most encouraging about this case, which was brought by a European plaintiff, is that it was informed by a spirit of solidarity within the ISP community and a concern for the overall health of the Internet.

- The Christian Brothers case

The Christian Brothers are a group based in Queens, New York, which uses the Internet to sell extracts of apricot seeds, Laetril or vitamin B17, which is claimed to be an effective treatment for cancer. The sales pitch is replete with insinuations of conspiracy and persecution. It is based on pseudo-scientific explanations backed up by biblical quotations ("And God said, Behold I have given you every herb bearing seed, which is upon the face of all the earth, and every tree, in the which is the fruit of a tree yielding seed; to you it shall be for meat" - Genesis 1:29). Laetril is in fact amygdalin, which is found in the seeds of many kinds of fruit. The substance was isolated in the first half of the nineteenth century by two French researchers. For almost 50 years, various individuals attempted to mass-market Laetril in the United States, but its effectiveness as a cancer treatment was never proved in any scien-

tific study. Following a number of high-profile deaths in the 70s, most notably that of the actor Steve McQueen, who was treated with Laetril in a Mexican clinic by a disbarred Texas dentist, the treatment was eventually banned after being discredited by a study conducted by the National Cancer Institute. It is no longer on sale apart from on a number of websites, including that of the Christian Brothers (heavenlyhealing.com, apricotsfromgod.com, canceranswer.com and eatseeds.com).

Since 1997, according to the report prepared for the court, Christian Brothers had unlawfully obtained mailing lists of the e-mail addresses of AOL members and sent more than 20 million messages to them using AOL's computer networks. The unsolicited messages, which included fraudulent headers misrepresenting that the messages came from aol.com, provided links to Web sites where the apricot seeds and related books and videotapes were for sale. After receiving thousands of complaints from its members, AOL sent a cease-and-desist letter to Christian Brothers in February 1998. The spamming persisted however. In December, AOL filed suit against Christian Brothers and its president, Jason Vale. In a default judgment entered against the Christian Brothers in June 1999, the court ruled that AOL was entitled to recover for unjust enrichment, since Christian Brothers unlawfully used the AOL mark and misappropriated services that otherwise could have been sold to advertisers. In a telephone conversation in January 2000, Mr. Vale told AOL's counsel that Christian Brothers was inclined to default. Ignoring the lawsuit entirely, the group continued to transmit bulk unsolicited e-mails over AOL's network. In addition, Jason Vale responded to an attempt by AOL's process server to hand-deliver AOL's motion for a default judgment by throwing the papers out the door.

Final judgment was given by a judge of the Southern District of New York at the end of December 1999. The judge issued a permanent injunction barring the group from using AOL's network and trademark. The injunction is backed up by the threat of contempt and punitive damages. In addition, the Christian Brothers were ordered to pay more than $600,000 in damages: $17,940 in hardware processing costs; treble damages of $389,020 for lost advertising revenue; $24,625 in attorney's fees; and $200,000 in punitive damages for clogging the computer systems of America Online Inc. with the transmission of millions of unsolicited e-mail messages: "The Defendants' transmission of unsolicited bulk e-mail to AOL has damaged, and, if unabated, will continue to damage, AOL's business, its goodwill, and its relationship with its members," wrote Judge Pitman. "AOL's valuable trademark and service mark and associated goodwill are diluted and damaged by

their wrongful association with junk e-mail and junk e-mailers like the Defendants." (29)

These two cases are symptomatic of the current fortunes of spammers in the US, those "(...) fly-by-night operators who are essentially judgement proof", in the words of a Californian lawyer who has brought five spamming cases on behalf of ISPs (30). The approach consisting of penalising spammers through substantial damages awards provides a remedy which, while it does not vindicate the substantive right to data privacy, is nonetheless an effective one and one which may help to eradicate the problem in the short term.

While spamming continues to subsist, though shunned by the industry as a whole, the e-mail marketing business is consolidating on a model which is far more powerful financially and technologically. The key features of the model are fairness and openness about data gathering and a voluntary and permission-based relationship between advertiser and prospect. The main players in this market, most of them start-ups, are now setting the parameters for the Internet marketing of tomorrow. It is worthwhile taking an in-depth look at their concept of data privacy based on ***opt-in e-mail lists***.

II.2) - Analysis of the business of the permission e-mail marketing companies – products and services

E-mail marketing is an emergent sector linked to the information society and the growth of electronic commerce. This chapter focuses on three firms in particular, chosen on the basis of the following criteria: they are all relatively long-established by the standards of the industry (4 to 5 years), they have high-profile operations and prestigious client lists, and they share a strong commitment to permission marketing. We will consider, in turn, their economic situations, growth strategies and products and services. The three companies are:

- **24/7 Media**: 24/7 Media has 470 employees worldwide. It claims to reach half of all US households that have Internet access. It operates as an advertising agency in addition to its e-mail marketing activity. Headquartered in New York, in the Silicon Alley district, it is also in the process of expanding into Europe. It has a stock market capitalisation of $430 million.

- **MessageMedia**: this company currently has 375 staff on its payroll (May 2000) and is entirely dedicated to e-messaging. Its client

29) **Bruce Balestier**: *"Big Fine for Spamming AOL Members"* - New York Law Journal - December 14, 1999.
30) **Carl S. Kaplan** – op. cit.

portfolio includes Cisco, AOL, Microsoft, Yahoo!, Geocities, CMP Media, Bertelsmann, etc. Headquartered in Boulder, Colorado, its main shareholder is SOFTBANK. Its European operation is a partnership venture with the Vivendi subsidiary @Viso. MessageMedia has a stock market capitalisation of $271 million.

- **NetCreations:** this is a smaller outfit, with just forty employees. Clients include Dell Computer, Compaq, J. Crew, Ziff-Davis and Business Week, whose newsletters it manages. NetCreations has a database of 6 million e-mail addresses (opt-in). It too is headquartered in New York, in the West Broadway district. Its Nasdaq valuation is $418 million.

II.2.1) - General facts on the e-mail marketing industry

The e-mail marketing sector in the US today comprises a number of different businesses in which approximately 50 major suppliers have specialised to one extent or another. At first sight, these companies are all very similar: they share the same values, many of them are listed on Nasdaq, they all subscribe to the principles of permission based marketing and opt-in e-mail. But looked at more closely, no two are really alike. Every time it makes an acquisition, each company acquires new expertise and new customers and becomes stronger in some particular niche of the market. In broad outline, however, there are six main types of business:

- **direct marketing by e-mail**. By definition, all the companies in this category are Internet start-ups: this is the case of NetCreations Inc., YesMail.com, BulletMail, Axciom and 24/7 Media, in relation to part of its operations, as we will see below.

- **incentive marketing**, consisting of online reward schemes in which points are earned by registered users who take part in games and contests and who of course supply personal data with a view to receiving targeted and consensual advertising messages. YoyoDyne Entertainment, founded by Seth Godin and now part of Yahoo!, is typical of this family of companies, which also includes MyPoints, Netcentives, Beenz, CyberGold, ClickRewards, Freeride.

- **e-mail outsourcing permission marketing** services such as those operated by Exactis.com Inc., a subsidiary of 24/7 Media and by MessageMedia.

- **portals** such as XOOM.com, Inc. (www.xoom.com), a subsidiary of the interactive division of the television network NBC (NBCI – NBC Internet), which runs its own database of 7.5 million sub-

scribers who regularly receive e-mail solicitations for e-commerce promotions, targeted according to their needs and interests.

- **advertising agencies**, such as DoubleClick or Flycast, who as well as running advertising campaigns on the Web now also offer e-mail marketing. Since its $1 billion all-equity merger with Abacus, DoubleClick has launched two new services, DARTmail Publishers and DARTmail Prospects, which are based on qualified lists of opt-in e-mail addresses.

- **traditional direct mail** companies who broker (buy and sell) lists of addresses and who have now expanded into e-mail marketing. The big names in this category include Direct Media (a subsidiary of Acxiom) and American List Counsel (ALC). These companies have powerful backers and have years of expertise in database marketing; they also have their own lists of qualified addresses (40,000 lists and 7 million e-mail addresses in the case of Direct Media –110 million households in the case of ALC).

The e-mail marketing sector looks set to expand. In particular, it could start to attract the interest of big corporations such as IBM, Microsoft, Netscape Communications, ATT and Hewlett-Packard, all of whom run large databases of customers and prospects and all of whom are capable of rapidly deploying the necessary resources and skills: database engineering, datamining, workflow and e-CRM (Electronic Customer Relationship Management). The publishing group IDG, for example, has already launched its own system (IDG List Services). Another example is the 1998 takeover of Metromail by Experian, a group originally specialising in credit reporting (TRW). ISPs are also likely to enter the e-mail marketing business with a view to leveraging their subscriber lists. Already major portals such as Yahoo!, AltaVista, Excite and NetZero provide opt-in e-mail services. In many cases, these services have been outsourced to specialist companies for the time being. Rosalind Resnick, CEO of NetCreations, has stated that **a portal earns approximately $4 a year per subscriber**; which represents substantial extra revenue when you have 400,000 names, as NetZero does (31).

II.2.2) - Economic data and growth strategy of e-mail marketing companies

As will be seen in the detailed analysis of 24/7 Media, Message Media and NetCreations, the e-mail marketing companies have all the hallmarks of new economy businesses: rapid growth, high market capi-

31) **Stefani Eads**: *"From $1,000 to an IPO in Only Four Years - New York entrepreneur Rosalind Resnick finds riches in E-mail direct marketing"* – Business Week - August 5, 1999 - New York

talisation, negative income. Most of them have opted for a strategy of external growth – expanding by taking over other firms in the same sector.

➢ Economic situation of three e-mail marketing companies

24/7 Media Inc. is growing at a spectacular rate (sales up by 331% between 1998 and 1999) but, as the table shows, is still a long way from profitability, having posted an operating loss of $43 million in 1999.

Three-year trading record of 24/7 Media Inc.
(source: SEC – 10-K 24-03-2000)

(US $)	**1999**	**1998**	**1997**
Sales:			
- *Network*	81,158,000	19,744,000	1,467,000
- ***E-mail***	**8,853,000**	**1,003,000**	**69,000**
- *Consulting and license fees*	-	119,000	1,681,000
Total sales	**90,011,000**	**20,866,000**	**3,217,000**
Purchases:			
- Network	61,000,000	15,970,000	1,655,000
- E-mail	4,963,000	179,000	14,000
Total purchases	**65,963,000**	**16,149,000**	**1,669,000**
Gross margin	**24,048,000**	**4,717,000**	**1,548,000**
Operating expenses:			
- *Sales and marketing*	23,396,000	8,235,000	1,857,000
- *General and administrative*	26,730,000	9,396,000	3,258,000
- *Product development*	1,891,000	2,097,000	1,603,000
- *Write-off of property and equipment*	-	-	757,000
- *Legal costs in connection with claim*	-	-	232,00
- *Write-off of acquired in-process technology*	-	5,000,000	-
- *Amortization of goodwill*	15,097,000	5,722,000	-
Total operating expenses	**67,114,000**	**30,450,000**	**7,707,000**
Operating loss	**(43,066,000)**	**(25,733,000)**	**(6,159,000)**

The breakdown of sales shows that the e-mail marketing business is still contributing only a small share of the company's overall revenues. E-mail marketing sales of $8.85 million in 1999 represented less than 10% of total sales. However, it is growing very strongly – up by 783% on 1998. The management of 24/7 Media Inc. predicts that e-mail marketing's share of sales could reach 17% in 2000. The table also shows that in 1999 the company's overall gross margin as a percentage of sales was 21.6%, as against a gross margin of 44% on e-mail marketing, indicating that this is potentially a highly profitable business.

MessageMedia grew by over 600% last year. The company has begun to market e-mail marketing software (only in the US for the time being) and this accounts for 10% of turnover. With operating costs of over $52 million compared to sales of $10 million and a gross margin of $5 million, MessageMedia is still a long way from profitability and has accumulated operating losses of $90 million.

Three-year trading record of MessageMedia Inc.
(source: SEC – 10-K 20-03-2000)

(US $)	**1999**	**1998**	**1997**
Sales			
- *e-messaging*	9,001,161	424,564	1,450,598
- *software licenses*	1,020,383	-	-
- *First Virtual Internet Payment System*	-	863,226	-
Total sales	**10,021,544**	**1,287,790**	**1,450,598**
Purchases	4,589,358	97,553	270,416
Gross margin	**5,432,186**	**1,190,237**	**1,180,182**
Operating expenses:			
- *Marketing and sales*	9,704,452	1,934,486	5,424,110
- *Research, development and engineering*	4,935,931	4,828,277	6,687,177
- *General and administrative*	7,677,527	3,810,073	4,377,688
- *Restructuring expenses*	1,025,000	812,166	
- *Write-off of in-process technology*		1,300,000	
- *Depreciation and amortization*	28,923,515	2,470,917	1,097,716
Total operating expenses	**52,266,425**	**15,155,919**	**17,586,691**
Operating loss	**(46,834,239)**	**(13,965,682)**	**(16,406,509)**

NetCreations also recorded very strong growth in 1999 with sales up by over 500%. In absolute terms, NetCreations' turnover is twice that of MessageMedia and, being a smaller company with lower operating expenses, NetCreations is the only one out of the three firms to have achieved profitability. As in the other two cases, it incurs very substantial purchases, reflecting, as will be seen, royalty payments to the websites that collect the e-mail addresses.

Three-year trading record of NetCreations Inc. (source: SEC – 10-K 20-03-2000)			
(US $)	**1999**	**1998**	**1997**
Sales	**20,658,223**	**3,446,539**	**1,100,781**
Purchases	10,464,359	1,509,776	173,124
Gross margin	**10,193,864**	**1,936,763**	**927,657**
Operating expenses:			
- *Marketing and sales*	2,088,100	492,004	289,904
- *Technology, support and development*	694,311	373,746	193,554
- *General and administrative*	1,914,608	365,343	151,221
- *Depreciation and amortization*	195,362	23,414	9,515
Total operating expenses	**4,892,381**	**1,254,507**	**644,194**
Operating profit	**5,301,483**	**682,256**	**283,463**

➢ The external growth model

Each of these e-mail marketing companies has its own story. In the case of **NetCreations**, it is the typical start-up story: the company was formed 5 years ago by Rosalind Resnick, a journalist with the Miami Herald, and Ryan Scott Druckenmiller, a computer expert, who are now its two main executives. NetCreations started out designing websites but seized the opportunity to branch out into e-mail marketing. In just 4 years the company has gone from drawing-board to IPO. The turning point came in November 1996 when the computer publishing group Ziff-Davis asked NetCreations to rent a list of 15,000 e-mail addresses belonging to webmasters who had registered on its site to receive information on website administration tools. This campaign was a success and Ziff-Davis has remained a stalwart client of NetCreations ever since. In 1997, with a new automated opt-in registration system called PostMasterDirect developed in-house under Druckenmiller's leadership, NetCreations completed its transition to an e-mail marketing company with two target markets: websites looking to set up their own opt-in e-mail services and businesses looking to rent lists of addresses.

24/7 Media was formed out of the December 1997 merger of two interactive marketing companies, Petry Interactive and Katz Millennium Marketing. It has pursued an aggressive strategy of external growth in both its markets – e-mail marketing and selling advertising space on the Internet – by buying up competing companies and incorporating their technology and client portfolios (advertisers and support sites) as well as their lists of e-mail ad-

dresses. In the course of the last 15 months, in the e-mail marketing field alone, 24/7 Media has been involved in three takeovers or mergers to the tune of over $560 million. The first of these deals (SIFT Inc.) represented the decisive move by 24/7 Media into e-mail marketing:

Mergers/acquisitions by 24/7 Media Inc.

Company	Date	Method	Business
SIFT Inc.	March 1999	Stock-for-stock purchase ($22 million) SIFT became a wholly-owned subsidiary of 24/7 Media Inc. and continues to operate under its original name. Headquartered in: Sunnyvale (CA)	E-mail marketing: management and rental of a list of 3 million e-mail addresses (opt-in) Main clients: Cahner's business Information, Cisco Systems, Dell Computer, Dun & Bradstreet, Experian, Hearst Books/Business Publishing, Intel, Netscape Communications, Oracle, RealNetworks, Scholastic Acquisition of CRM technology
Consumer-Net	August 1999	Purchase ($52 million) Merged into 24/7 Mail	E-mail marketing: management and brokerage of a database of over 3 million e-mail addresses (opt-in) 125 websites are clients of ConsumerNet and members of the ConsumerNet Alliance (including: Fox Interactive, GameSpot, Columbia TriStar, BMG, RCA) Acquisition of database management technology and purchase behaviour profiling technology
Exactis.com	February 2000 – Effective in June 2000	Stock-for-stock transaction ($490 million)	Permission e-mail marketing and outsourcing services – Distribution of newsletters (2 million subscribers to one daily newsletter – Infobeat from Sony Music) and news bulletins 75 clients in the media, e-commerce and financial services sectors Advanced proprietary technology

There is even talk of a merger with DoubleClick. Discussions are in fact taking place but nothing concrete has come of them as yet. One striking feature of the new economy is that there is a lot of talk, whereas in the old economy merger negotiations have traditionally been kept secret right up to the last moment.

MessageMedia has a very similar profile. The company was formed in 1994 to develop an Internet payments system (FVIPS: First Virtual Internet Payment System). Thanks to a majority stake taken by the financial group Softbank, the company turned to e-messaging in the 2nd half of 1998, acquiring two specialist companies, E-mail Publishing, Inc. (Epub) for $20 million and Distributed Bits L.L.C. (Dbits) for $5.5 million. In August 1999 two further

companies were acquired, Revnet Systems Inc. ($41 million) and Decisive Technology Corporation ($39 million).

➢ The export growth strategy

The e-mail marketing companies do not intend to confine their activities to the US domestic market. They are all working on plans to expand worldwide, particularly into Europe with its current total of 153 million electronic mailboxes and where e-commerce will be worth some €36 billion in 2000 and account for 6.3% of total commerce by 2004, according to Forrester Research.

In October 1999, **MessageMedia** established its European subsidiary in the form of a joint venture with @viso, an incubator company owned 50:50 by SOFTBANK and Vivendi. This company is headquartered in Paris, but has already opened regional offices in Dusseldorf and Stockholm, while its technical facilities and research & development teams are based in Switzerland. Further offices are to open shortly in Munich, Madrid, Amsterdam and Milan. The company expects to employ 100 staff in Europe by the end of this year. Letters of intent have also been signed with eVentures UK and eVentures Holdings Pty Ltd in Australia with a view to creating local subsidiaries of the company in those two countries. The Sydney operation will act as a base for MessageMedia to expand its business throughout the Asia-Pacific region.

24/7 Media carries on its advertising and e-mail marketing business in 27 countries around the world, including 11 member states of the European Union (Germany, Belgium, Denmark, Spain, Finland, France, Italy, Netherlands, Portugal, United Kingdom and Sweden). This expansion into export markets has been achieved through acquisitions: thus 24/7 Media Europe was created in January 1999 through the purchase of a majority interest in InterAd Holdings Ltd. Likewise, the company established a presence in Canada by acquiring Clickthrough Interactive and in Asia through cooperation agreements with the sales forces of Chinadotcom. The European operations of 24/7 Mail are based in London. Its aim is to offer European advertisers and list brokers the full range of permission based e-mail marketing services and to expand the database of e-mail addresses by collecting voluntary registrations from European web surfers.

II.2.3) - The eight families of services comprised in opt-in e-mail marketing

The opt-in e-mail marketing companies operating on the US market together supply quite a broad range of services. Their strengths vary according to their origins and their technological resources. There are no fewer that eight distinct families of services involved and the following description supplied by MessageMedia sets them out in their logical sequence:

- ✓ **Acquisition of personal data** using client websites or support sites. The principle is much the same as where Internet advertising agencies such as DoubleClick place banner advertisements on websites. In other words, it involves setting up a network of sites with heavy traffic on which the e-marketing company will place opt-in forms, of varying degrees of detail, enabling visitors to submit their personal information voluntarily. The information collected in this way can be used to compile marketable lists. This process may also be used to convert an existing list of e-mail addresses held by the advertiser into a list of permission profiles.

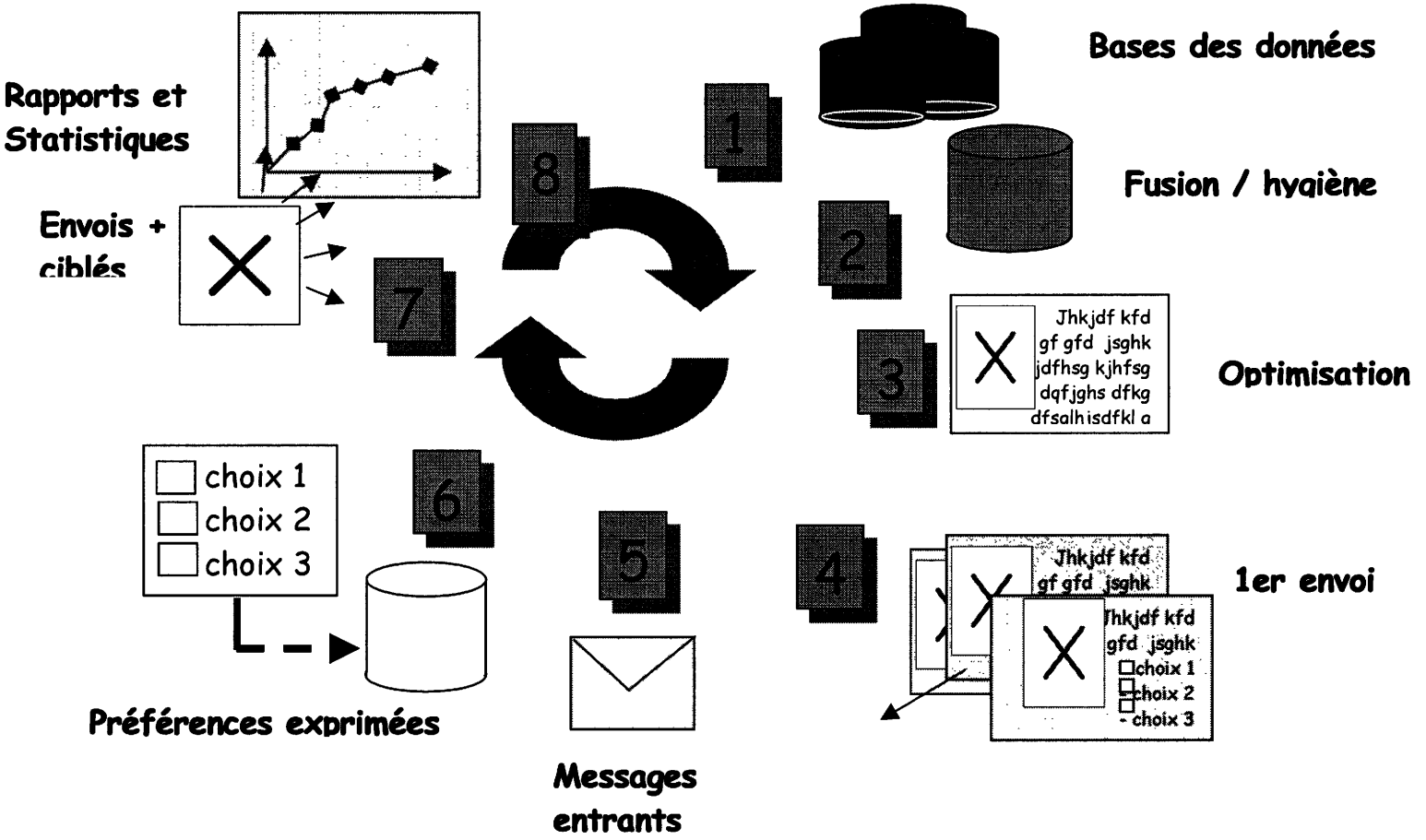
- ✓ **Administration and management of databases** and in some cases operation of clients' databases on a Facilities Management basis. This is the automated management and cleaning of files: updating, de-duplication and in some cases matching against opt-out lists, synchronisation with a master database, etc.

- ✓ **Database brokerage** based on standard socio-demographic criteria (age / gender / income / geographic location / interests etc.). This is renting opt-in e-mail lists to advertisers or intermediaries, either lists managed by the company itself or other opt-in e-mail lists available on the market which the company will obtain for the client.

- ✓ **Designing e-mail marketing campaigns**: this is a consulting service provided to advertisers and distance selling companies on the design of advertising and promotional campaigns, registration forms and opt-in clauses, drafting messages, formatting e-mails and integrating HTML code and audio or video objects, selecting targeting criteria and mailing lists, organising response procedures. This design support may also include a test run on a small sample of addressees.

Exemple concret de dialogue client (*newsletter*)

(Sources : MessageMedia)



- ✓ **Push operations** (host e-mailing): these may be either one-off (stand alone e-mail) or regular (periodic mailing of newsletters to subscribers according to frequency parameters selected by the client). The e-mail marketing companies have powerful engines to do this and have agreements with ISPs possessing sufficient bandwidth (T1 connection) to handle large volumes of traffic.

- ✓ **CRM (Customer Relationship Management)**: this is a front and middle-office service whereby the e-mail marketing company takes charge of the client's one-to-one relationship with prospects contacted by e-mail and seeks to persuade them to buy the client's products. It involves enhancing the database with additional personal data, customer confidence building, customer retention, processing registration and opt-out requests, dealing with fulfilment problems, handling users' miscellaneous queries and complaints, sending out confirmation messages and recording changes of e-mail address. These tasks are facilitated by dedicated software applications known as CRM or ERM (E-mail Relationship Management).

- ✓ **Campaign monitoring and reporting**: all the e-mail marketing companies are equipped with tools which enable them to monitor precisely the effectiveness of their campaigns and the return on investment for their clients: instant logging of messages received, identification of invalid addresses, logging of click-throughs to links inserted in e-mails or in newsletters.

- ✓ **Billing monitoring**: when an e-mail marketing company uses its cooperative database i.e. the database of e-mail addresses collected from partner websites on online registration forms, the practice is for the website which originated the data to be paid for each use of the e-mail address in respect of 50% of the selling price. This system requires information processing tools capable of monitoring data collection and use in order to calculate royalty payments.

II.2.4) - The methods used to acquire and manage personal data in a permission-based context

The e-mail marketing companies have built up considerable expertise in developing files of personal data submitted voluntarily by website visitors. The collection method used is to place opt-in forms on a network of sites. Visitors complete the forms in order to subscribe to a newsletter, take part in a competition or promotion, or receive special offers in line with the interests they register – these are all legitimate ways of gathering personal data openly through a website. At every stage in this process the e-mail marketing companies draw on their

expertise and know-how: drafting the opt-in agreement, outsourcing, datamining, economic exploitation of the information.

24/7 Media manages a total of 200 partner websites which represent a total audience of 56% of the entire US population of Internet users. These sites include:

- NetZero: offers free Internet access in return for exposure to advertising and registration of interests.
- FastWeb: registration in an information system which enables students to receive information on university grants: 2,500,000 members.
- PC Drivers HQ: a system whereby Internet users are paid to surf the web; subscription to a mailing list with a description of lifestyle characteristics: 142,800 members, 77% women.
- Guitar.com: registration on a site dedicated to amateur guitarists: MP3 files for downloading, taking part in competitions, discussion forums, commercial promotions: 20,600 subscribers.
- E-diets: registration in a personalised weight-loss programme and for a specialised newsletter: 298,000 subscribers, 89% women
- GotoWorld: registration with a portal and downloading of a browser which enables the user to surf the web and be paid 40 cents per hour of exposure to advertising (Get Paid to Surf, Chat and Shop!). 1,400,000 subscribers, 60% students.
- Riddler: registration with an online games site: 526,400 subscribers

Alongside these lists which 24/7 Media manages and markets, the company has compiled its own databases the content of which is in a sense co-owned with the web sites on which the data were collected:

- Mail Alliance: this is a general database segmented according to twenty or so lifestyle criteria: 5.7 million opt-in e-mail addresses
- Hi-Tech Alliance: this is a database of users of personal computers, software and peripherals: 1.9 million opt-in e-mail addresses.

In January of this year 24/7 Media signed a two-year agreement with Naviant, an e-marketing company specialised in one-to-one relationships, to manage a list of e-mail addresses of 5 million high-technology households on an outsourcing basis. With this new contract, 24/7 Media is now responsible for managing a total database of over 20 million opt-in e-mail addresses; this is probably the largest e-mail marketing database in the world today. According to company representatives, its databases contain 2 million e-mail addresses in the UK and 4 million in Europe as a whole.

NetCreations manages a cooperative database of 6 million opt-in e-mail addresses. During 2000 it expects to add 20,000 new addresses a day, which would bring it up to 15 million addresses within less than

a year. As in the case of 24/7 Media, this database is generated from 225 third party sites on which visitors register. These sites include:

- Internet.com: visitors to any one of this network of website's 13 technology information channels can sign up to receive newsletters.
- CMPNet: this is a publishing group specialising in information technology which operates ten or so specialist sites where readers can register to receive high-quality newsletters (CNET Digital Dispatch, for example) or to be put on a mailing list for commercial offers in their areas of interest.
- Regards.com: this site enables visitors who register to send electronic greeting cards to e-mail addresses in their address book; by registering, visitors can also receive commercial e-mails from various partners, customised according to 70 interest categories.
- Volition: this is a website offering free personalisation of Internet content ("Best of the Web"), where visitors can register, take part in games, competitions, win discount coupons or earn loyalty points etc. They may also subscribe for free to an commercial mailing list.

Depending on the terms of the contract with the website and the technological model used by the e-mail marketing company with its partner sites, these data are then managed in different ways: the simplest arrangement is where the website itself handles the opt-in process and the incoming data. In that case, the e-mail marketing company receives a copy of the registration form. This copy can be fed into the cooperative database or can be managed separately. In other cases, the website will outsource the complete management of the information to the e-marketing company, to the point of delegating all communication with those who have registered. Here the website's objective is to generate income to fund the site by collecting and selling personal data.

There are then two main data transmission modes. In the case of 24/7 Media, data are transferred periodically in batches aggregated in the Mail Alliance database. In the case of NetCreations and its PostMasterDirect.com system, the data can be transferred in real time. MessageMedia also hosts opt-in forms for some clients. The way the **PostMasterDirect.com** system operates is exemplary in terms of the quality of the consent obtained and the transparency of the process. When a user subscribes to a **CNET newsletter**, for example, a pop-up window appears containing a series of boxes to be ticked if the user wishes to receive commercial messages in relation to the areas specified. At the bottom of this list is a link to the site's privacy policy. This policy is very comprehensive and contains a notice to those wishing to subscribe to the newsletter explaining clearly the role of NetCreations:

Opt-in E-mail Newsletters

CNET offers free e-mail newsletters to users in association with NetCreations' PostMasterDirect, an independent company that creates targeted e-mail newsletters to announce various products and services. When users subscribe to a CNET newsletter, they are given the opportunity to opt in, or join, announcement lists administered by PostMasterDirect. If users choose to opt in for an announcement list, they will receive e-mail newsletters from third parties via PostMasterDirect on topics selected by the users. Users may have their e-mail addresses removed from the opt-in announcement lists at any time by following the instructions printed in the e-mail newsletters.

PostMasterDirect's e-mail tracking system recognizes when a URL in the newsletter is clicked, and records information about the user and the user's computer, such as the e-mail address registered with PostMasterDirect, the browser, the operating system, and the user's IP address. Use of this information is governed by CNET's privacy policy and the PostMasterDirect privacy policy. Personally identifiable information will not be used by CNET or PostMasterDirect for any purpose other than to deliver the newsletters. Neither CNET nor PostMasterDirect will provide this information to any third party.

When the form has been completed and the topics of interest specified, the user is asked to confirm registration – this is the initial opting in. The user is then sent an instant confirmation message from PostMasterDirect.com, the purpose of which is to ensure that the opt-in was made by the individual concerned and not by somebody else in his or her name. This confirmation message is worded as follows:

***From**: "Your subscription request" <yes@confirm.postmasterdirect.com>*
***To**: <dupont@isp.fr>*
***Date**: Friday 5 May 2000 06:07*
***Subject**: **Activate your CNET.com subscription!** [dupont@isp.fr /1248]*

Just one more step! Simply click the link below to activate the CNET.com subscription request you just sent us!
http://c.postmasterdirect.com/confirm?E= dupont@isp.fr &T=1248

If asked, your codes are E: dupont@isp.fr T:1248.

Or you can simply reply to this message. (If you do, please don't change the subject line.) In order to protect your privacy, if you do not activate your subscription, we will be unable to send you the information you have requested. So please click the link above right now!

When you confirm, you will be subscribed to:
CNET.com/Advertising.list
CNET.com/Internet_Marketing.list
CNET.com/e-commerce.list

You can unsubscribe or change the topics you get information about easily, at any time. We hope you enjoy the convenience and we'll see you online!

Thanks!
CNET.com

Three points may be made in relation to this confirmation message: the first is that it again draws the recipient's attention to the involvement of a named third party in his or her relationship with CNET. This is important because the user may not have clicked on the link to the privacy policy page. The second point is that this message confirms the details of the newsletters and the particular mailing list to which the user has subscribed. The third is that nothing can be sent to the user unless he or she

returns the confirmation e-mail. The procedure is virtually a contract between the Internet user and the website. As soon as the opt-in confirmation is received by PostMasterDirect.com, the subscriber automatically receives a second e-mail welcoming him to the mailing list:

> ***From**: "PostMasterDirect.com" <mailbox@netcreations.com>*
> ***To**: <dupont@isp.fr>*
> ***Date**: Friday 5 May 2000 06:24*
> ***Subject**: **Subscription Welcome! Thank you for your opt-in e-mail confirmation!***
>
> *Welcome to our free service! We strive to bring useful information direct to your e-mail box without spamming, and without compromising your privacy! We do not sell our lists, but we mail on behalf of vendors who want to contact you with interesting news and product information in the only topics you have specified.*
>
> *Note that every message we send will have a header like this one:*
>
> ---
>
> *This mail is never sent unsolicited. This is a PostMasterDirect.com mailing!*
> *You have subscribed to receive this information through CNET.com*
> *UNSUB ALL: -forward- this entire message to deleteall@postmasterdirect.com*
> *(be sure to **forward** the ENTIRE message, or it will not unsubscribe you!)*
> *To review your subscription: http://review.postmasterdirect.com/*
> *MAIL TO LISTS: http://www.PostMasterDirect.com/ 100% OPT-IN™*
>
> ---
>
> *To review your subscription and preferences, please visit: http://review.PostMasterDirect.com*
>
> *If you are interested in MAILING your product or service information to any of thousands of topical 100% opt-in e-mail lists, please visit: http://www.PostMasterDirect.com/*

This process of **active participation** is exemplary and shows how e-mail marketing companies are able to operate an effective and automated **double opt-in** mechanism. It must be pointed out, however, that not all the opt-in systems set up by e-mail marketing companies display the same concern for transparency. In the case, for example, of registration on the FastWeb site (student grant information), the opt-in notice at the bottom of the form is rather vague and refers only to "marketing partners" (in fact 24/7 Media), explaining however that it is only because of this arrangement that FastWeb can offer the grants search service free of charge:

> *FastWeb is able to offer its free services, in part, based on the willingness of our users to be reached by our marketing partners. By checking YES below, FastWeb may make the information you supply available to leading companies so you'll receive free information on college financing and admissions, offers and promotions designed just for students, coupons from campus bookstores, freebies and more.*
>
> ☐ *YES! I want to receive this information*
> ☐ *No, please exclude me*

The "Privacy at FastWeb" page provides some additional information on the marketing partners, explaining that these may be "data aggregators, marketers (possibly in the form of list rental) or other organizations", but, in contrast to the previous case looked at, the name of the partner is not given. The page does have the merit, however, of stating which informa-

tion will be passed on to third parties and which third parties are excluded: "(...) pornography, tobacco or other industries we find to be objectionable or potentially harmful".

> *During the registration process, FastWeb asks you whether information about you can be sent to other organizations that have products, services and opportunities useful to students and their parents. FastWeb understands how important your information is to you. Therefore, FastWeb does not share any information that can be tied to you without your permission. If you give your permission, information about you may be shared with colleges, universities, data aggregators, marketers (possibly in the form of list rental) or other organizations. This information may include, but may not be limited to name, street address, e-mail address, telephone number, or other data you provide during your visit to FastWeb. Information will not be shared with companies and organizations involved with pornography, tobacco or other industries we find to be objectionable or potentially harmful.*
>
> *You will receive e-mail periodically to notify you of additional FastWeb opportunities. If you specifically provide FastWeb with permission, you may also receive some commercial emails. You can update your personal information by clicking on the "Update Profile" link in your Message Center or on the bottom of any e-mail message you receive from FastWeb.*

Some permission marketing programmes contain boxes which are already ticked e.g. the registration forms posted on the websites of BigFoot, Dreamlife and Theglobe.com, all of whose opt-in forms are managed by 24/7 Media. It must be said that this practice is hardly in keeping with the spirit of permission marketing since it provides no guarantee that the consent is genuine – it being quite possible for visitors to skip over the relevant line without having read it. The risk then is that when such visitors subsequently receive commercial e-mail they will think it is spam, since they will have no recollection of having requested it.

All these systems and the messages generated by them naturally contain opt-out links which give subscribers a simple means of removing themselves from mailing lists. 24/7 Media reports says it receives a number of opt-out requests every day as well as inquiries from individuals wishing to know where i.e. from what site, and when their opt-in was registered or the exact nature and extent of their personal information on file. One person on the 24/7 Media team is assigned to dealing with such requests.

II.2.5) - Marketing and processing of address lists

It is the business of e-mail marketing companies to market their lists of e-mail addresses, whether these are cooperative lists or lists specific to each partner site. This marketing may be done in two different ways:

- ✓ **Brokerage**: brokerage means renting out the use of lists managed by an e-mail marketing company to advertisers, competitors or online retailers. For practical reasons, it is the company itself which

handles the use of these lists for e-mail marketing campaigns, a sort of host-mailing, very similar to the practice in conventional direct mail.

✓ **E-mail Service Bureau** (ESB): this involves the e-mail marketing company adding value to the basic mailing operation by taking charge of the different phases of the process, including dealing with returns and inquiries from customers and operating a loyalty scheme. All these companies offer this service, using CRM tools which enable them to construct the one-to-one relationship step by step. By virtue of its external growth strategy, 24/7 Media has acquired through AwardTrack a proprietary CRM application which is particularly well-suited to running incentive marketing programmes (awarding, exchanging, repurchasing and converting points or miles).

The rates charged naturally vary according to the nature and scope of the service required. A standard offering by the operator of a cooperative database comprises five services: the rental of the actual addresses, the placing of a link in the message to the advertiser's website, pushing the messages, monitoring click-throughs and measuring the success of the campaign. Rates are calculated on the same CPM basis as that used by advertising agencies, with the going rate for professional e-mail marketing currently $200 per thousand, or 20 cents per unit.

Comparative analysis of the costs of a direct marketing campaign
(source: 24/7 Media)

	Direct Mail	Opt-in Email
Design	$2,500	$2,500
Print	$6,000	--
Fulfillment	$4,500	--
Postage	$9,500	--
List Cost	$4,500	$12,000
Total	**$27,500**	**$14,500**
Average Response Time	**6-10 weeks**	**12-48 hours**

24/7 Media applies these basic rates but allows a rebate of $20 per thousand for members of the Mail Alliance i.e. client sites which also collect addresses. This price obviously does not compare with the rates quoted by the spam-friendly hard-discounters, who charge $5 per thousand (32). The above table shows clearly how the cost of an e-mail marketing campaign is nonetheless very competitive compared to a traditional direct mail campaign which is about twice as expensive and takes five times as long to execute.

32) Cf. page 35

Higher charges apply for additional selection criteria: by domain name or geographical region, by socio-demographic feature (gender / age group / marital status / number of children), by income bracket, by position held in an organisation, by educational standard or by interests. There appears to be no limit to the degree of precision that can be achieved in terms of personal interests criteria, but ultimately these do not more than reflect the precision of the information gathered from the registration forms (33). NetCreations claims to be able to segment its 6 million addresses into over 3,000 different categories. 24/7 Media's Mail Alliance database contains 35 fields of declared information and over 260 fields of additional information generated by data processing techniques about which the interviewees were very secretive. From the standpoint of data protection, some record attributes are undoubtedly sensitive in that they allow identification – while remaining within the scope of the permission granted – of ethnic groups, religious groups, smokers, diabetics or cancer sufferers. The lists of e-mail addresses also include behavioural information which has a high added value, particularly data relating to online purchases over the previous 1 month, 3 month, 6 month or 12 month periods. In many instances, this information is not obtained directly from the data subject but passed on to the e-mail marketing company by the online store where the purchase was made.

For each additional selection criterion and narrowing down of the target audience a higher rate per thousand is charged. The more sophisticated the selection criteria specified the higher the price. The most highly prized – and most expensive – criterion is propensity to shop online. The rates charged by 24/7 Media are as follows:

---

33) The FastWeb site's student grant application form, for example, collects remarkably detailed information on various sensitive topics such as medical conditions (*AIDS related, Amputee, Arthritis, Asthma, Attention Deficit Disorders –ADD, Blind Visually/impaired, Blood-Bleeding disorders, Cancer, Cerebral Palsy, Cystic Fibrosis, Dyslexia, Emotional, Epileptic, Hearing, Learning disabilities, Multiple Sclerosis, Neurological disorders, Primary Immune Deficiency Disease, Respiratory, Speech Impairment);* FastWeb is also interested in students' religious beliefs *(Assembly Of God, Baha'i, Baptist, Buddhism, Byzantine Rite, Catholic, Christian, Christian Science, Church of Brethren, Church of Christ, Congregational Christian Churches, Disciple of Christ, Eastern Orthodox, Episcopal, Evangelical Covenant, Evangelical Lutheran, Free Methodist Church, Free Will Baptist, Greek Orthodox, Hindi, Islam, Jehovah's Witness, Jewish, Judeo-Christian, Lutheran, Mennonite, Methodist, Mormon, Pentecostal, Presbyterian, Protestant, Quaker, Roman Catholic, Seven Day Adventist, Sikh, Southern Baptist, Unitarian, United Church of Christ, United Methodist, United Presbyterian).*

Rates per thousand for different selection criteria in 24/7 Media's Mail Alliance database *(source: 24/7 Media)*	
State, SCF	+ $5.00
Zip	+ $5.00
Gender	+ $5.00
Age	+ $5.00
Credit Card	+ $10.00
Product Select	+ $10.00
Enhancements	+ $10.00
Lifestyle	+ $10.00
Run Charges	+ $6.00
Last 12 Month Buyers	+ $5.00
Last 6 Month Buyers	+ $10.00
Last 3 Month Buyers	+ $15.00
Last 1 Month Buyers	+ $20.00
Postal Address	+ $75.00

Finally, the e-mail marketing companies pay royalties to the websites that collect the e-mail addresses. In other words, every time an e-mail address is used, the website that supplied it receives a payment. The amount varies but it can go as high as 50% of the purchase price. These costs obviously are a major expense for the e-marketing companies. The financial figures reproduced earlier in this study (34) show that royalty payments in 1999 were $5 million at 24/7 Media, $4.5 at MessageMedia and a little over $10 million at NetCreations. Incidentally, NetCreations has devised a sophisticated system for adjudicating between collecting sites disputing ownership of the same address: the rule is that the entire commission is paid to the website whose list of e-mail addresses the client prefers. It also appears that NetCreations gives advances on revenue to a small number of websites, notably ICQ.

II.2.6) - The technology used by the e-mail marketing companies

The e-mail marketing companies are businesses in which technology and innovation play a very major role. They reveal very little about the technology they use, seeing as it is a differentiating factor in a competitive market. In broad outline, the technical architecture of their operation centres comprises three principal elements:

34) Cf. pp. 43-45.

- a DBMS (Database Management System)

  The databases are usually built using Oracle in a Unix environment. These databases form the actual repository of data from which the user can retrieve the e-mail addresses, the additional information supplied by the subject and all the other data acquired or calculated, in particular RFM data (recency, frequency, monetary amount), which enables datamining to be carried out and to determine targets on the basis of behavioural categories. The DBMSs require powerful processors. That is why, for example, NetCreations's data-processing centre is equipped with 3 clustered DEC (now Compaq) servers operating with Alpha processors.

- a push engine

  The e-mailing engines in most cases consist of a battery of between 50 and 100 Intel servers (Compaq Proliant, for example) operating in a Linux environment (Red Hat software) and linked to an Internet backbone (T1) via Cisco routers. It is these engines also that collect the returned opt-in forms completed by prospects. With this architecture, the e-mail marketing companies possess a phenomenal e-mailing capacity: 24/7 Media has the capacity to send over 10 million messages a day. In 1999 NetCreations sent out 146 million messages on behalf of direct marketing advertisers such as Dell Computer, Compaq, Ziff Davis and J. Crew. Exactis, a subsidiary of 24/7 Media, mailed 675 million messages last year for 75 major clients in the e-commerce and financial services sectors. Exactis's current sending capacity is 30 million e-mails per day, soon to be increased to 100 million e-mails per day.

- a CRM system

  The CRM system consists of servers and workstations in a network, via which all aspects of the relationship with customers can be managed, including in some cases electronic payment platforms. These systems are often combined with call centres and CTI systems. The aim obviously is to automate the dialogue as much as possible and to avoid the need to employ large numbers of staff to answer telephone calls.

All these systems must be able to operate without interruption at every hour of the day and night. They are therefore highly protected: data back-up using peer-to-peer technology (PPRC), equipment redundancy, redundancy of connections to the Internet backbones, multiples firewalls.

24/7 Media is exceptional in that it outsources its technology functions to a number of contractors, including notably Global Center in the USA for an annual fee of $500,000, PLC in the UK, UUNet in Australia and Digital Islands in Hong Kong. But with the acquisition of Exactis it is planned to perform these functions in-house with a data-processing centre to be opened shortly in Denver, Colorado. The management of 24/7 Media insist that Global Center has no access to the data and that it is bound by a confidentiality and exclusivity agreement.

MessageMedia, for its part, having hesitated between Amsterdam, Barcelona and Dublin, has just located its technical facility in the canton of Vaud (Switzerland) between Geneva and Lausanne; the choice of this location was determined by considerations of geography, infrastructure and data security. With this facility, MessageMedia can claim to be able to provide a European-based service and to avoid the uncertainties affecting flows of personal data between Europe and the United States. To date, 50 servers have been installed in this centre and this will soon be increased to 100 servers (Sun, Dell, HP). The storage capacity is 1.5 Terabytes and the centre has its own Internet backbone access. All operations originating in Europe, in particular marketing campaigns carried out on behalf of clients, will be managed from this centre. The servers will have the benefit of all the technical expertise built up by the company in the US over the last few years and will be taking over from the US-based systems. A team of 50 multi-lingual engineers and technicians will be employed in the centre this year working on R&D programmes and on customer service issues. The staff is to rise to about 100 by the end of 2001.

In terms of software, finally, all the e-marketing companies use proprietary applications developed in-house by their technical staff. NetCreations employs 11 computer staff out of a total of 40, 24/7 Media, 50 computer staff out of 470, plus the 86 computer staff employed by its Exactis subsidiary. In order to protect their rights in the software, the companies have patented some of these applications, although this has not stopped a flurry of litigation between them: a patent infringement action is pending between DoubleClick and 24/7 Media, for example, in relation to the Target-it system. A similar such action was brought in October 1998 by Exactis against EPub, a subsidiary of MessageMedia. Ten days later, MessageMedia in turn brought an action against Exactis on the same grounds.

II.3) - Which opt-in are we talking about?

The majority of professional e-mail marketing companies practise a policy of consensual marketing based on stringent requirements in relation to opt-in. However, it still has to be said that these companies are not

immune from various errors and omissions which could set them on the slippery slope to UCE. More specifically, the fact has to be faced that the opt-in approach will not kill off spam, for two main reasons. First, initiating a permission-based relationship requires conducting a campaign which to one extent or another will resemble spam. Secondly, since everybody is now jumping on the opt-in bandwagon, the risk is that the underlying principles may become a little bit diluted as a result.

II.3.1) - Is spam a prerequisite for e-mail marketing?

Stated in those terms, the question may appear somewhat provocative, but it is nonetheless relevant because the real problem for direct marketers is how to initiate the permission-based relationship and, unfortunately, the only known method of doing this is by interrupting people, catching their attention and encouraging contact using various tricks of the trade. In other words, as Seth Godin himself acknowledges, there is a great danger that permission marketing will not be able to eschew interruption marketing completely in its initial stage: "(...) But the first step is still to interrupt the consumer. That's one reason there will always be especially acceptable Interruption Marketing media. We need to get that initial attention. Sometimes you're lucky enough that a stranger comes to you of his own accord. There will always be a few people who straggle onto your Web site, for example, or potential customers who call your toll-free number or walk into your store. These are the freebies. Most of the time, however, you've got to use the tried-and-true interruptive techniques to reach large numbers of people. Using measurable techniques, marketers can choose television, radio, print, direct mail, or electronic media to grab the attention of consumers. But without some way to grab attention of a stranger, the permission process never starts" (35).

How then is a business to make itself known on the Internet? The obvious temptation is to use targeted e-mail marketing – the risk here is that the advertiser may turn to a list broker and bulk-mail millions of solicitations in the hope that out of all of this a few recipients will read the message and respond. This technique however is socially unacceptable and is contrary to the rules of conduct recommended by an increasing number of direct marketing associations who espouse the principle of "user's prior acceptance". The only acceptable method – and even then not without some qualifications – is banner advertising on websites profiled by interests and lifestyles compatible with the advertiser's products or services. Banner advertisements have links to the advertiser's website enabling visitors to click through and initiate the opt-in e-mail relationship by completing a registration form.

---

35) **Seth Godin** – op. cit. Cf. page 72

II.3.2) - The need for a restrictive interpretation of the opt-in

All major online businesses and direct marketers are now switching to an opt-in approach. Most surprisingly, this is true even of the pornographic sites, who have been among the most prolific of spammers in recent years. Thus, it is increasingly common to find in one's inbox e-mails which even a few months ago one would have immediately classified as spam preceded by the following notice: "You've received this message because while visiting a partner website, you opted in to receive special online offers and discounts" or alternatively: "This newsletter is being sent to an opt-in mailing list. This message is sent in compliance with all known local and International laws and it complies with the proposed United States Federal Requirements for commercial e-mail. WE HONOR ALL REMOVE REQUESTS: If you wish to be removed from any future mailings please send an e-mail to xxxx@mail.com We assure you that you will receive no further mailings". This immediately raises the question of the quality of consent obtained. Might advertisers – of all types – tend in future to take an unduly broad view of consent, reminiscent of what happened with affirmative action in the US?

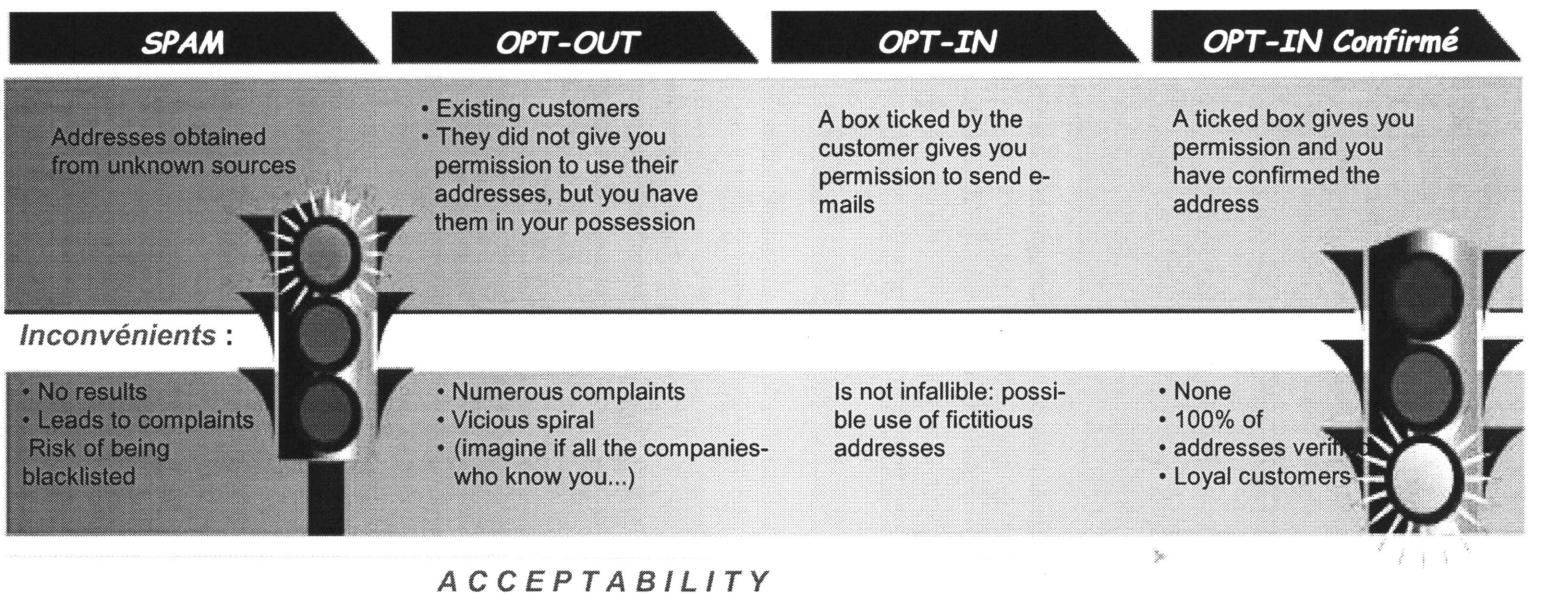
To take an extreme example, a website might have a feature allowing visitors to bookmark the site by clicking on an OK button in a dialogue box. It would be the easiest thing in the world to place some obscure small print in a terms and conditions page buried in some inaccessible corner of the website providing that the act of bookmarking the site constitutes consent to receiving e-mail advertising. To take a more innocuous example, could registering on a list of sub-aqua enthusiasts to receive advertisements for underwater equipment constitute consent to receiving brochures from every scuba diving centre in the world? In sum, the concept of opt-in needs to be looked at very closely. If it is to be effective and authentic, **the parameters of opt-in will have to be defined**. It will also be necessary to reflect on the concept of "partner". Websites frequently mention that their "partners" may make related commercial offers to a visitor registering in a mailing list. What is a partner? Do the partners' offers meet the standards which the collecting site has committed itself to upholding? What sort of control is there over the partner? The truth is that one rarely finds answers to these questions. However there is one interesting provision contained in MessageMedia's "Ten Rules for Permission-based E-mail Marketing" which requires that the addressee must be informed of the identity of the company hosting and vouching for the commercial e-mail (36). It would be well if this practice were to become the standard.

---

36) Cf. Annex 1: Anti-Spam policies – Ten Rules for Permission-based E-mail marketing: *"(...) make sure you control the mailings, and that your brand "introduces" other brands. Example: "Because you opted to receive promotional offers of our valued partners, we at ABC Corp are please to give you a special offer from XYZ Corp."*

From Spam to Double Opt-In

(Source: MessageMedia)



In order to differentiate themselves from the spammers and to eliminate them from the market, the e-mail marketing companies have adopted strict and unequivocal anti-spam policies by which, for example, they undertake to state the exact origin of the recipient's opt-in in the message header. This rule is applied by Exactis (37) and NetCreations, among others. MessageMedia, for its part, has devised an interesting approach based on the computer graphic shown on the preceding page and which it uses as a training tool in customer relations: the chart defines the level of acceptability of commercial mailings according to the level of permission granted by the customer and shows clearly that the fact of having had a prior business relationship is not sufficient to authorise the sending of commercial offers. What MessageMedia has done is to take the RFM (recency, frequency and monetary amount) behavioural analysis model used by marketers and transpose it into the context of opt-in e-mail marketing. Consider the case of a web surfer who happens to buy a tie for $39.50 on the jcrew.com site: this does not give J. Crew the right to e-mail this small customer several times a week, even with a special promotional offer for natural silk ties. Some of the leading players in e-commerce, such as Amazon, Barnes & Noble, CD Now and Travelocity, would do well to reconsider some of their practices in this regard especially with respect to occasional customers.

On a practical level, this policy has led the e-mail marketing companies to be very demanding with respect to the quality of their opt-in e-mail lists. Very often, clients who come to them with their own lists will be asked about the context in which the opt-ins were obtained. Where doubts remain, the companies have adopted a practice of testing the quality of the opt-ins on a small sample of addressees. If the tests provoke negative reactions on the part of recipients, the campaign is postponed and the list is purged of all the addresses with doubtful opt-ins.

37) Cf. Annex 1: Anti-Spam policies – and specifically the anti-spam policy of Exactis (3- Additional Principles – Cf. 131)

Conclusions of Part One

The conclusion to be drawn from this first part is that there are three major risks entailed in the growth of e-mail marketing: one is of a policy nature and concerns the sterile dichotomy between opt-in and opt-out, which has become the focal point for the policy debate in EU member states over online commercial communications. The second is of a sociological nature and concerns the individual's progressive loss of control over his own identity due to the processing of personal data being carried out on a massive scale by the e-marketing industry. The third is of an industrial nature and concerns the prospect of Internet entropy in the not-too-distant future if decisive regulatory action is not taken. This risk is also a financial one, with part of the cost being borne by the Internet users.

The focus on the opt-in/opt-out alternative reflects two different approaches to the issue of when it is permissible to send Internet users commercial e-mail. Both approaches are calculated to protect individuals' privacy but to different degrees. For countries which have announced their intention of having a high level of data protection, it is difficult to see the advantage in stopping at the minimum standard of the opt-out, unless it is to placate backward-looking industry interests and to shore up business practices which with the advent of consensual marketing now belong firmly in the past. To portray the opt-out approach as a compromise between privacy protection and free enterprise is a gross distortion. To use a somewhat fanciful analogy, the opt-out approach amounts to giving the e-mail user a sponge to mop up a flood of commercial messages which will never run dry (or to mop the sweat from his brow, perhaps) while the opt-in approach gives him access to the source and allows him to control the level of the flow. As for free enterprise, it is hard to imagine that any legislator would wish to sacrifice citizens' privacy in the name of free enterprise. In the final analysis, the opt-in/opt-out debate merely re-opens an issue which had already been resolved by the general directive of October 1995, which very clearly establishes two basic rights: first, the right to observance of the principle of finality, whereby disclosure of an e-mail address either in a discussion forum or directly to a merchant in a given context under no circumstances whatsoever authorises the use of the address in any other context or for any other purpose; and, secondly, the right of the individual to object *ex ante*. By allowing the recipient to register his objection only after the event i.e. after the initial prejudice has been suffered, the opt-out approach deprives Internet users of their rights over their own mailboxes. This approach is thus contrary to the general directive.

In general, the processing of marketing data engenders a loss of control by the individual over his own identity. This is because the whole point of marketing engineering is to accumulate maximum data on prospects in order to target advertising campaigns and promotional offers as precisely as possible. This is true also of e-mail marketing. There appears to be a direct correlation between the quality of the data used in a campaign and the sales conversion ratio. This correlation leads all marketers to build up vast repositories of data and to use profiling techniques in order to reduce to a minimum the degree of uncertainty regarding the response of consumers to the offers sent to their mailboxes. To do so, they need to accumulate as many different categories of personal data as they can. Therefore, website operators are unlikely to stop at the data knowingly submitted by a visitor on an electronic form, however detailed that information may be. Where, for example, it is possible to find out the general shopping habits of an Internet user, every marketer will regard that as must-have information. Thus personal data are refined by successive matchings and enhancements, and composite identities are created by the addition of various bits and pieces of information: data submitted by the subject to various parties, items revealed involuntarily when surfing the Internet, purchase records, opinions expressed in public areas etc. Thus each individual has a virtual double and the questions everyone will be unconsciously asking himself are what is the architecture of this double, does it correspond to one's image of oneself or to the image one wishes to portray to others? Even where this double is nothing more than the sum of opt-in data, is the individual profile generated by data enhancement techniques necessarily consensual and permitted? The real issue of online privacy protection is the issue raised by these questions. The requirement of opt-in for mailing lists or commercial e-mail represents a means by which the individual can control his double and shape it to some extent, but it is far from sufficient and the fact must be recognised that the individual will never be fully in control of the arcane processes to which his personal data are subjected.

Finally, let us make some projections of volumes and costs. There are currently 234 million Internet users worldwide and this figure is likely to reach 300 million by the end of 2000. If it is assumed that sooner or later every e-mail marketer will acquire the technical capacity to transmit 100 million e-mails daily, Internet users could potentially be overwhelmed by the resulting flood of messages – 200 senders with that sort of capacity could mean 20 billion commercial e-mails being sent every day. Every web surfer would receive an average of over 60 e-mails a day, representing a total download time of approximately 1 hour with current technology. And this is without taking account of the increasing use of photographic and video content in commercial e-mails. Is there not a real risk of Internet entropy if steps are not taken expeditiously to introduce the necessary degree of regulation? An extremely rigorous interpretation of the opt-in concept would appear vital to the system's survival.

Regarding the financial burden borne by web surfers, consider the following calculations and projections. Assuming that an average Internet user paying a flat-rate fee of €12 a month for 10 hours connection time (including telephone calls) and using standard equipment (without a broadband connection) can

download messages at a rate of about 180 K/bits per minute, the cost of downloading just 15 or so messages a day totalling between 500 and 800 K/bits in size could be as high as €30 a year. If this is multiplied by the number of Internet users in a given country, the overall cost becomes very substantial indeed. Or on a world scale, assuming a worldwide online community of 400 million, the global cost of downloading advertising messages using current technology may be conservatively estimated at €10 billion – and that is just the portion of the cost borne by the web surfers themselves.

The second issue is that of the time spent by e-mail users sorting the commercial messages from the personal or business messages they wish to read and process. It is not a matter of simply clicking on the mouse to delete the unsolicited messages, first one has to satisfy oneself as to the nature of each message and this is where the difficulty lies. Who has not at one time or another deleted an important message after mistaking it for an advertisement? Of course, this problem also arises in the case of letters delivered by post. The time needed to determine the nature of a message may be quite significant, something like 3 or 4 seconds, in the estimation of A Schwartz and Simson Garfinkel (38), "(...) but those seconds add up quickly: one million people clicking Delete corresponds to roughly a month of wasted human activity. Or put another way, if you get six spam messages a day, you're wasting two hours each year deleting spam." (39).

It would be idle speculation to attempt to quantify the cost of all this waste of the time of private individuals. But the question is very relevant in the case of employees. Workplace e-mail addresses are not immune from e-marketing campaigns and employers may well wonder as to the cost to their companies of the time spent by employees checking their mail and regularly purging their inboxes of all the advertising messages they receive. It should not be forgotten that one of the great successes of Internet technology, which has gone largely unnoticed, is to enable advertising to be delivered right to the desks of tens of millions of working people.

---

38) Op.cit.
39) Ibid. page 5

Part Two:
What Protection in Europe ?

Chapter III: The legal framework for unsolicited commercial e-mail in Europe

It may appear somewhat paradoxical to devote this first chapter to the legal framework for data privacy in relation to unsolicited commercial communications and to entitle this Part "What Protection in Europe ?". However, this will not interrupt the analysis, which is resumed in the next chapter.

The purpose is to show how the four successive stages in the establishment of the legal framework currently applicable to unsolicited commercial communications took place in the context of debates which are reflected differently in each of the directives concerned but which nonetheless follow the same rationale.

Accordingly, it is necessary to look at this series of directives and their specific provisions prior to embarking on an analysis, in order to illustrate the existing legislative context for the recent Commission Proposal for a Directive concerning the processing of personal data and the protection of privacy in the electronic communications sector. This proposal takes on board some pioneering developments in relation to unsolicited commercial advertising (COM[2000] 385, 12 July 2000).

The recent initiative of the European Commission puts the findings drawn from these investigations into perspective. It opportunely re-opens a debate which appeared to have been closed recently with the adoption of Directive 2000/31/EC on electronic commerce. The need for this initiative and its likely effects will be analysed here in the light of the legal framework which preceded it.

There is no doubt that this Commission initiative considerably augments the relevance of the question which this part of the study attempts to answer.

III.1) - The general principles laid down by Directive 95/46/EC (40)

It is not in dispute that an e-mail address constitutes personal data for the purposes of all data protection legislation both at national and Community level, in particular Article 2(a) of the Directive of 24 October 1995 (41), as in many cases it enables the surname, first name and/or the work address of its owner to be identified and in all cases relates to a natural person.

Needless to say, even in countries such as the United States, which have no general data protection legislation, an e-mail address comes within the private sphere and is covered by the right to be left alone.

Directive 95/46 of 24 October 1995, which was to be transposed into national law by the Member States before the 25 October 1998, provides, in Articles 6, 7, 10, 11 and 14, that personal data may not be processed unless they are collected and processed fairly and for specified and legitimate purposes.

Article 7 sets out the conditions under which personal data may lawfully be processed.

Two of these conditions can apply to e-mail marketing: the condition laid down in Article 7(a), whereby processing is legitimate if the data subject has unambiguously given his consent, and the condition laid down in Article 7(f) that the processing "is necessary for the purposes of the legitimate interests pursued by the controller except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject".

Article 6.1(a) establishes the principle that data must be collected and processed fairly.

Article 10 provides that in the case of data collected from the data subject directly, the data subject must be informed about the purpose for which the data are being gathered, the recipients of the data, whether replies to the questions are obligatory or voluntary and the existence of the right of access to and the right to rectify the data concerning him.

---

40) 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.

41) Directive 95/46/EC of 24 October 1995, Article 2 (a): "Definitions: For the purposes of this Directive: 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity".

Article 11 provides that where the data have not been obtained from the data subject directly, the controller must inform the data subject of the data collection at the time of recording the personal data or, if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed.

Finally, article 14 provides two rights to object in relation to different situations. First, data subjects may object, on request and free of charge, to the processing of personal data relating to them for the purposes of direct marketing. Secondly, data subjects must be informed by the processing controller that their data are liable to be disclosed to third parties. This must be done prior to the disclosure of the data. The data subjects may then, if they wish, object to such disclosure of their data to third parties.

III.2) - Application of these principles to the field of telecommunications by Directive 97/66/EC (42)

Directive 97/66/EC of 15 December 1997 concerning the protection of personal data in the telecommunications sector, which was to be transposed into national law by the Member States of the European Union before 25 October 1998, does not explicitly mention commercial communications by e-mail.

It does however cover two direct marketing techniques in Article 12.

First, Directive 97/66/EC provides that "the use of automated calling systems without human intervention (automatic calling machine) or facsimile machines (fax) for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent". Suffice it for now to observe that the description "automated calling systems without human intervention" is very close, if not identical, to a description of direct marketing by e-mail.

Secondly, it provides that, in relation to other telemarketing techniques, Member States shall "take appropriate measures to ensure that, free of charge, unsolicited calls for purposes of direct marketing [...] are not allowed either without the consent of the subscribers concerned or in respect of subscribers who do not wish to receive these calls, the choice between these options to be determined by national legislation".

Admittedly, this directive does not explicitly mention e-mail marketing.

---

42) 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.

However, it should be pointed out that to date five Member States have adopted a rule of mandatory prior consent to the sending of unsolicited commercial communications. Four of them, Austria, Denmark, Finland and Italy opted to include e-mail marketing in their national legislation transposing Directive 97/66/EC among the direct marketing techniques without human intervention which cannot be used without the prior consent of the subjects.

In the case of Austria, the entry into force in August 1999 of section 101 of the Telecommunications Regulation Act (Austrian Official Gazette n° 100/1997) requires the prior consent of direct marketing recipients where automated calling systems, fax or bulk e-mail are used for commercial purposes. Section 104 provides for heavy penalties, of up to 500,000 Austrian schillings (€36,336).

In Denmark, Act n° 418 of 31 May 2000 transposed Directive 97/66/EC. Article 12 of the directive is implemented by way of an amendment of the Marketing Act which is codified by Act n° 699 of 17 July 2000. This provides expressly that the use of e-mail, automated calling systems or fax machines for unsolicited marketing purposes is unlawful in the absence of the recipient's prior consent.

Incidentally, as far as other direct marketing techniques are concerned, the Danish legislation establishes a public opt-out register which must be consulted on a quarterly basis.

In Finland, Act 1999/565 of 22 April 1999 on the protection of personal data in the telecommunications sector, which transposes Directive 97/66/EC of 15 December 1997 into Finnish law, provides in Article 21 (telecommunications and direct marketing) that prior consent is required for the use of automated calling systems and fax machines for purposes of direct marketing. The Act also empowers the Finnish Telecommunications Minister to require prior consent in relation to other media used for direct marketing, including e-mail, taking into account the functionality and security of the media concerned. Finally, the Act provides that direct marketing directed at consumers comes under the provisions of the Consumer Protection Act 1978/38.

The Finnish Telecommunications Minister recently exercised the power conferred under the Act to extend its provisions to other media by introducing an opt-in requirement for e-mail marketing at the end of 2000. Moreover, in October 2000, the Finnish direct marketing federation adopted a code of conduct making direct marketing by e-mail subject to an opt-in requirement.

In Italy (43), implementing decree n° 171 of 13 May 1998, which transposes Directive 97/66/EC into national law, refers to the concept of consent laid down in Articles 11 to 13 of the Italian Data Protection Act n° 675 of 31 December 1996 (which is similar to Directive 95/46/EC) and provides that the data subject's consent is required prior to the sending of unsolicited advertising messages by automatic calling systems, including e-mail. In the case of other direct marketing media, recipients must be informed that they have the right to object to receiving such marketing messages.

Germany also has an opt-in requirement, but its legal basis is not the legislation transposing Directive 97/66/EC, but case-law developed in relation to other German legislation (see section IV.2.2 below).

III.3) - Consumer protection in distant selling contracts

Directive 97/7/EC of 20 May 1997 (44), which was to be transposed by Member States into their national law before 21 May 2000, also distinguishes, in Article 10 (Restrictions on the use of certain means of distance communication), between different types of medium in terms of the protection offered to data subjects.

It provides, first, that the use of automated calling systems without human intervention (automatic calling machines) and facsimile machines (fax) requires the prior consent of the consumer.

Secondly, it requires Member States to ensure that means of distance communication, other than those referred to above may be used only where there is no clear objection from the consumer. These means explicitly include e-mail.

III.4) - Directive 2000/31/EC on electronic commerce

The recent Directive 2000/31/EC of 8 June 2000 (45),which has to be transposed into national law by Member States before 17 January 2002, has given rise to a very wide range of interpretations as to its precise

---

43) English translations available at http://www.garanteprivacy.it or www.dataprotection.org

44) 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. This Directive was to have been transposed into Member States' national legislation by 21 May 2000.

45) 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 (electronic commerce directive – OJ L. 178 of 17 July 2000).

scope and as to its binding nature or otherwise, giving rise to a confusion which is detrimental to e-commerce merchants and Internet users alike.

III.4.1) - The objectives set out by the Community legislator

From a strictly legal viewpoint, exceptional precautions were taken in the preamble to Directive 2000/31/EC to prevent it interfering with the existing Community legislation on the protection of personal data (Directives 95/46/EC and 97/66/EC) and the protection of consumers in relation to distance contracts (Directive 97/7/EC). These precautions reflect the difficulties that arise when attempting to combine general legislation with sectoral legislation.

Thus, the directive is designed both to address specific legal issues (recital 6) and to lay down a general framework for electronic commerce (recital 7).

Moreover, it seeks at the same time to ensure a high level of consumer protection (recital 10) and to complement the information requirements laid down by Directive 97/7/EC (recital 11), while stating that it does not affect existing Community legislation on consumer protection (recital 11).

It then notes that the protection of individuals with regard to the processing of personal data is solely governed by Directives 95/46/EC and 97/66/EC (recital 14), which are applicable to information society services including commercial communications by e-mail, while introducing new provisions for transparency in relation to e-mail marketing and for the filtering of unsolicited commercial communications using opt-out registers (recital 18).

Lastly, Directive 2000/31/EC does not apply to service providers established outside the European Union but aims to be consistent with international rules (recital 58). It does not intend to prejudice the future results of current discussions within WTO, OECD and Uncitral but to constitute a common negotiating position in international forums (recital 59). Recital 60 expresses the aspiration that Directive 2000/31/EC will contribute to a legal framework which is clear and simple, predictable, and consistent with the rules applicable at international level.

III.4.2) - The system envisaged by the Community legislator

Directive 2000/31/EC lays down, in Article 7, two technical requirements for the sending of unsolicited electronic mail.

Article 7(1) provides that in addition to other requirements established by Community law, "Member States which permit unsolicited commercial communication by electronic mail shall ensure that such commercial communication by a service provider established in their territory shall be identifiable clearly and unambiguously as such as soon as it is received by the recipient".

Article 7(2) provides that "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".

Contrary to the stated intention of the Community legislator, Directive 2000/31/EC is – unfortunately – not silent as to the nature of the safeguards which are to be required, in that by making a specific reference to opt-out registers it implicitly – but nonetheless automatically – promotes the concept of a mere right to opt out of receiving unsolicited commercial communications.

III.4.3) - The ambiguity of the e-commerce directive: a source of legal uncertainty

Article 7(1) of the directive expressly refers to the option left to Member States by existing Community legislation to prohibit unsolicited commercial e-mail. Where such a prohibition is not introduced, the commercial nature of the message must be immediately identifiable by the recipient.

Article 7(2), however, mentions neither the possibility of Member States prohibiting unsolicited commercial communications nor the possibility of Member States imposing a requirement of the recipient's prior consent for the sending of such messages. By thus confining itself to laying down an obligation – to be introduced by all Member States – of regular consultation of opt-out registers, Directive 2000/31/EC promotes a technical measure the only purpose of which is to implement an opt-out approach.

Since the first version of the proposal for an electronic commerce directive was published, on 18 October 1998, the issue of the safeguards to be put in place for Internet users has given rise to a sometimes heated debate between the supporters of prior consent (opt-in) and those advocating a mere right to object (opt-out) to receiving unsolicited commercial e-mail.

This debate, which the proposal for a directive was never intended to resolve, saw heavy involvement on the part of national and European online industry organisations, ISPs, associations of consumers and Internet users, Member States and national data protection authorities.

When the final draft of the directive was agreed, even the most radical voices on both sides were unanimous in the view, as conveyed by the media, that the directive had come down clearly in favour of an opt-out regime. It must be said that the media reporting of this view largely ignored the intention stated in the preamble to the directive not to modify the basic rights already enjoyed by Internet users in Europe.

The interviews and consultations carried out for the purposes of this study confirm that both supporters and opponents of an opt-out approach are convinced that Directive 2000/31/EC favours that solution.

This belief, whether one shares it or not, is a fact which is essential to a proper understanding of the current situation in Europe concerning the public or private regulation of unsolicited commercial e-mail.

The opt-out right envisaged by the directive, to be implemented by means of national or international registers under the control of the Member States, is a blunt, undiscriminating instrument. It may be exercised by any Internet user, European or non-European alike. It must be honoured by all European providers of information society services, regardless of any previous links which may exist between an Internet user and a particular service provider. Yet such relationships are very diverse in terms of their origin: visit to a website, subscription to a free service, single contact with the company, previous transactions – or no prior link of any kind.

Prior to the adoption of Directive 2000/31/EC, the right to opt out could apply only in respect of a relationship between a particular individual and a particular service provider. Under Article 14 of Directive 95/46/EC, the right to object to receiving commercial communications may be exercised against (and must be offered by) the party who directly collected the e-mail address. Article 14 contemplates two different possibilities: an objection to receiving commercial e-mails from the party who collected the e-mail address and an objection to receiving such e-mails from third parties following the disclosure of the e-mail address to such third parties. Directive 2000/31/EC introduces a right to opt out from receiving commercial e-mails from all service providers established in Europe, without requiring that the collecting party or the third party advertiser be informed as to the exercise of the right of objection.

Finally, the electronic commerce directive does not require the opt-out registers to be systematically consulted prior to the sending of any

message but merely that they be consulted “regularly”. This again is a source of ambiguity. “Regular” consultation does not mean prior or systematic consultation.

Chapter IV: The Spamming phenomenon has not yet invaded Europe

IV.1) - A European reaction to American privacy issues

Two big issues relating to privacy protection on the Internet which have emerged in the United States over the last five years.

These were not the publication on the Web of details of President Clinton's relationship with Monica Lewinsky or the posting of the names and addresses of doctors who perform abortions, in order to "prepare the trial of the greatest crime against humanity".

The two issues are in fact the controversy surrounding the commercial use of "cookie" files, which erupted in 1994, and the practice of sending unsolicited commercial bulk e-mail, which hit the headlines in 1996. For Americans, these two issues have focused attention on what limits should be placed by society on unpopular commercial practices.

In the case of cookies, the response was one of self-regulation. Under pressure from American family and consumer associations, the IETF (46) adopted technical measures which enable users to prevent cookies being stored on their computers, on a one-time or permanent basis. While the level of awareness among users of this possibility is still low, it must be acknowledged that, technically, this right is available to Internet users worldwide thanks to the work of the IETF.

Thus, even if from a strictly legal viewpoint, cookies do not necessarily process personal data within the meaning of Article 2 of the 1995 directive (47), there is certainly reason to be pleased that even in the absence of a general data protection law in the United States and despite the broad American interpretation of the concept of privacy, US Internet users succeeded in pressurising American software manufacturers into introducing the opt-out solution demanded by the market, which is now enjoyed by users of browser applications the world over.

---

46) IETF: Internet Engineering Task Force, the international body which standardises the technical protocols of the Internet.
47) See above, section III.1, footnote 39.

Spam, on the other hand, is perceived as a legal issue, both in the US and in Europe.

In the United States, one of the economic explanations for this approach is that American Internet access and e-mail providers did not want to have to bear indefinitely the technical and commercial burden of the inconvenience caused by spam and for want of an effective technical remedy turned to the legislators for help. The second common explanation is pressure of public opinion, responding to the scale of the phenomenon as reported by the media and denounced by American privacy advocates.

In Europe, it was natural for the spam issue to be addressed from a legal perspective. This is because the relevant law was in place before the phenomenon ever emerged in Europe.

It was not a question in Europe of drawing up new legislation to deal with a new phenomenon which was not captured by the existing laws. What had to be done was to identify the legal characteristics of spam to determine whether the existing law would have to be amended or extended in order to deal with the phenomenon or whether it would have to be repealed because it was unsuited to the practices employed on the Internet.

It was in 1997 that the European media began to provide heavy coverage of the nature and extent of the spam phenomenon in the United States, giving rise to fears of its spreading to Europe.

This imminent threat rekindled the legal debate in Europe during the two years of discussion of the electronic commerce directive. This debate had already been carried on during the discussion of Directive 97/66/EC of 15 December 1997 concerning the protection of privacy in the telecommunications sector, Directive 97/7/EC of 20 May 1997 on the protection of consumers in respect of distance contracts and, two years previously, during the discussion of Directive 95/46/EC of 24 October 1995 harmonising general data protection principles in Europe.

However, the research conducted for this study reveal that Europe has not yet experienced an acute outbreak of unsolicited commercial e-mail or of spam.

IV.2) - Much debate but little in the way of conflict

IV.2.1) - The national data protection authorities and spam

It must be observed that almost all of the national data protection authorities throughout the European Union report that they have not yet had to deal with any complaints concerning cases of blatant spamming. It must also be observed that where the authorities have intervened in cases of unsolicited commercial e-mail, the situation has generally been resolved amicably. However, there is one decision which merits attention and analysis.

- ***A heavy fine imposed in Spain***

  In Spain, the supervisory authority handed down a decision imposing a heavy fine on a company responsible for several unsolicited commercial e-mails.

  The facts of the case were as follows.

  A company which had received numerous e-mails as a result of a protest campaign by Internet users against the national operator Telefonica, had systematically incorporated into its own marketing database the e-mail addresses of the Internet users who had written to it together with the e-mail addresses specified in the "copy to" field (Cc:).

  One individual who had been copied an e-mail message sent to this company had shortly afterwards received an e-mail from the company advertising computer products. The recipient immediately contacted the company requesting the immediate removal of his e-mail address from the company's mailing list.

  He subsequently received a new e-mail from the same company. This second message was considered "threatening" by the Spanish Data Protection Agency.

  In its decision, which is currently under appeal to the Spanish courts, the Spanish Data Protection Agency dismissed all the arguments put forward by the company in its defence. It ruled that an individual's e-mail address constitutes personal data and it rejected the argument that e-mail addresses were in the public domain and hence capable of being used without restriction. On this point, the Agency stated that a company which obtains an e-mail address must make sure that the individual concerned has given his consent to its use for commercial purposes.

As the company in this case was unable to show that it had obtained the consent of the individual concerned, the Agency held that it had committed a "serious violation" within the meaning of the Spanish Data Protection Act and imposed a fine of 10,000,001 Pesetas (approximately €60,100). It should be remembered that this decision is not final as an appeal is pending. This prevents the identity of the defendant company being revealed.

- ***An in-depth report in France***

In France, the CNIL adopted a report on 14 October 1999 containing a legal and practical analysis of direct marketing by e-mail. The report was circulated to the CNIL's European colleagues in the framework of the data protection working party established by Article 29 of Directive 95/46/EC.

The CNIL's key statement is that "the sending of electronic messages [...] entails the prior collection of e-mail addresses", which "constitute personal data".

"The manner in which e-mail addresses are collected on the Internet must be in conformity with the rules laid down by data protection legislation and with the rights of the persons concerned".

"The automated collection for marketing purposes of e-mail addresses from public areas on the Internet is subject to the requirement laid down by the general Directive 95/46/EC of the "unambiguous consent" of the persons concerned".

The CNIL concludes from this analysis that it is not possible to address the phenomenon of spam or unsolicited commercial e-mail without differentiating on the basis of the relationship that exists between a particular advertiser and an Internet user. Thus, the CNIL appears to acknowledge that under certain conditions merchants may send commercial e-mail to an Internet user who did not solicit it where the individual in question has had prior contact with that merchant (visit to its website, previous contact, purchase etc.).

On the other hand, the CNIL is strongly of the view that e-mail addresses may under no circumstances be collected from the public areas of the Internet (websites, newsgroups, public mailing lists).

- ***The opinion of the Article 29 Working Party***

The national data protection authorities constituting the data protection working party established by Article 29 of Directive 95/46/EC of 24 October 1995 adopted an Opinion on 3 February

2000 (48) on the issue of unsolicited commercial e-mail with specific reference to the European legal framework applicable to spam.

First, the members of the Working Party noted that the Community's data protection legislation extends to the domain of electronic commerce and that the issues raised by e-mail marketing can be resolved in the light of the general principles enshrined in Directives 95/46/EC and 97/66/EC.

Secondly, the Working Party pointed out that the technical measures provided for in Directive 2000/31/EC do not in any way derogate from the application of the principles whereby data must be collected fairly and data subjects informed of the purpose for which the data will be used and of their right to object to the data being used for commercial purposes or disclosed to third parties.

Thirdly, the Working Party was of the view that the collection of e-mail addresses from public spaces on the Internet is a flagrant breach of the principles of fair collection (Article 6.1(a) of Directive 95/46/EC), finality (Article 6.1(b)) (49),and legitimate processing (Article 7(f)) (50).

This opinion was issued during the course of the legal debate surrounding the discussion of Directive 2000/31/EC on electronic commerce. It deserves careful consideration despite the fact that it was presented as a provisional position pending further examination of anti-spam software techniques. It constitutes a stable and common analysis of European data protection legislation on a "like-for-like" basis and it rightly draws attention to the technical rather than exhaustive nature of the provisions of Directive 2000/31/EC.

Finally, the Article 29 Working Party, in an exhaustive working paper on respect for privacy, adopted on 21 November 2000 (51), again referred to the definition of spam adopted by the French authority in its October 1999 report on direct marketing by e-mail and reaffirmed the Working Party's Opinion 1/2000 of 3 February 2000 (see above, footnote 48) and the clear applicability of the

---

48) See http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm: Opinion 1/2000 of 3 February 2000 on certain data protection aspects of electronic commerce.

49) Article 6 of Directive 95/46/EC: "1. Member States shall provide that personal data must be: (a) processed fairly and lawfully; (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes [...]"

50) Article 7(f) of Directive 95/46/EC: "Member States shall provide that personal data may be processed only if [...] processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject."

51) See http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/

provisions of Directive 95/46/EC and in particular Articles 6(1)(a), 6(1)(b), 7(f), 10, 12 and 14. Noting that direct marketing by e-mail accounts for 10% of all e-mails sent, according to a recent study (52), the Article 29 Working Party mentions, as techniques liable to enhance privacy protection, the filtering out of unwanted e-mails and the use of anonymous e-mail, in which messages are routed through a remailer service.

IV.2.2) - The courts of the Member States and spam

The research carried out for the purposes of this study reveals that by and large Member States' courts have not had to consider cases concerning spam or unsolicited commercial e-mail. There are two exceptions: Spain, in respect of the dispute described above (see II.2.1), and Germany, as will now be described.

The data protection commissioner for the Land of Berlin, Mr Hans-Jürgen Garstka, reports that the German lower courts have, since December 1997, extended to unsolicited e-mail the case-law (53) which they had previously developed in relation to marketing by fax and telephone.

These courts take the view that unsolicited marketing practices constitute unfair competition in the light of the settled case-law developed on the basis of the Unfair Competition Act of 7 June 1909.

Thus, even though the legal basis of these decisions is not the protection of privacy and personal data, unsolicited commercial e-mail has already been punished on several occasions by the German courts.

In relation to the law in Germany, it may be noted at this point that the Federal Telecommunications Act of 31 July 1996 (54), the Information and Communication Services Act of 13 June 1997 (55) and the Fed-

---

52) See Hagel III J. & Singer M. "Net Worth : the emerging role of the informediary in the race for customer information", Harvard Business School Press, 1999, p. 275.

53) Since 1970, the German Federal Supreme Court has taken the view that unsolicited telemarketing practices are contrary to a law of 7 June 1909 on unfair trading and in breach of Article 823 of the German Civil Code. This case-law was extended to unsolicited marketing by fax and by the Federal electronic messaging service (Bundesgerichtshof (BGH) decision of 25 October 1995, I ZR 255/93 – LG Munchen II). More recently, some lower courts have extended this case-law to unsolicited marketing by e-mail (Landgericht Traunstein, 18 December 1997, 2 HKO 3755/97; Landgericht Berlin, 13 October 1998, 16 O 320/98; Landgericht Ellwangen, 27 August 1999, 2 KfH O 5/99.)

54) Available in English translation at http://www.datenschutz-berlin.de/gesetze/tkg/tkge.htm#p89, in particular Article 89(7).

55) Act of 13 June 1997, **Federal Law Gazette I, 1997, issue 52, p 1870)**. Available in English translation at http://www.datenschutz-berlin.de/recht/de/rv/tk_med/iukdg_en.htm#a2.

eral Media Services Treaty of 23 June 1997 (56) all require telecommunications operators and suppliers of teleservices and media services to obtain the prior consent of subscribers or customers as a condition of the use or commercial disclosure of their data. Where the marketer is not a telecommunications operator or a supplier of teleservices or media services, the requirement of prior consent applies in any event as a consequence of the German courts' interpretation of the Unfair Competition Act of 1909.

There are two factors explaining the absence of litigation in the other countries of the European Union.

First, the fact that the transposition deadlines for Directives 97/66/EC (25 October 1998) and 97/7/EC (1 June 2000) are still comparatively recent together with the delay in transposing the directives on the part of a number of Member States have meant that victims of spamming in Europe have not had the legal remedies available to them nor would it naturally occur to them to go to the courts to seek redress for fraudulent marketing.

Secondly, the spontaneous response of Internet users who have suffered from spam is to complain to their ISP: it appears to be the case that the inconvenience caused by unsolicited commercial e-mail at present is not perceived as being sufficiently serious to warrant taking legal proceedings in order to bring it to an end.

IV.3) - Consensus and caution of the industry

IV.3.1) - The existing position

- ***Broad anti-spam consensus in the industry***

  FEDMA (57) (Federation of European Direct Marketing), refers to the definition of spam adopted by the French CNIL in its report on direct marketing e-mail of 14 October 1999 (58) and expresses the view that "spamming must be combated".

  According to the definition drawn up by the CNIL, which was broadly followed by the Data Protection Working Party established by Article 29 of Directive 95/46/EC in its Opinion 1/2000 of 3 Feb-

56) Federal Treaty on Media Services of 23 June 1997, available (in German) at http://www.datenschutz-berlin.de/recht/de/stv/mdstv.htm#nr14
57) See http://www.fedma.org
58) Available (in French) at http://www.cnil.fr/thematic/index.htm

ruary 2000 (see above, footnote 45), spamming is "the practice of sending unsolicited emails, usually of a commercial nature, in large numbers to individuals with whom the sender has had no previous contact and whose e-mail addresses have been collected in a public space on the Internet: mailing lists, directories, websites etc.".

Almost every European distance selling trade association has stated its opposition in principle to spam.

Within this unanimity, a large majority of these bodies has come out in favour of the opt-out approach, discussed and then promoted by Directive 2000/31/EC on electronic commerce. This is the case of the all the national organisations and some of the European federations such as FEDMA, the International Chamber of Commerce and the Internet Advertising Bureau.

➢ ***The cautious attitude of the industry representative bodies***

It is striking that the main distance selling industry federations and trade associations dismiss the notion that any of their members might be a spammer. At most, some of them will concede that spam in Europe is the work of isolated individuals not having access to large numbers of e-mail addresses, operating in a very short-term perspective often on the fringes of misleading advertising or fraud.

At the same time – and no doubt for this reason – none of the organisations consulted reports having made any provision in its by-laws to expel any member found "guilty" of spamming.

However, having been asked the question, some replied that they were planning to put this item on their agendas in the near future (this was the case in Denmark, Finland, France and Italy) with a view to providing expressly for expulsion in the case of spamming.

In this regard, the parties responsible for the industry labels currently being introduced in Europe and which stand for compliance with rules of conduct in relation to distance selling and/or data privacy, are conscious in most cases of the need for the sanction of expulsion, without which the credibility of their labels could be compromised if one of their labelled members was found to be spamming.

This happened, for example, in the case of the privacy protection label Trust-e in the United States, which had its image badly tarnished as a result of media coverage of the takeover of the direct marketing company Abacus by the advertising agency DoubleClick. DoubleClick, which had the Trust-e seal of approval at the

time, wanted to cross-reference its files with those of Abacus. But the Abacus acquisition, which was driven by this prospect of exploiting the cross-referenced personal data files, provoked a torrent of protest and fears which badly damaged the credibility of the Trust-e label. This is also a constant concern of those responsible for the personal data and consumer protection label L@belsite, promoted by FEVAD (Fédération française des Entreprises de Ventes à Distance) within FEDMA, EUROCOMMERCE and the GBDe (Global Business Dialog Exchange).

IV.3.2) - A twofold explanation: earlier stage of development and European culture

- ***Spam was addressed in Europe before it ever existed***

The market value of technology stocks and numerous studies carried out on the emergence of e-business show that the European e-commerce industry has not yet reached maturity or achieved profitability. It seems to be the case that right from the outset the majority of European e-commerce merchants are aware that they operate in an environment where not everything is allowed and that there is an existing legal framework that constrains their activities.

It is reported by consumer groups and associations of Internet users (such as EuroCAUCE) (59) that Europe witnessed an incipient spam phenomenon in 1997 and 1998 which was cut short as a result of media coverage of the debate surrounding the e-commerce directive.

In effect, spam was already perceived as outlawed in Europe by all sides (Internet users, public authorities and industry) even before it actually existed, in other words, before the European market for e-mail addresses could reach maturity free from any legal constraints – as had happened in the US. Indeed, it is reported by ISPs in most Member States that 80% of spam cases in Europe originate with the big American sites such as Amazon, Travelocity and Barnes & Noble, with whom the recipients have previously had direct contact.

This disparity between the level of hostility to spam and its low incidence appears to be confining the European spam phenomenon to the embryonic stage. The truth of this statement is borne out by the inability of marketing professionals to answer the question "how much is an e-mail address worth?", which is a basic piece of information for any merchant.

---

59) See http://www.eurocauce.org: Euro Coalition Against Unsolicited Commercial E-mailing.

For the purposes of the study, this question was put to over 100 Internet marketing industry associations throughout the fifteen Member States of the European Union and to almost 30 companies that rent e-mail addresses for commercial advertising purposes.

Only one answer quoted a figure: €4 per e-mail address. Since no cross-checking was possible, this figure cannot be regarded as reliable or representative. In any event, this single response referred to the price of the e-mail address in isolation. There were no responses received to the question as to the price of a European consumer's e-mail address combined with his known fields of interest.

These findings – or absence of findings – at least permit the conclusion that the market for e-mail addresses in Europe is not yet structured in terms either of supply or of demand nor in terms of its participants.

This situation is in sharp contrast to the situation in the US where lists of e-mail addresses are processed and traded using highly elaborate systems of cost-pooling, profit-sharing and commission payments (see Part One, II.2.5).

- ***The strong European culture of data protection***

Europe has a strong culture of personal data protection which is ingrained in its traditional distance selling industry. All Member States have a general data protection law and a supervisory authority, which in some cases have been around for many years. This legal and institutional framework heightens awareness of data protection issues among Europe's direct marketers who are increasingly sensitive to the bad publicity and damage to business that can result from a complaint or an official sanction in relation to privacy violations.

In addition, Europe already had experience of spam's forerunners which used the older media of telephone and fax. It was clear from this experience that spam would be subject to a strict legal framework and a measure of self-censorship on the part of the majority of operators.

This was because the response from consumers and data protection authorities to these marketing techniques was such that the industry quickly understood that certain practices should be prohibited given their unpopularity.

Consider, for example, the recommendations of the CNIL in France which in 1985 led to a requirement of prior consent for telephone marketing by automated calling systems.

The support of all sides (consumers and industry) for this new rule – which was not in fact given statutory force – was such that it was embodied in the sectoral directive of 15 December 1997 on data protection in the telecommunications sector and extended to direct marketing by fax.

It may be recalled that Directive 97/66/EC also gave Member States the alternative of an opt-in or opt-out approach to telephone marketing and to subscribers' right to be omitted from telephone directories. In this area, the 1997 directive has indisputably had a very positive effect on attitudes and should have a significant practical impact – as soon as it has been transposed into the domestic law of all the Member States.

IV.3.3) - The effects of caution

- ***The proliferation of opt-out lists***

Some industry associations have spontaneously anticipated the adoption of the e-commerce directive by setting up their own opt-out lists, some of which are specific to particular trade associations or business sectors while others are national in scope.

In France, for example, the Fédération des Entreprises de Vente à Distance (Direct Marketing Federation - FEVAD) is the first body to have created an opt-out list (60) by which consumers can ask to be removed from all marketing lists. This list may be consulted by any service provider, including non-members of FEVAD, on payment of a modest annual fee towards the cost of managing the list.

Created in 1998, this list has been actively promoted by FEVAD since the summer of 1999, notably vis-à-vis its European counterparts in the Federation of European Direct Marketing (FEDMA). It is a potential model for other national opt-out lists currently being established. An agreement has already been signed with the German direct marketing federation to this effect.

The Association Belge du Marketing Direct (ABMD) has also set up a nationally-based general opt-out list, which is additional to the opt-out lists maintained by each member of the association. The ABMD is currently in discussions with the Belgian Ministry of Eco-

60) See http://www.e-robinson.com

nomic Affairs to work out the practical details of the implementation of Directive 2000/31 on electronic commerce, in particular the procedure for exercising an opt-out and for inclusion in a national opt-out register.

In other European countries, opt-out lists are being put in place either by direct marketing industry federations or by newer organisations representing the online industry.

Almost all these initiatives were taken in response to the adoption of Directive 2000/31/EC on e-commerce, Article 7(2) of which provides: "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".

Between May and October 2000, a comprehensive survey of European industry federations was undertaken for the purposes of this study in order to identify all the private sector initiatives which had been or were being taken in each Member State.

It was found that opt-out lists are currently being set up in the UK, Germany, the Netherlands, Spain, Norway, Sweden, Finland and Italy. They are all designed initially to cover only the particular Member State concerned but most of the federations behind the initiatives plan to extend these national opt-out registers in the near future to the EU as a whole or even to countries outside the EU, in particular the United States.

Note that FEDMA is currently promoting four different opt-out lists on the Internet (61), each of which is specific to a particular marketing medium: MPS (Mailing Preference Service), TPS (Telephone Preference Service), FPS (Fax Preference Service) and E-MPS (E-mail Preference Service) for direct mail, telephone, fax and e-mail marketing respectively.

It is hard to see the point of an opt-out list for fax marketing, given that since 25 October 1998, Article 12(1) of Directive 97/66/EC of 15 December 1997 imposes a clear requirement of prior consent rather than a mere right to object for all marketing by fax.

On this point, it may be observed that the development of shared opt-out lists by industry federations has proceeded in parallel with the enacting of legislation by Member States requiring the setting up of national opt-out registers or imposing a requirement of prior consent.

---

61) See http://www.fedma.org/code/page.cfm?id_page=77

There is no contradiction here. This process reflects the natural complementarity that can exist between statutory provisions and industry codes of practice. Some direct marketing companies have long since understood that an individual's express wish not to receive marketing solicitations in itself constitutes valuable information which when shared among retailers enables them to cut down unproductive marketing expenditure and to avoid negative responses and complaints.

In fact, some recent enactments at national level have built on private sector initiatives, usually by seeking to ensure a uniform code of practice for e-mail marketing within the Member State concerned. Legislative action of this kind tends to be taken where there is a risk of duplication and redundancy as between several different opt-out lists, each aspiring to national coverage.

Finally, the Belgian Direct Marketing Association has announced that from the beginning of 2001 it intends to start promoting the opt-out list set up by the American DMA (Direct Marketing Association) and known as the "E-mail Preference Service". There are also plans for the American DMA and various of its European counterparts to work together to create an opt-out register covering several European and non-European countries (62).

Already, the United Kingdom's direct marketing association, the UKDMA, has joined with the American DMA in this project to build a joint register. It may be observed in passing that the implementation of this list, which is to be managed in the US but made accessible to Internet users through the UKDMA portal, has given rise in the UK to difficulties relating to cross-border flows of personal data. These difficulties have held up the project.

➢ ***Other ethical policy commitments***

Some e-commerce merchants have adopted ethical policy measures which go beyond simply setting up an opt-out register and enable the recipient of an e-mail identified as commercial to be included in the register by simply clicking on a link placed at the end of the message. This practice is recommended by the French Direct Marketing Federation (FEVAD).

Many European commercial websites also now have a check-box either on a special privacy page or on their registration forms al-

62) See http://www.e-mps.org for the E-mail Preference Service of the American DMA, which is currently being extended to Europe.

lowing users to indicate a wish not to be sent e-mail and/or marketing messages.

The educational role played by the European data protection authorities has very likely been influential in the implementation of these practices and initiatives. In France, the Fédération du Commerce et de la Distribution, which is the supermarkets industry federation, recently adopted a code of practice recommending that all forms on commercial websites should have two check-boxes: one to allow users to indicate they do not wish to receive e-mail marketing messages and the other to allow them to refuse disclosure of their data to third parties.

IV.4) - Spam: a practice ISPs are trying to quale

The above analysis may have conveyed too optimistic an impression of the situation and that must now be qualified. The apparently low incidence of spam in Europe can be largely explained by the anti-spam measures that have been put in place by ISPs in Europe and the US who wage a daily battle against the waves of bulk e-mail that spammers attempt to relay through their mail servers.

The ISPs create and informally exchange "black lists" of e-mail addresses and domain names belonging to known spammers. Most ISPs have implemented technical measures to detect and block bulk e-mail. As it happens, none of the ISPs consulted were able to provide any quantitative data on the effectiveness of these filtering tools in stemming the flow of spam.

These filtering devices also raise the question as to whether it is legitimate for a private ISP to decide unilaterally not to deliver messages mailed by a particular sender. Moreover, they may not work if the sender's e-mail address has been masked or falsified. In any event, the use of these methods make it impossible to ascertain the potential volume of spam which is prevented from reaching the mailboxes of European Internet users through the vigilance of the ISPs.

An important consideration is the cost incurred on the fight against spam by ISPs and managers of private or commercial mailing lists. It shows that Europe cannot consider itself immune from the effects of spam.

In its report on direct marketing by e-mail, the CNIL noted that for these service providers spam represents an "additional strain on their financial, human, technical and commercial resources which is proportional to the number of their subscribers".

"Financial and human, in terms of the time spent by staff, some of whom are assigned full-time to the battle against spam (monitoring and detection systems may require manning on a 24-hour basis) while others have to respond to complaints received from subscribers." "Technical, in terms of the significant volume of bandwidth consumed by an e-mail message sent simultaneously to a large number of their subscribers. More bandwidth therefore has to be provided than would be necessary solely to cater for normal use of Internet services by subscribers." "Commercial, in terms of the common assumption on the part of Internet users that their e-mail addresses were improperly disclosed to third parties by their ISPs."

In its report, the CNIL says that in 1999 the US online service provider America On Line, all of whose access and e-mail servers are located in the US, had a team of 15 deployed on technical measures to combat spam.

EuroISPA, which represents the vast majority of Europe's ISPs, has been fighting spam for over two years now and has on several occasions lobbied national data protection authorities in favour of the opt-in approach to unsolicited commercial e-mail. This, it believes, is the only approach consistent with the requirements of Directive 95/46/EC.

In France, the Comité Réseaux des Universités (Universities Network Committee – CRU) operates several thousand (7,000) mailing lists to which most French students and universities are subscribed as well as providing e-mail services to a sizeable portion of France's student and academic population.

The members of the CRU report that spam is a major nuisance for them. First, users of their services complain of problems in managing and sorting incoming e-mail.

Secondly, users are so infuriated by the volume of unsolicited messages that they are tending to reject e-mail altogether. Lastly, the CRU cites the extra cost entailed by the technical measures deployed in an effort to block or filter out as much of the spam as possible.

In the light of all this, the low penetration of unsolicited commercial e-mail ought not deter the European Union from laying down clear rules for senders of commercial e-mail, in the interest of legal certainty.

It is therefore fortunate that unsolicited commercial e-mail may be constrained by legal regulation before it has the chance to develop unchecked, as US Internet users may testify.

But when discussing the safeguards needed in relation to spam or unsolicited commercial e-mail, there needs to be clarity on exactly what is at

issue: are the safeguards based on rules governing the collection of e-mail addresses or on rules governing the sending of commercial communications – or both?

Chapter V: Confusion of approaches leading to divergence of practices

Reference has been made in the preceding chapters of this study to the industry consensus in favour of the opt-out approach to unsolicited commercial e-mail. This consensus crystallised during the discussions of the electronic commerce directive between the end of 1998 and the summer of 2000. Yet behind the industry's apparent united front, there appears to be confusion as to what forms of e-mail marketing are allowed in Europe according to whether the recipients are:

- customers or prospective customers who supplied their e-mail addresses to the sender themselves;

- individuals whose e-mail addresses were obtained by the sender from a third party who in turn obtained them directly from the individuals themselves;

- individuals whose e-mail addresses were collected in a public space on the Internet (website, directory or mailing list), without their knowledge.

This is the conclusion that may be drawn from the responses received from industry by the authors of this study. The confusion is no doubt partly a matter of terminology. It does not appear to have been dispelled by the multiple directives applicable to unsolicited commercial communications. And it appears to have been exacerbated by a mistaken belief in the trade that the provisions of Directive 2000/31/EC are self-contained and all-embracing.

V.1) - A certain confusion of approaches ...

Borrowed from a Monty Python sketch, the term "spam" (63) was coined to refer to intrusive marketing practices which, particularly in the early cases, often involved computer hacking.

63) The term seems to have originated in a Monty Python sketch in which some of the characters keep repeating the word "spam" (a kind of luncheon meat) after every two or three words, thereby infuriating the other characters.

The US state statutes dealing with spam refer to "unsolicited commercial e-mail". Similar terminology has been adopted by the various European directives in this domain.

V.1.1) - Confusion between spam and unsolicited commercial e-mail

Spam is generally understood to mean the repeated mass mailing of unsolicited commercial messages by a sender who disguises or forges his identity. Thus, while it has in common with other forms of commercial communication the fact that it is unsolicited, it differs from them by its massive, repetitive and unfair nature. In short, all spam is by definition unsolicited commercial communication but not all unsolicited commercial communication is spam.

Spammers are often portrayed, particularly by the mainstream industry, as "cowboys" who have nothing in common with image-conscious legitimate businesses, since they have no qualms about disguising their identity and mailing in bulk.

Regarding this bulk-mail aspect of spam, it should be noted that the spammers have been able to use the relay function – a function which all too often is still available in the mail servers of ISPs – to relay spam to all the e-mail addresses managed by those servers. From the responses of European ISP federations it transpires that even today over 40% of mail servers in operation in Europe still have a relay function and are therefore unable to prevent spam being relayed to all the e-mail addresses managed by them.

The industry tends to argue, at least by implication, that there is the same distinction between spam and other forms of unsolicited commercial e-mail as that between automated calling systems and telephone marketing. Spam, according to this view, is an aggressive and unscrupulous marketing technique which is shunned by the majority of businesses. This is probably correct and invites legal re-assessment of the suitability of the privacy safeguards currently in place.

In any event, an automated calling system makes the telephone ring and interrupts the subscriber in the same way as an unsolicited e-mail interrupts the Internet user – whether or not it is spam.

The industry's responses to questions on the collection of e-mail addresses are revealing in this regard. For while the vast majority of businesses eschew spamming and while their federations may officially ban it (see above: "The cautious attitude of the industry representative bodies"), most of them are non-committal or silent as to

whether they reserve the right to send unsolicited commercial communications..

This ambivalence gives rise to two considerations. First, it shows that it is possible to be opposed to spam, meaning unscrupulous bulk e-mail, while not taking any position on the question of unsolicited commercial e-mail. Secondly and more importantly, an issue which equally concerns spam and other forms of unsolicited commercial e-mail is virtually never addressed by the industry: the circumstances in which the e-mail addresses were collected.

But to focus on the distinction between spam and the other forms of unsolicited commercial communication is to overlook the pivotal issue of how e-mail addresses are collected.

V.1.2) - Different concepts of unsolicited commercial e-mail

Strictly speaking, an unsolicited commercial communication has two essential characteristics: its commercial nature and the fact that it is unsolicited i.e. not requested in advance by the Internet user.

This is the approach which appears to have been adopted in the electronic commerce directive, which makes no distinction according to whether a commercial communication is sent by an e-commerce merchant to its customer, to a visitor to its website (who may have supplied his e-mail address in order to take part in a competition) or simply to an Internet user with whom it has never previously had contact.

It is revealing to note that MEDEF, the largest French employers organisation (64), in its submission to the CNIL in October 1999, pleaded for a clear definition of the concept of "unsolicited commercial communication". It was critical of the fact that the same obligations are imposed on businesses in all three scenarios referred to above. MEDEF argues, as does FEDMA, that a marketing message sent by a business to previous customers is never an unsolicited commercial communication. According to this view, a commercial communication may be implicitly solicited by a prospective customer or visitor to a website who, without subscribing to a particular service, supplies his e-mail address in a commercial contact form. Accordingly, there is no doubt that a marketing message subsequently sent to that individual can be regarded as having been solicited.

In short, all the confusion can be dispelled if it is agreed that the legitimacy of the sending of an unsolicited message depends primarily on the circumstances in which the e-mail address concerned was obtained.

---

64) MEDEF: Mouvement des Entreprises de France.

V.2) - ... which has not been remedied by the many European directives

V.2.1) - Directive 97/7/EC of 20 May 1997

Directive 97/7/EC of 20 May 1997, on the protection of consumers in respect of distance contracts, by permitting marketing messages to be sent via e-mail where there is no clear objection from the consumer may have given industry the understandable impression that Europe had opted for a minimum opt-out approach, whereby there would be no restrictions on e-mail marketing to any customer, website visitor or other Internet user who had not clearly indicated a wish not to receive such information, the onus being on the Internet user to invoke the safeguard: his consent is presumed until the contrary is proved.

V.2.2) - Directive 95/46/EC of 24 October 1995

The Directive of 24 October 1995, however, qualifies this position by laying down strict rules governing the collection of personal data (specified, explicit and legitimate purpose, fair and lawful processing) and information requirements (obligation to advise individuals of their right to object to commercial use or disclosure of their data to third parties).

The onus is thus no longer on the Internet user to invoke the safeguard. The e-commerce merchant is now bound by specific obligations both when collecting and before making use of the data.

How then are the e-commerce merchant's data protection obligations to be reconciled with the apparent flexibility of the distance selling directive?

V.2.3) - Directive 97/66/EC of 15 December 1997

Although this directive does not deal with e-mail marketing, it subjects the most intrusive forms of commercial communication (automatic calling systems, fax) to a requirement of prior consent.

How is this level of safeguard to be reconciled with the previous directives when the characteristics of e-mail solicitation are so similar to those of automatic calling systems and given that e-mail may be considered the most intrusive marketing medium of all, there being no way of avoiding it and – above all – it being the most costly for the recipient (see above: conclusions of Part I)?

V.2.4) - Directive 2000/31/EC of 8 June 2000

By opting for the lowest common denominator, the electronic commerce directive appears to drop the link between the legitimacy of an unsolicited mailing and the wishes of the recipient, whether expressed as prior consent (Directives 95/46/EC and, to some extent, 97/66/EC), clear objection (Directive 97/66/EC), ordinary objection (Directives 95/46/EC and 2000/31/EC and, to a certain extent, 97/66/EC) or abstention.

The rule laid down in Article 7(1) concerns only the characteristics of the message sent: the commercial nature of the communication must be immediately identifiable. This provision is perceived by most in the industry as providing clear sanction for unsolicited commercial communications.

Of course an opt-out register must be set up enabling individuals to indicate they do not wish to receive commercial e-mail. But the directive does not appear to require Member States to oblige service providers to consult this opt-out register systematically prior to every mailing campaign but only to ensure that they do so regularly. On the face of it, the era of the minimum opt-out approach under the distance selling directive looks like a "golden age of consumer protection" by comparison! Henceforth, even a clear objection may be to no avail due to this provision requiring "regular" consultation only and the inability of the industry to compile a complete inventory of all the opt-out lists in operation.

The situation is redressed to some extent by the reference in Article 7 to "other requirements established by Community law" which, from both a legal and a political perspective, must be taken to include the protection of personal data and the general principles enshrined in Directive 95/46/EC.

But this vague reference to existing Community law is not very explicit and is of little assistance to e-commerce merchants when they come to ask themselves these three questions:

- do I or do I not have the right to send a commercial e-mail message to one of my customers and, if so, subject to what conditions?

- do I or do I not have the right to send a commercial e-mail message to a visitor to my website and, if so, subject to what conditions?

- what means may I legitimately employ to make myself known to Internet users who are unaware of my existence?

The net effect of all this was that the debate surrounding the adoption of Directive 2000/31/EC focused more on the conditions on which commercial e-mails may legitimately be sent than on the circumstances in which the e-mail addresses are initially collected.

V.3) - A wide variety of industry practices

V.3.1) - From the check-box to the pre-checked box

On more and more websites visitors can now tick one box to indicate whether or not they wish to receive commercial messages from the website in question and another box to indicate if they do not wish their data to be disclosed to third parties for commercial purposes.

A survey conducted by the CNIL in March 2000 of the top 100 French e-commerce sites shows that this practice is very widely followed. It is also recommended by many industry associations in Europe. What is striking is that this practice goes well beyond what is required under the e-commerce directive. One has to wonder as to the relevance of legislation which even the industry concerned does not regard as offering the minimum safeguards required to elicit the trust of Internet users.

However, probably under the influence of a practice common in the US, other European sites use electronic forms with boxes which are already ticked, thus authorising by default – if the user is not careful – not only the use of the data for marketing purposes but also disclosure of the data to third parties for marketing purposes.

This practice and others like it, such as that of concealing the mandatory statement of the intended use of the data in a lengthy legal notice which is difficult to find and couched in convoluted language, are violations of the rights of Internet users and are contrary to the requirements of transparency and fairness laid down in Directive 95/46/EC.

In the case of the disclosure of data to third parties, one often comes across highly misleading statements. Some sites, for example, use phrases such as "your personal data are for the exclusive use of company X and its partners, subsidiaries and affiliates and will not be disclosed to third parties" or "your personal data are for the exclusive use of company X and its partners, subsidiaries and affiliates; they may be

disclosed to third parties; you may refuse such disclosure by ticking the box".

However other businesses want to have no truck with such practices which they regards as just as reprehensible as spam and equally destructive of consumers' trust. These sites see a clear statement of the opt-in alternative as the best business policy.

V.3.2) - From the success of the check-box to the opt-in approach

The current strong industry trend in favour of the opt-in approach is a case of commerce finding common cause with data privacy.

Some e-commerce merchants readily acknowledge that a check-box accompanied by a clear statement of the right to opt out of receiving marketing information has a strong psychological effect on users. A very high proportion of users (up to 70%) choose to tick the box, according to some industry sources. It seems the mere presence of such a check-box prompts a reflex to tick it. Where the check-box's function is to indicate a preference not to receive marketing information, a great many users will thus tend to opt out.

In order to turn this psychological reflex to their advantage, all e-commerce merchants need to do is to keep the check-box but reformulate the statement along the lines of "I wish to receive all your advertising offers" or "I wish to receive all the advertising offers you or your partners may choose to send me in the following areas: cinema, computers etc.".

Instead of prompting the user to end the relationship by offering an opt-out, now the e-commerce merchant is inviting him to continue their exchanges: the permission marketing process is underway.

Many US and European businesses have understood that from a commercial standpoint an interactive relationship model – the opt-in – offers many commercial advantages.

In a permission marketing relationship, consumers are more likely to be offered services they actually want since they have been asked to indicate their preferences. In so doing, consumers provide highly-prized information which can be packaged and traded and which is authorised for processing. The collection and commercial exploitation of data obtained with the consumer's prior consent thus represents not only a source of profit and a new financing method for electronic commerce but also the most effective means of tracking the uses to which the data are put.

In this set-up, the party who collected the information receives a payment whenever one of its business partners uses it in a marketing campaign. In return, the advertiser has the assurance of targeting a population that is interested in receiving commercial messages and can thus advertise more efficiently. Moreover, if a member of the public asks to be removed from a mailing list or for details of where and when the data were collected, the advertiser and the party who originally collected the data are able to provide exact information as to when, why and to whom the individual's e-mail address was supplied.

Thus, businesses prepared to eschew unpopular and counterproductive online marketing practices and adopt the ethos of the Internet community stand to win the confidence of web surfers. And while opt-out registers have no commercial value, consent-based lists represent a valuable commodity.

The growing trend towards permission marketing was confirmed in Europe at an international conference held in Paris from 12 to 15 September 2000 (www.webcommerce-europe.com), in particular during a round table session devoted to e-mail marketing, attended amongst others by the European subsidiaries of the US firms MessageMedia and 24/7 Media. Those present had the impression of an awkward disunity between the exponents of this new trend and the advocates of the opt-out approach, such as FEDMA and the American DMA.

In Finland, this trend has recently been endorsed in a code of conduct for direct marketers based on the opt-in approach, following the entry into force of the Act of 22 April 1999 on the protection of personal data in the telecommunications sector, specifically Article 21 thereof which imposes a requirement of prior consent (opt-in).

Chapter VI: The need for a clarification

Given the apparently contradictory legal requirements, the marked divergence in industry practices and the growing trend in favour of the opt-in model, a clarification of the issue at EU level is now urgently required.

VI.1) - The application of the current law

Direct marketing by e-mail occurs in any one of three very different scenarios, each of which will now be analysed from a legal perspective in the light of the applicable directives.

VI.1.1) - Previous contact between sender and recipient

This is the direct collection scenario: the mailing list used consists of the e-mail addresses of customers and visitors with whom the advertiser has been in direct contact.

Under the general directive (95/46/EC), commercial e-mails may be sent to such persons subject only to their right to opt out of receiving them.

Article 10 of Directive 95/46/EC requires that the data subject be informed of the purpose for which his data are to be used and thus whether they will be used for direct marketing. Furthermore, if the party collecting the data intends to disclose them to third parties, Article 14 of the 1995 directive requires that party first to inform the data subject and to give him an opportunity to object to such disclosure before it takes place.

However, it might be argued that, in strict legal terms, the 1995 directive does not explicitly require an e-commerce merchant to inform the data subject of his right to object to receiving unsolicited commercial communications sent by that particular merchant: according to this view, the recipient has that right and can exercise it at any time but the e-commerce merchant is under no obligation to inform him of it.

On the other hand, in the light of Article 6 of Directive 95/46/EC and the application of the principle of fairness as expressed in Article 10(b) and (c) of that directive, it may be inferred that the use of the words "anticipates being processed" in Article 14 necessarily implies that data subjects must be informed before their data are disclosed to third parties.

This interpretation of Directive 95/46/EC is not contradicted by Directive 97/7/EC of 20 May 1997 on distance selling, which provides that everything is allowed unless there is a "clear objection" on the part of the recipient. But a clear objection presupposes that the data subject has first been clearly – i.e. explicitly – informed of his right to object. It is inconceivable that the Community legislator, in a directive supposed to provide a high standard of harmonised consumer protection, intended to leave it up to consumers to guess whether or not their data are liable to be disclosed to third parties.

Nor does this interpretation conflict with the telecommunications directive of 15 December 1997 which does not explicitly subject commercial e-mail to recipients' prior consent, although some Member States (Austria, Denmark, Finland and Italy) have used the opportunity offered by the transposition of this directive to extend the right of prior consent to cover commercial e-mail.

On this interpretation it is ironically Directive 2000/31/EC on electronic commerce which imposes additional obligations on e-commerce merchants sending commercial communications to their own customers – the obligation to clearly identify such messages as being of a commercial nature and the obligation to consult the opt-out registers "regularly". It may be noted that this second requirement may have the effect of preventing businesses from engaging in normal correspondence with customers if the latter decide to register themselves on a national opt-out list that is binding on all advertisers.

This legal analysis indicates that both the general confusion and the e-commerce directive are increasing the obligations on business and fuelling debates (opt-in versus opt-out, check-box etc.) in which each view is supported by plausible legal arguments. The goal of providing e-commerce with an environment of legal certainty has therefore not been achieved.

VI.1.2) - E-mail address supplied by a third party

This is the indirect collection scenario: an Internet user gives his e-mail address to an e-commerce merchant which subsequently makes its mailing list available to a third party for direct marketing purposes.

The supply of the mailing list is lawful from the data protection standpoint if the e-commerce merchant who originally collected the e-mail address and proposes to make it available to a third party has informed the addressee that his data may be disclosed to a third party for direct marketing purposes and has given him the opportunity to object to such disclosure online and free of charge.

Article 14 of the general directive of 24 October 1995 provides clearly that information may not be disclosed to third parties if the data subject has not first been given an opportunity to object. Applying this provision in the context of online data collection, it effectively means that the electronic form used to collect the data must contain a clear statement of the right to object and a check-box. It is worth noting that only in the 1995 directive is this scenario addressed in the form of general principles.

VI.1.3) - E-mail address collected from public spaces on the Internet

In this final scenario, the e-mail address is obtained in the public areas of the Internet (newsgroups, mailing lists, directories posted on websites etc.) without the knowledge of the data subject or of the administrator of the site containing the information.

This practice is outlawed by the Directive of 24 October 1995. To begin with, it is contrary to Article 6 (principle of finality): an individual who expresses a view on a particular subject in an online discussion forum or who subscribes to a mailing list in order to share information with a group of individuals having an interest in common is clearly unaware that a third party plans to use his data for a purpose other than that of the discussion.

The practice is probably also contrary to Article 7(f) of the 1995 directive (legitimacy of processing): unless one were to argue that the automated collection for direct marketing purposes of all the e-mail addresses found in a public area of the Internet is in pursuit of a legitimate commercial interest which overrides the legitimate interests of the addressees, the general Directive 95/46/EC prohibits such processing unless the "data subject has unambiguously given his consent".

The practice is also at variance with the provisions of Articles 10 and 11. The information obligation imposed on a party collecting data must be discharged at the time the data are recorded or – where disclosure to a third party is envisaged – no later than the time when the data are first disclosed. In any case, these articles prohibit direct marketers who have collected e-mail addresses in the public areas of the Internet from using them for their own purposes, unless they first inform the

data subjects, and from disclosing them to third parties, unless they first inform the data subjects of their right to object to such disclosure.

The practice is also in breach of Article 14 of the directive which gives every individual the right to object to his data being used for direct marketing purposes or being disclosed to third parties.

The Directives of 20 May 1997 on distance selling and of 8 June 2000 on electronic commerce deal only with the conditions for the sending of unsolicited commercial e-mail and do not address the lawfulness of the circumstances in which e-mail addresses are obtained. This issue is governed by Directive 95/46/EC (and in the case of traffic and billing data, Article 6 of Directive 97/66/EC) and is subject to the requirements described above.

VI.2) - Shifting the focus of debate from the lawfulness of sending to the lawfulness of data collection

VI.2.1) - The debate has been focused only on the lawfulness of the sending of commercial communications

Many contributions received from the industry side concentrate on the format and size of messages, the identification of their commercial nature or the inclusion of a link to an opt-out list. The premise is that commercial e-mail is acceptable if it is brief, identified as being of a commercial nature and if the recipient can avoid receiving any further messages by exercising an immediate opt-out after one message.

Notwithstanding its reference to "existing Community legislation", Directive 2000/31/EC appears to come down in favour of this approach. If so, the effect is to impose the same constraints on a retailer contacting a customer as on a spammer using unlawfully obtained e-mail addresses.

This approach is criticised by the CNIL in France, by the Spanish Data Protection Agency, by the Data Protection Working Party established by Article 29 of the 1995 directive and by the growing number of those within the industry who are in favour of an opt-in policy.

Such criticism is not surprising given that the approach in question avoids the issue of lawful collection and the more general principle of fairness of processing. This despite the fact that the history of the Internet proves that lack of transparency and disregard for the principle of fairness have seriously held back the growth of e-commerce and undermined consumer confidence.

The controversies over cookie files, the serial number of Intel's Pentium III processor or the serial number of Microsoft's software products have been fuelled by lack of explanation, information and transparency rather than by any malevolent intent on the part of the suppliers concerned. The Internet community's sensitivity to dubious commercial practices was again demonstrated in relation to recent schemes whereby retailers offered financial inducements to Internet users in exchange for their friends' e-mail addresses (this was the IKEA case, currently being litigated in the US courts), a new form of viral marketing or word-of-mouth.

The debate must therefore be focused on the principle of fairness and the need to avoid practices liable to engender mistrust.

VI.2.2) - Focusing the debate on the fairness of collection

The preceding analysis of the different scenarios in which the e-mail addresses used for unsolicited commercial communications are obtained illustrates the complexity of the applicable legal framework, the confusion to which this gives rise, the practices which it can appear to authorise and the doubt which it still leaves open in relation to practices which should be clearly prohibited.

The 1995 directive prohibits the collection of e-mail addresses from the public areas of the Internet, including newsgroups.

On the other hand, no directive clearly imposes an opt-in approach to the direct relationship between a business and one of its customers. Yet apart from a section of the industry which justifies its opt-out approach on the basis of the implicit obligation to implement the provisions of the electronic commerce directive, the general trend on the Internet is already towards opt-in.

The timid approach taken by the European directives appears to have been overtaken by events and no longer to reflect the objective interests of e-commerce merchants. Moreover, by imposing the same obligations on all senders of commercial e-mail, the electronic commerce directive fails to achieve its stated aim. For it creates a situation where a business which chooses the opt-in route and makes the effort to ascertain a customer's interests and to inform him clearly that his e-mail address will be used for direct marketing purposes is nonetheless obliged to consult a general purpose opt-out list, be it national, European or transnational in coverage, which may prevent that business from notifying that customer of its latest products and offers.

Spelling out the circumstances in which data may be fairly collected allows the e-commerce merchant and the Internet user to take control over the nature and the future course of their relationship in a climate of transparency.

Apart from the fact that it is in the mutual interest of Internet users and e-commerce merchants, it would seem natural to extend to direct marketing by e-mail the same rules as apply to direct marketing by automated calling system or by fax, given that they have in common their intrusiveness and unstoppability: with all three techniques, the recipient is unable to interrupt reception of the message and, in the case of e-mail, he also has to bear the costs of reception (65).

The history of the advertising industry shows that the lower the cost of a direct marketing technique the greater the risk of abuse, as witnessed by the fact that as long ago as 1974 the United States had to enact legislation outlawing fax marketing without the recipient's prior consent. And e-mail marketing is by far the cheapest form of direct marketing yet invented.

Moreover, the history of data protection legislation shows that the degree of protection given to consumers has always been appropriate to the threat to privacy, according to a system which is well-established in most Member States, ranging from the right to object (telephone marketing) to the requirement of prior consent (direct marketing by automated calling system and by fax).

All things considered, the opt-in approach seems to be the model which is best-suited to the Internet. It allows e-mail databases to be operated profitably, it promotes personalised relationships between e-commerce merchants and their online customers and it is the system most in accordance with the culture and accepted practices of the Internet – as the experience in the US and of some European businesses testifies. In contrast, under an opt-out system the Internet user has no longer any means – short of exercising his right to object – of controlling how his data are used once they have been collected while an e-commerce merchant contacting a customer has no way of distinguishing himself from a spammer enjoying a spurious legitimacy thanks to the opt-out registers.

---

65) Cf. page 67.

VI.3) - Validity and acceptability of opt-in

Practically all of European e-commerce merchants claim to prefer the opt-out approach. Yet many of them have already implemented opt-in systems which provide higher value data. Like Monsieur Jourdain in Molière's "Le Bourgeois Gentilhomme" (who did not realise he had been genial speaking prose all his life), they practise opt-in without knowing it, or without saying it. Those using opt-out systems – who may be members of the same industry federations – run the commercial risk of alienating prospective customers by excess marketing, whereby a single over-eager advertiser may lead recipients to exercise a blanket opt-out which is applicable to all.

The opt-in approach has the added advantage of certainty that the data are being used with the subject's consent. Under an opt-out system, how can the sender of a commercial e-mail be sure that the recipient has not already registered on an opt-out register? Supporters of the opt-out approach have not yet managed to provide an answer to this question. FEDMA, for example, has announced on its website that it is carrying out a massive survey of all existing opt-out registers. With an opt-out model, it is quite conceivable that considerations of legal certainty will ultimately necessitate EU legislation to consolidate all opt-out requests in a single Community-wide register. The effect of this would be draconian: an opt-out request directed at a handful of advertisers or even at a single advertiser would apply to the entire e-commerce industry, thus destroying one-to-one relationships between individual Internet users and online merchants. With that in mind, it is the opt-in approach which appears best-suited to the creation – or termination – of personalised relations between online suppliers and web surfers.

VI.3.1) - The opt-in approach does not prohibit the sending of commercial e-mail to customers or website visitors

No more than it is prohibited for a company to contact its customers by fax, the opt-in approach does not prohibit the sending of commercial e-mail. On the contrary, it authorises it.

All that is required is that the information given to the addressee be sufficiently clear and unambiguous on this point. It is already common practice in the industry to provide an explicit information notice next to a check-box. The choice as to how this notice is worded, as was explained earlier, is not dictated by a theoretical debate between supporters of the opt-in and opt-out models but by the market and by the need for clarity on the part of the e-commerce merchant, in whose interest it is to obtain clear and specific consent so as to maximise the value of the e-mail addresses collected.

Moreover, the opt-in approach emphasises the continuation of the relationship rather than its prohibition. Many sites already offer visitors the possibility of subscribing to a newsletter, joining a mailing list or receiving notification of future modifications to the site, new offers etc. In all these cases, the e-mail address is collected with the owner's consent and can be used within the scope of that consent without further ado, unless and until he should revoke his consent.

VI.3.2) - The opt-in approach does not prohibit disclosure to third parties of data supplied by Internet users

The 1995 directive already imposes an obligation to clearly inform Internet users of any envisaged disclosure of their data to third parties for direct marketing purposes and to give them an opportunity to object to such disclosure. The use of the check-box for this purpose is on the increase, in the US, France and elsewhere.

The opt-in approach to unsolicited commercial e-mail has no bearing on the issue of disclosure to third parties of data collected. Thus it does not impose any additional obligation over and above those obligations (information requirement and data subject's right to object) already laid down by the general rules governing the commercial disclosure of personal data to third parties (Article 14 of the 1995 directive).

VI.3.3) - The opt-in approach does not prohibit the compilation of mailing lists

In the bricks-and-mortar world, it is routine for businesses to keep files of individuals wishing to receive information on a particular category or products or services and this practice does not generally give rise to problems. In fact it forms the basis for a database marketing business which turns this information into a valuable commodity. This is an activity with the potential to flourish on the Internet.

The opt-in approach also provides another valuable marketing resource in that opt-in mailing lists reveal a multitude of specific consumer preferences and fields of interest rather than being just a blank list of undifferentiated names of dubious or unpredictable value.

VI.3.4) - The opt-in approach prohibits unfair collection and use of data

In doing so it ensures effective protection of personal data, provides legal certainty for industry, creates a climate of trust and removes the

artificial conflict between the original free spirit of the Internet and the needs of e-business.

Granted, the circumstances in which consent may be obtained need to be better defined. Is it permissible, for example, to offer a financial inducement to obtain consent? Does the Internet user always appreciate the scope of the consent given? No doubt he consents to receiving solicitations in his fields of interest but is he aware that his consent may be used to construct his profile as a consumer or as an individual?

These questions are still open as of now. They will be resolved only after the confusion is brought to an end by a resolute commitment to the opt-in approach, which is the one policy capable of providing a propitious and secure legal and economic framework for the interactive relationships which are inherent to e-commerce.

Conclusions of Part Two

The need for a coherent legal framework for all electronic communications

The debate in Europe over the nature of the safeguards to be provided in relation to commercial communications has now been going on for over seven years.

It was during the discussion of the 1995 directive that the question was first raised as to whether the individual's right should take the form of an opt-out or opt-in. Eventually, that directive adopted the opt-out principle in the form of a right to object to the use of personal data for direct marketing purposes, with the requirement of prior consent (opt-in) being reserved for cases where the interests of the data processor are overridden by the data subject's interest in the protection of his fundamental rights (Article 7(f) and 7(a) of Directive 95/46/EC) and the requirement of prior and explicit consent being reserved for the processing of sensitive data (Article 8 of Directive 95/46/EC).

The 1997 directive on distance selling could not have followed a different approach than that taken in 1995. However, the industry lobbied successfully for the creation of a new opt-out concept within the existing range of safeguards: the "clear objection", although there had not been any danger that consumers would seek to rely on an implied objection.

The 1997 directive established a new regime for the telecommunications sector, which by its nature processes data falling within the private sphere (whom you call, who calls you, when, from where etc.) and which had already seen the use of automated direct marketing techniques before 1997. This new regime was designed to take account of the seriousness of the threat to individuals' privacy. Under the directive, direct marketing by means of automated calling systems or by fax was subject to a requirement of prior consent, while telephone marketing was authorised only subject either to a requirement of prior consent or to a mere right to object, at the option of the Member State concerned.

The common European position was now clear: the greater the threat to privacy, the greater should be the level of protection provided. This clarity, which offered legal certainty to the business community, was lost sight of in the electronic commerce directive.

The eighteen month-long discussion of Article 7 of Directive 2000/31/EC was mainly concerned with finding an approach acceptable to the e-commerce sector rather than with the protection of individuals. In the process, the legislators forgot not only about the undesirable characteristics of unsolicited commercial e-mail (unfairness, intrusiveness, costs borne by recipient), but also about the existing legislation and the considerations which had previously formed the basis for a clear, certain and proportionate rule.

The resulting consensus reached by the Member States in May 2000 was to make an oblique reference to the existing legislation. This veiled reference is the source of the current confusion which this study has described. What with the provision in the directive for regular consultation of opt-out registers and the prominent role played by e-commerce industry representatives in the discussions leading up to the directive, the majority within the industry now believe that the new directive represents the entire body of legislation applicable to unsolicited commercial communications. However, the 1995 directive is not abrogated solely by virtue of the e-commerce directive's failure to mention it.

Meanwhile, in the United States, the market was feeling its way towards a rule. A number of states enacted statutes making spamming a criminal offence. Then the e-mail marketing industry, faced with the fact that unpopular commercial practices inevitably result in binding legislation, decided to take on board the concerns of privacy advocates and to espouse the principles and practices of permission marketing.

Today, the situation in Europe is a hybrid

On the one hand, five countries – Germany, Austria, Denmark, Finland and Italy – have chosen an opt-in system.

On the other hand, most industry federations are in the process of setting up the opt-out registries referred to in the electronic commerce Directive 2000/31/EC. Some European federations are entering into partnership with American opt-out registers, although the commercial or legal point of such partnerships, which are operated for profit, is not clear. Finally, a number of European online businesses, having noted the commercial attractions of the opt-in approach and the beneficial effects of American-style permission marketing, have implemented systems based on prior consent.

Given this current situation, which it benefits nobody to maintain, the Commission proposal of 12 July 2000 for a directive concerning the processing of personal data and the protection of privacy in the electronic communications sector (66) is timely indeed. It is intended to replace Directive 97/66/EC of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector.

---

66) 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, OJ COM (2000) 385, of 12 July 2000.

The Commission's stated objective is to make the Community's data privacy regulatory framework technology-neutral.

In addition to this explicit aim, it may be observed that the Commission proposal also has the considerable merit of being "sector-neutral" in relation to unsolicited commercial communications i.e. it is proposed that the requirement of prior consent to unsolicited commercial communications should apply irrespective of the sector in which the sender carries on business – telecommunications, mail order, e-commerce or direct marketing of financial products and services.

This is the thrust of the revised version of Article 12 (Unsolicited Calls) of Directive 97/66/EC contained in Article 13 of the Commission proposal for a new directive, which would provide as follows: "The use of automated calling systems without human intervention [...], facsimile machines (fax) or electronic mail for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent".

The Commission's choice of an opt-in approach meets a pressing need, in the light of the findings of this report concerning the situation in Europe and in the US. But the proposed directive also represents a good opportunity to reconcile national laws – which are already going their separate ways even before the e-commerce directive has been transposed – and to establish a common European approach on the specific form prior consent should take, based on a definition of the exact scope of the concept of consent in a data privacy context.

The scope of consent

In Directive 95/46, "consent" is construed as the absolute exercise by an individual of his lawful rights. Thus, an individual can consent to the processing of data of a religious, political or otherwise sensitive nature (Article 8), to the transfer of his personal data to a third country which does not ensure an adequate level of protection (Article 26), or simply to processing in general absent any specific legitimate interest (Article 7(a)). This conforms to the theory of permission marketing: anything is possible once consent has been obtained.

This attitude throws up a number of political and legal issues. In relation to the marketing of personal data, the paramount consideration of individual consent suggests that a two-tier system of data protection may emerge, with one level of protection for the less well off, which would diminish accordingly as these data subjects granted further consent and waived their rights in response to commercial offers, and a lower level of protection for the better off, whose financial well-being provides a sufficient safeguard for their freedom of consent.

But all this is subject to two provisos. First, from a legal standpoint, consent can be given only in respect of data processing for a defined purpose. The scope of consent will therefore depend in practice on the clarity and transparency of the

prior information supplied to the data subject. Secondly, consent may be revoked at any time by the data subject, either by exercising his right to object to any further processing of his data or by exercising his right to have his processed data erased.

However, even with these provisos there remains the fear that consent, which is the expression of a quasi-absolute right, may be the means by which the data subject waives the protection offered him by data privacy legislation. In this regard, there are two crucial safeguards which are indivisibly linked to consent: the prior information given to the data subject regarding the scope of his consent (principle of informed consent) and the data subject's freedom of choice (principle of free consent).

The clarity requirement in respect of the information to be given to the data subject when he grants his consent is also a necessary consequence of the timing of the act of consent, which is obtained prior to collection of the data.

Thus, in marked contrast to the exercise of the right to object, which may be exercised either ex ante upon collection of the data (refusal to receive commercial communications) or ex post at any time (request to receive no further commercial communications), consent by its nature must be construed as being granted prior to the act of marketing.

The procedures by which consent can be given online must be spelled out

The American-style opt-in involves obtaining the Internet user's express authorisation, sometimes coupled with a confirmation (double opt-in). This was developed in the absence of a legal framework: the market was able to choose freely the rules which it perceived as eliciting the greatest level of trust on the part of Internet users and providing legal certainty for the e-commerce merchant. In this instance, the most protective rule advocated by the exponents of permission marketing is that of prior express authorisation.

According to US practice, the procedure for obtaining consent which provides the highest level of legal certainty is the double opt-in, whereby the Internet user confirms his consent by re-sending to the party collecting his e-mail address a message mailed by the latter following the collection of the address.

In Europe, it is surprising to note that neither the Member States represented on the committee established by Article 31 of the directive, nor the national supervisory authorities represented on the Article 29 Working Party have yet adopted any official opinion describing the conditions or manner of obtaining consent prior to the processing or transfer of data. It may be that the Member States did not regard agreement on this matter as urgent, probably because of the perceived merits of keeping the legal provisions general.

In this regard, it may be recalled first that the 1995 directive provides a very stringent definition in Article 2(h): "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed". A straight reading of this definition, taking account of the language used ("indication of his wishes by which the data subject signifies his agreement") seems to indicate that there can only be one possible form of consent: express authorisation consisting of (1) a positive act of the will (2) in favour of something.

However it must also be remembered that the 1995 directive provides for several categories of consent: "unambiguous consent" to the processing of personal data (Article 7(a)) and to the transfer of personal data to a third country which does not ensure an adequate level of protection (Article 26), and "explicit consent" (Article 8.2(a)) to the processing of sensitive data (political, religious, philosophical opinions etc.).

The existence of these two concepts of consent – "unambiguous consent" and "explicit consent" might lead one to wonder in what circumstances an individual's consent could be deemed unambiguous but not explicit. This is a source of legal uncertainty which was manifestly not intended by the Community legislator in view of the precise and unequivocal definition of consent in Article 2(h).

The requirement of an acknowledgment of receipt of orders placed, laid down by Article 11(1) of Directive 2000/31/EC, might well be invoked by proponents of a European double opt-in system. They might argue that this requirement can apply to any form of commitment given online. Accordingly, an individual providing his e-mail address with a view to receiving commercial information on a particular product or service would receive a request for confirmation of this "order" in his inbox to be re-sent to the e-commerce merchant as proof of the confirmed order (the double opt-in).

It must be pointed out however that Article 11(3) of the directive is of no assistance to this point of view as it expressly excludes e-mail exchanges from the scope of Article 11(1).

Consequently, the most obvious way to make certain that the web surfer has given his consent to receiving commercial e-mail would be to make it obligatory for him to express his wishes on the matter. Thus, when data are being collected from an Internet user, the procedure for obtaining consent could take the form of requiring a tick to be placed in a box in a registration form. This specific manner of obtaining consent would satisfy the definition given in Article 2(h) of the 1995 directive. Unless the web surfer takes the active step of ticking the consent box, consent cannot be regarded as having been given.

Obtaining prior consent would thus consist of enabling the individual, at the time he supplies his data (via the medium through which the data are collected), to indicate explicitly whether he agrees or does not agree to be sent further commercial communications. At the same time, great care must also be taken to

ensure the clarity of information provided to the Internet user as to the consequences of ticking the box.

If a procedure of this kind is used for data collection, personal data can be recorded together with the conditions which the data subject has attached to their processing. In this regard, it is clear that best that can be said about the practice of using boxes which are already ticked is that it shows up the data collector's dubious intentions.

This procedure for obtaining consent, because it operates at the time when the e-mail address is initially collected, automatically promotes fairness in the collection of data, one of the core principles of existing data privacy legislation.

It is geared towards the productive use of data collected directly via an electronic medium: the collection of the data and the associated rights must be concomitant in order to allow the data to be used immediately for commercial purposes and in the certain knowledge that personal rights have been respected.

The transparency of the prior consent procedure must be seen as a standard requirement and everybody must understand that it is detrimental to the growth of e-commerce if before making a purchase prospective web shoppers have to make inquiries in order to satisfy themselves of the fairness of the e-commerce merchant concerned.

Annex 1 **:**
Anti-spam Policies of the e-mail marketing companies

SPAM POLICY

Overview:
Neither Exactis.com Inc. nor Exactis.com Express, Inc. (collectively referred to herein as "Exactis.com") condones unsolicited, off-topic bulk e-mail ("Spam"); thus, Exactis.com prohibits the practices commonly known as "*spamming*." This document defines Exactis.com's policy regarding Spam and applies to the clients of Exactis.com.

Purpose:
E-mail is a powerful and focused communication tool. Used effectively it can help establish valuable relationships with your customers. Used improperly it can cause irreparable harm and undermine the value of an important communication line between you and your customers. Based on considerable experience with our own subscriber lists and others' mailing lists, certain guidelines should be followed to maximize the effectiveness of e-mail as a relationship-building tool.

Definitions:
"List" is a set of e-mail addresses provided by the client to Exactis.com for the purpose of sending e-mail to them. "Opt-In Approach" is a method whereby a person who wishes to subscribe must request to be added to the List. "Opt-Out Approach" is a method whereby a person is automatically subscribed, and they must ask to be removed from the List.

Summary:
To comply with Exactis.com's Spam policy, demonstrable evidence must exist that the e-mail, its objective and its sender fits expectations established with the subscriber when they provided their e-mail address.

Policy:

1. **Subscriber Expectations**
   If the subscribers deliberately provided their e-mail addresses to receive the e-mail to be sent, Exactis.com will send the mail. If the subscribers are not expecting the e-mail as a direct result of providing their e-mail addresses, the issue of content relevance must be addressed.

2. **Content Relevance**
   A determination must be made whether the content of the mailing contains subject matter relevant to the List. That is, the content of the e-mail must reasonably fit subscribers' expectations of what they were going to receive when they provided their e-mail address. For instance, a subscriber who elected to receive recent news items about high-tech developments could reasonably expect to receive Silicon Valley updates from the same content provider, but would not reasonably expect to receive general world news.

   After a dialogue with the client about relevance, Exactis.com will make a determination regarding send viability. In the rare event of a difference of opinion, small scale testing of a List can be conducted to provide additional data for a decision by Exactis.com. If relevancy exists, the subscribers may be added to a List through an Opt-In Approach or Opt-Out Approach mailing. Opt-Out Approach mailings are only available if a previous relationship exists between the client and the addressee. The Opt-In Approach mailing may be either a multiple issue trial (of reasonable duration) or a one-time mailing (announcing the offer). Any Opt-In Approach or Opt-Out Approach mailing must explicitly inform the end-user of the situation and their options to subscribe or unsubscribe.

   If relevancy does not exist, Exactis.com will not send the proposed mailing until the client has taken measures to allow subscribers to choose to participate in the List or not.

3. **Additional Principles:**
   In the event the source of a List or expectations of all users on a particular List is unclear, or the duration of the time between when the addresses were collected and the first e-mail is to be sent could cause confusion, clarity must be provided in the form of a preamble in each of the first two e-mails sent. The preamble must explain whom the e-mail is from, the reason the person is receiving the message and the possible source of the e-mail address (i.e. ways in which the address may have been gathered by the client) and clear instructions on how to unsubscribe.

Any client supplying Exactis.com with a new List to be added to the system or new subscribers to be added to an existing List will be required to represent and warrant that the new names adhere to Exactis.com's policy regarding the source of names.

When an e-mail address is provided, the user should have clear expectations regarding information the client plans to send. This expectation should be based on direct notice from the client.

Unsubscribe instructions must be made readily available with in the e-mail body to all recipients.

Forging of header information (the practice of making it appear as though an e-mail message originated from another source) or intentionally misleading subject lines is not permitted.

Publishers may not forward or otherwise propagate chain letters, whether or not the recipient wishes to receive such mailings.

Malicious e-mail, including but not limited to "mailbombing" (flooding a user or site with very large or numerous pieces of e-mail), is prohibited.

All one-time or announcement mailings completed for a client must adhere to these same policies.

Exactis.com reserves the right at any time to implement technical mechanisms to prevent such activities, refuse to send e-mail that does not meet the aforementioned requirements, terminate service or take other legal action against any Customer that engages in or tolerates *spamming* or any other illegal, harassing, obscene or other potential liability-causing activity. Exactis.com reserves all legal and equitable rights in enforcing this policy.

Note: This policy has been created in conjunction with widely accepted policies on the Internet. In addition, Exactis.com has conducted extensive tests, using our own subscribers, in setting these policies. These tests generated measurable results that were used to form the basis of this policy.

Ten Rules for Permission-based E-mail marketing

Marketers everywhere are embracing opt-in e-mail marketing. Though similar in many ways to traditional direct marketing, opt-in e-mail operates under very different rules. Those who violate the rules are often deluged with complaints and find that response rates suffer. These guidelines will help you avoid the problems and focus on success.

1. **Send e-mail only to those who have "opted-in" to receive it.**
   Ideally you should use "confirmed" opt-in, in which a confirmation message must be sent to the recipient, who in turn must reply to the message for the opt-in to take effect. Avoid "opt-out," which forces the recipient to receive messages until he says no. This widespread practice of opt-out appears to actually discourage e-commerce. A recent survey by Intelliquest found that 63% of Web users agreed with the statement, "If I buy online, I'll end up getting junk e-mail." And the trend is up - Intelliquest found only 58% agreed with that statement in 1998. Perhaps this is why many people use fake e-mail addresses when buying online; Shop.org found in a 1998 survey that 60% of surfers have given false information when filling out online forms.
   Bottom line: Consumer trust is something you have to earn. One of the best ways is to respect their wishes when it comes to e-mail.
2. **Always honor user requests to opt-out.**
   Make it a simple process and include a Web site URL in every message that allows the user to opt-out. (A simple "reply to unsubscribe" does not always work if the user has multiple e-mail accounts, which can be extremely frustrating for the end user.) For some companies, it might make sense to "downsell" the end user. For example, a news site that provides daily deliveries may have success in offering the user an opportunity to "downgrade" to weekly digests. After all, many opt-outs are simply a natural reaction to too much e-mail in general; a reduced burden is often welcome.
3. **Confirm everything by e-mail: The initial opt-in, orders, shipping notification and changes in the customer profile.**
   This blunts the problem of false information. If a fake e-mail address has been entered, the confirmation will either bounce or be delivered to someone who possibly has never heard of you, in which case he will contact you and let you know your database needs to be updated. Always include an opt-out mechanism in these messages. As an added bonus, use these messages as an upsell opportunity. For example, an airline could offer the user a reduced rate for renting a car from a particular sponsoring vendor.
4. **Allow users to specify their preferences.**
   What kind of information do they want to receive? How often? Encourage users to give you as much information as necessary to allow you to effectively target them in your e-mail promotions and other e-commerce activities. But avoid asking for her life story. Instead, structure your program so that you gain more information over time -- with her permission, of course!
5. **Give and you shall receive.**
   Customers don't give you their e-mail address and other personal information out of altruism. They do it in exchange for something of value. It could be information (on your Web site, via e-mail or through some other media), a free gift, a coupon or a chance to win a sweepstakes. Be creative, but also follow through by delivering real value to the recipient with every message.
6. **Your list is an asset that only you can use; do not sell or rent it.**
   If you want to realize incremental revenue beyond your own offerings, allow the users to opt-in to receive offers from your partners. If you do this, make sure you control the mailings, and that your brand "introduces" other brands. Example: "Because you opted to receive promotional offers of our valued partners, we at ABC Corp are please to give you a special offer from XYZ Corp." Ask the company doing the promotion to give you

an exclusive on the offer for a limited time; limiting the offer to only your customers increases the value of opting in.

7. **Develop and post a privacy policy for your web site.**
   Do NOT violate it!
8. **Respond to customer e-mail inquiries promptly.**
   It reinforces how valuable they are to you and reminds them that there are real, live people "behind the scenes" of your web site.
9. **Do not use rented lists.**
   The only exception is vendors who use the method described in number 6.
10. **Always remember the network effect.**
    Bad news travels much faster than good on the Internet.
    An angry online customer can broadcast his ire to million by creating an "I hate [your company]" Web site, e-mailing the experience to friends, posting it on message boards and other ways. Remember, in the new economy the customer is in control. Do not make the mistake of treating e-mail and the Web like the telephone and snail mail.

Our List Member Guarantee

1. **Your privacy will be protected.**
   At NetCreations, we respect your right to privacy. Your name, e-mail address, zipcode and any other identifying information that you give us will not be revealed to any of the direct marketers who rent our lists. Should we ever change our policy, you will be given the chance to remove yourself from our lists before your information is disclosed.
2. **You will not be spammed.**
   We hate spamming, and we know that you do, too. When you sign up for our PostMasterDirect.com mailing lists, you will receive commercial e-mail messages only about those topical categories that you have selected. Before any mailing goes out, our staff personally screens each marketer's message to make sure that it's relevant to the list's topic.
3. **You will be able to get off our lists at any time, no questions asked.**
   Just because you joined a list a month ago doesn't mean you want to stay on it forever. Every PostMasterDirect.com message we send out is coded with a special header and footer that allows you to remove your name from all lists automatically by forwarding the message to deleteall@postmasterdirect.com. We also offer a Subscription Review Service at http://review.postmasterdirect.com that enables you to unsubscribe from specific lists and update your personal profile

Annex 2 :

References and extracts from national laws mentioned in the study which require an opt-in approach

Germany:

Federal Telecommunications Act of 31 July 1996 (extracts)

Unofficial English translation available on the Federal Data Protection Agency's website at: http://www.bfd.bund.de/information/tkgeng.pdf

§89 Data Protection :

(1) The Federal Government shall issue, by ordinance having the force of law with the consent of the German Bundesrat, provisions on the protection of the personal data of those engaging in telecommunications which govern the collection, processing and use of such data for companies commercially providing telecommunications services or contributing to the provision of such services. These provisions shall take account of the principle of reasonableness, specifically of restricting collection, processing and use to that which is necessary, and the principle of purpose-tying. Maximum storage periods shall be laid down and overall the justified interests of the company and parties concerned taken into account. Particulars of legal persons who are subject to telecommunications secrecy shall be treated as
equivalent to personal data.

(2) Companies and persons commercially providing telecommunications services or contributing to the provision of such services may, in accordance with the applicable ordinance, collect, process and use the data of natural and legal persons insofar as this is necessary:

[...] (7) **The companies and persons specified in (2) above may process and use personal data which they have collected for the establishment, framing of the content or modification of a contractual relationship insofar as this is required for purposes of advertising, customer consulting or market research for the companies and persons specified in (2) above and the customer has given his consent.** Personal customer data already collected by the companies and persons specified in (2) above at the date of entry into force of this Act may be processed and used for the purposes referred to in sentence 1 above if the customer does not raise any objections. His consent shall be deemed given if he has been adequately informed but has not made use of his right of objection.

Germany (continued) :

Federal Teleservices Data Protection Act of 13 June 1997 (extracts)

Unofficial English translation available on the website of the Data Protection Commissioner of Berlin Land at:
http://www.datenschutz-berlin.de/recht/de/rv/tk_med/iukdg_en.htm#a2

Article 5, § 2

1. The provider may collect, process and use the personal data of a user to the extent necessary the data are required for concluding with him a contract on the use of teleservices and for determining or modifying the terms of such contract (contractual data).

2. Processing and use of contractual data for the purpose of advising, advertising, market research or for the demand-oriented design of the teleservices is only permissible if the user has given his explicit consent.

Federal Treaty on Mediaservices of 23 June 1997 (extracts)

German text using the same wording as the Teleservices Act of 13 June 1997, available on the website of the Data Protection Commissioner of Berlin Land at:
http://www.datenschutz-berlin.de/recht/de/stv/mdstv.htm#nr14

Article 14, § 2

1. Der Anbieter von Mediendiensten darf personenbezogene Daten eines Nutzers erheben, verarbeiten und nutzen, soweit sie fur die Begrundung, inhaltliche Ausgestaltung oder Anderung eines Vertragsverhaltnisses mit ihm uber die Nutzung von Mediendiensten erforderlich sind (Bestandsdaten).

2. Eine Verarbeitung und Nutzung der Bestandsdaten fur Zwecke der Beratung, der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung technischer Einrichtungen des Anbieters ist nur zulassig, soweit der Nutzer in diese ausdrucklich eingewilligt hat.

Austria:

Telecommunications Act (extract)

Unofficial English translation of section 101 of the Telecommunications Act which entered into force in August 1999

Section 101

Calls - including fax transmissions - for advertising purposes that do not have the prior consent of the subscribers are not permitted. Consent may be withdrawn at any time; unsolicited bulk e-mail or unsolicited commercial e-mail shall require the recipient's prior consent, which may be withdrawn at any time.

Denmark:

Act n° 418 of 31 May 2000 (extract)

Unofficial English translation of the legislation transposing Directive 97/66/EC into Danish domestic law

Article 6a(1)

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

Article 6a(2)

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

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

Finland:

Act n° 1999/565 of April 1999

Unofficial English translation of the legislation transposing Directive 97/66/EC

Section 21 – Telecommunications in direct marketing

1. Telecommunications may not be used for direct marketing without the prior consent of the subscriber if the calls to the called subscriber are made by means of automated calling systems or facsimile machine unless otherwise decided by the ministry under paragraph 4.

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

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

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

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

   - in telecommunications referred to in paragraph 2 require prior consent of the subscriber.

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

Section 22 – Availability of refusals to accept regarding direct marketing

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

Italy:

Implementing Decree n°171 of 13 May 1998

Transposing into Italian law Directive 97/66/EC and those provisions of Directive 95/46/EC which concern the work of journalists

Unofficial English translation

Article 10 - Unsolicited calls

5. The use of automated calling systems without human intervention or facsimile machines for the purposes of direct marketing or sending advertising materials, or else for carrying out market surveys or interactive business communication shall only be allowed with the subscriber's express consent.

6. Any calls made for the purposes referred to in paragraph 1 by means other than those mentioned therein shall be allowed in pursuance of Articles 11 and 12 of the Act.

Act n° 675 of 31 December 1996

Transposing Directive 95/46/EC into Italian law

Article 11 - Data subject's consent

1. Processing of personal data by private entities or profit-seeking public bodies shall be deemed lawful only if the data subject gives his express consent.

2. The data subject's consent may relate to the overall processing or to one or more of the operations thereof.

3. The data subject's consent shall be deemed to be effective only if it has been given freely, in a specific form and in writing and if the data subject was provided with the information as per article 10.

Article 12 - Cases in which the data subject's consent is not required

1. The data subject's consent shall not be required :

a) if the processing concerns data collected and kept in compliance with an obligation imposed by a law, regulations or Community legislation;

b) if the processing is necessary for the performance of obligations resulting from a contract to which the data subject is a party, or for gathering information at the data subject's request prior to entering into a contract, or for the performance of a lawful obligation;
c) if the processing concerns data extracted from public registers, lists, documents or records which are publicly available;
d) *if the processing is carried out exclusively for scientific research or statistics purposes and complies with the codes of conduct and professional ethics undersigned in pursuance of Article 31*;
e) if the processing is carried out within the scope of the journalistic profession and for the sole purposes related thereto. *In the latter case, the* code of conduct referred to in article 25 *shall apply*;
f) if the processing concerns data relating to economic activities which have been collected, *inter alia*, for the purposes mentioned in para. 1, subheading *e*), of article 13 without prejudice to the laws in force regarding business and industrial secrecy;
g) if the processing is necessary to safeguard life or bodily integrity either of the data subject or of a third party, and the data subject cannot give his consent because of physical or legal incapacity or mental disorder;
h) if the processing is necessary for carrying out the investigations referred to in article 38 of the implementing, coordination and transitional provisions of the Criminal Procedure Code as approved by legislative decree no. 271 of 28 July 1989, subsequently amended, or else for the exercise or defence of a legal claim, provided that the data are processed exclusively for said purposes and for no longer than is necessary therefor.

Article 13 - Data subject's rights

1. In respect of the processing of personal data, any data subject shall have the right to:

2.

a) be informed, by having access, free of charge, to the register mentioned under paragraph 1, subheading *a*), of article 31, of the existence of the processing of data that may concern him;
b) be informed of what is mentioned under paragraph 4, subheadings *a*), *b*) and *h*), of article 7;
c) obtain, without delay, either from the controller or from the processor:
1 - confirmation as to whether or not personal data relating to him exist, regardless of their being already recorded, and the intelligible communication of such data and their source, as well as of the logic and the purposes underlying the processing; such request is renewable at intervals of not less than ninety days, unless there are well-grounded reasons therefore;
2 - the erasure, blocking or anonymization of data which have been processed unlawfully, including those the keeping of which is not necessary for the purposes for which they were collected or subsequently processed;

3 - the updating, rectification or, where interested therein, integration of the data;
4 - the statement that the operations as per 2) and 3) above have been notified, as also related to their contents, to the subjects to whom the data were communicated or disseminated, except when the provision of such information proves impossible or involves a manifestly disproportionate effort compared with the right that is to be protected;

d) object, in whole or in part, on legitimate grounds, to the processing of personal data relating to him, even though relevant to the purpose of the collection;
e) **object, in whole or in part, to the processing of personal data relating to him which is carried out for purposes of commercial information or advertising or direct marketing, or else for the performance of market or interactive commercial communication surveys, and be informed by the controller, no later than at the time when the data are communicated or disseminated, of the possibility to exercise such right free of charge.**

2. Where it is not confirmed that personal data relating to the data subject exist, the latter may be charged a sum which shall not be greater than the expenses actually incurred, for each request as per para. 1, subheading *c*), number 1), in accordance with the modalities and within the limits set out by the regulations as per article 33(3).The rights as per paragraph 1, where relating to the personal data of a deceased, may be exercised by anyone who is interested in them.

3. The data subject may grant, in writing, power of attorney or representation to natural persons or associations in the exercise of the rights as per paragraph 1.

4. The provisions concerning professional secrecy of the journalistic profession shall further apply as related to the source of the information.

Annex 3 :

List of individuals and organisations consulted for the study

I - NATIONAL DATA PROTECTION AUTHORITIES

Title	First name	Surname	Position	Name of authority	Country
Dr	Waltraut	**KOTSCHY**	Chairman	Datenschutzkommission und des Datenschutzrates	AUSTRIA
Dr	Gustav	**MAIER**		Datenschutzkommission und des Datenschutzrates	AUSTRIA
Dr	Anton	**SPENLING**		Datenschutzkommission und des Datenschutzrates	AUSTRIA
Mr	Paul	**THOMAS**	Chairman	ComMsion de la Protection de la Vie Privée	BELGIUM
Ms	Lotte	**JORGENSEN**		Datatilsynet	DENMARK
Dr	Helmut	**BAÜMLER**	LfD D	Der Landesbeaufragte für den Datenschutz bei der Präsidentin des Schleswig-Holsteinischen Landtages	GERMANY
Dr	Ulrich	**DAMMANN**	LfD D	Der Bundesbeaufragter fur den Datenschutz	GERMANY
Mr	Bernd	**DANNEMANN**	LfD D	Der Landesbeaufragte für den Datenschutz	GERMANY
Mr	Alexander	**DIX**	LfD D	Der Landesbeaufragte für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg	GERMANY
Dr	Gerhard	**DRONSCH**	LfD D	Der Landesbeaufragte für den Datenschutz Niedersachsen	GERMANY
Dr	Hansjürgen	**GARSTKA**	LfD D	Der Berliner Datenschutzbeaufragte	GERMANY
Mr	Sven	**MÖRS**		Der Berliner Datenschutzbeaufragte	GERMANY
Dr	Thomas	**GIESEN**	LfD D	Der Sächsische Datenschutzbeaufragte	GERMANY
Dr	Rainer	**HAMM**	LfD D	Der Hessiche Datenschutzbeaufragte	GERMANY
Dr	Joachim	**JACOB**	LfD D	Der Bundesbeaufragter fur den Datenschutz	GERMANY
Mr	Klaus-Reiner	**KALK**		Der Landesbeaufragte für den Datenschutz Sachsen-Anhalt	GERMANY
Dr	Werner	**KESSEL**	LfD D	Der Landesbeaufragte für den Datenschutz Mecklenburg-Vorpommern	GERMANY
Ms	Silvia	**LIEBAUG**	LfD D	Der Thüringer Landesbeaufragte für den Dantenschutz	GERMANY
Dr	Walter	**RUDOLP**	LfD D	Der Landesbeaufragte für den Datenschutz Rheinland-Pfalz	GERMANY
Dr	Hans-Hermann	**SCHRADER**	LfD D	Der Hamburgische Datenschutzbeaufragte	GERMANY
Ms	Bettina	**SOKOL**	LfD D	Die Landesbeaufragte für den Datenschutz Nordrhein-westfalen	GERMANY
Mr	Reinhard	**VETTER**	LfD D	Der Bayerische Landesbeaufragte für den Datenschutz	GERMANY
Ms	Elisabeth	**FRANCE**	Commissioner	Data Protection Commissioner	UNITED KINGDOM
Mr	Juan-Manuel	**FERNANDEZ-LOPEZ**	Chairman	Agencia de Proteccion de Datos	SPAIN
Mr	Reijo	**AARNIO**	Ombudsman	Data Protection Ombusdsman	FINLAND
Mr	Konstantinos	**DAFERMOS**	Chairman	Hellenic Data Protection Authority	GREECE
Mr	Fergus	**GLAVEY**	Commissioner	Data Protection Commissioner -	IRELAND

Dr	Giovanni	**BUTTARELLLI**	Secretary	Garante per la Protezione dei data Personali	ITALY
Prof.	Stefano	**RODOTA**	Chairman	Garante per la Protezione dei data Personali	ITALY
Prof.	Giuseppe	**SANTANIELLO**	Vice- Chairman	Garante per la Protezione dei data Personali	ITALY
Mr	René	**FABER**	Chairman	Commission à la Protection des données nominatives	LUXEMBOURG
Mr	Peter J.	**HUSTINX**	Chairman	Registratiekamer	NETHERLANDS
Mr	Georg	**APENES**	Chairman's Office	Data Inspectorate	NORWAY
Dr	Joao	**LABESCAT DA SILVA**	Chairman	Commissao Nacional de Protecçao de Dados Pessoais Informatizados	PORTUGAL
Mr	Ulf	**WIDEBËCK**	Chairman	Datainspektionen	SWEDEN

II – INDUSTRY ORGANISATIONS

Title	First name	Surname	Position	Organisation	Country
Mr	Thomas	**BERENDT**	Secretary	BUNDESVERBAND DES DEUTSCHEN	GERMANY
Mr	Hasso	**HERBST**	Managing Director	DDV	GERMANY
Mr	Michael	**SCHNEIDER**	Director of Regulation/ Self-Regulation	EuroISPA	GERMANY
Mr	Thomas	**STEINMARK**	Secretary	BUNDESVERBAND DES DEUTSCHEN	GERMANY
Mr	Klaus	**WIRTH**	President	BUNDESVERBAND DES DEUTSCHEN	GERMANY
Ms	Hildergard	**FISCHER**	Secretary	HANDELSVERBAND ARBEITSGRUPPE VER-SANDHAUSER	AUSTRIA
Mr	Joseph	**HAMBERGER**	Secretary	DIRECT MARKETING VERBAND OSTER	AUSTRIA
Mr	Paul	**MAILATH POKORNY**	Chairman	HANDELSVERBAND ARBEITSGRUPPE VER-SANDHAUSER	AUSTRIA
Mr	Helmut	**RITTER**	AEVPC Correspondent	RITTER CONSULTING	AUSTRIA
Mr	Michel	**CASTERS**	Président	BDMV/ABMD	BELGIUM
Mr	Dirk	**FRANS**	Director General Business Development	FEDMA (Federation of European Direct Market-ing)	BELGIUM
Mr	Didier	**LAHACHE**	President	ASSOCIATION EUROPEENNE DE VENTE PAR CORRESPONDANCE	BELGIUM
Mr	Rudi	**ROTH**	Secretary General	EuroISPA	BELGIUM
Mr	Alastair	**TEMPEST**	Director General Public Af-fairs & Self Regulation	FEDMA	BELGIUM
Mr	Paul	**VAN LIL**	Secretary General	BDMV/ABMD	BELGIUM
Mr	Aad	**WEENING**	Secretary General	ASSOCIATION EUROPEENNE DE VENTE PAR CORRESPONDANCE	BELGIUM
Mr	Erick	**RYGE**	Secretary General	DANSK POSTORDREFOREINING	DENMARK
Ms	Elena	**GOMEZ DEL POZUELO**	Secretary General	FECEMD	SPAIN
Ms	Elena	**GOMEZ DEL POZUELO**	Secretary General	AEMD	SPAIN
Mr	Miguel	**REIRIS**	President	FECEMD	SPAIN
Mr	Miguel	**REIRIS**	President	AEMD	SPAIN
Mr	Jouko	**KOVERO**	President	SSML	FINLAND
Mr	Sakari	**VIRTANEN**	Secretary General	SSML	FINLAND
Mr	Serge	**AUMONT**		Comité Réseaux des Universités (CRU)	FRANCE
Mr	Antoine	**BEAUSSANT**	President	Groupement des Editeurs de Services en ligne	FRANCE

				(GESTE)	
Ms	Nadia	**BELMOURI**	Secretary	ACSEL	FRANCE
Mr	Hubert	**BRIN**	President	Union Nationale des Associations Familiales (U.N.A.F.)	FRANCE
Mr	Henri	**de MAUBLANC**	President	Association pour le Commerce et les services en Ligne (ACSEL)	FRANCE
Mr	Etienne	**DUPONT**	Director	Association Française de Normalisation (AFNOR)	FRANCE
Mr	Jean-Christian	**FANDEUX**	President	Fédération des Entreprises de Vente à Distance (FEVAD)	FRANCE
Mr	Georges	**FISCHER**		Chambre de Commerce et d'Industrie de Paris	FRANCE
Mr	Michel	**FRANCK**	President	Chambre de Commerce et d'Industrie de Paris	FRANCE
Ms	Marie-Agnès	**GIROUD**	Chargée de Mission	Association pour le Commerce et les services en Ligne (ACSEL)	FRANCE
Mr	Noël	**GOUTARD**	Vice-Président du groupe "RECHERCHE ET INNOVATION"	Mouvement des Entreprises de France (MEDEF)	FRANCE
Mr	Eric	**HAYAT**	Président du groupe "RECHERCHE ET INNOVATION"	Mouvement des Entreprises de France (MEDEF)	FRANCE
Mr	Jacques	**KUNTZ**	Président de la Délégation de Paris	Chambre de Commerce et d'Industrie de Paris	FRANCE
Mr	Gérard	**LADOUX**	Secrétaire Général	Association pour le Commerce et les services en Ligne (ACSEL)	FRANCE
Mr	Jean-Christophe	**Le TOQUIN**	Vice-Président	EuroISPA	
Mr	Jean-Christophe	**Le TOQUIN**	Délégué Permanent	Association des Fournisseurs d'accès et de services Internet (AFA)	FRANCE
Mr	Jean-Pierre	**LEVIEUX**	Président	IAB France	FRANCE
Ms	Véronique	**MILAN-BESLAY**	Chargée de la communication	Union Française du Direct marketing	FRANCE
Mr	Jean-Marc	**PINCET**	Directeur du Pôle Juridique	Association Française de Normalisation (AFNOR)	FRANCE
Mr	Pascal	**POUPET**	Dép.Technologies de l'Information et Communication	Association Française de Normalisation (AFNOR)	FRANCE
Mr	Bernard	**SIOUFFI**	Délégué Général	Fédération des Entreprises de Vente à Distance (FEVAD)	FRANCE
Ms	Marie-France	**TULASNE**	Secrétaire	Association pour le Commerce et les services en Ligne (ACSEL)	FRANCE
Ms	Delphine	**VARA**	Executive Manager	Chambre de Commerce Internationale (ICC)	FRANCE
Mr	Lionel	**WALSH**	Directeur des communications	Chambre de Commerce Internationale (ICC)	FRANCE

Mr	Jim	**DIXON**	Director of Telecommunica-tions Issues	EuroISPA	UNITED KING-DOM
Mr	Colin	**FRICKER**	Legal Affairs	THE BRITISH DMA	UNITED KING-DOM
Mr	Malcolm	**LANDAU**	Secretary	THE MAIL ORDER TRADER'S ASSOCIATION	UNITED KING-DOM
Mr	Colin	**LLOYD**	Chief Executive	THE BRITISH DMA	UNITED KING-DOM
Mr	Jim	**MARTIN**	President	THE MAIL ORDER TRADER'S ASSOCIATION	UNITED KING-DOM
Mr	Ewan	**BYRNE**	President	THE IRISH MAIL ORDER ASSOCIATION	IRELAND
Mr	Howard	**JACOBS**	Secretary	THE IRISH MAIL ORDER ASSOCIATION	IRELAND
Mr	Bill	**MOSS**	Chairman	IRISH DMA	IRELAND
Mr	John	**O'ROURKE**	Treasurer	IRISH DMA	IRELAND
Mr	Paolo	**LAVINO**	President	ANVED	ITALY
Mr	Mirko	**PLANTA**	Managing Director	AIDIM	ITALY
Mr	Pier-Attilio	**RUBINI**	Secretary	ANVED	ITALY
Mr	Pietro	**SANFELICE MORTEFORTE**	President	AIDIM	ITALY
Mr	Arne	**EGGEN**	Chairman	NORSK DIREKTE MARKEDSFORDING FOR	NORWAY
Mr	Eddy	**HANSEN**	President	NORSK POSTORDREFORENING	NORWAYE
Mr	Tore	**KVARUD**	Secretary	NORSK POSTORDREFORENING	NORWAY
Mr	Herbert	**HAAIJ**	President	DMSA	NETHERLANDS
Mr	Gerard	**MARSMAN**	President	NEDERLANDSE POSTORDERBOND	NETHERLANDS
Mr	Menno	**VAN DER PUT**	Secretary General	NEDERLANDSE POSTORDERBOND	NETHERLANDS
Mr	Frits	**VAN DORST**	Managing Director	DMSA	NETHERLANDS
Mr	Joao	**NOVAIS DE PAULA**	Secretary General	ASSOCIACAO PORTUGUESA DE MD	PORTUGAL
Mr	Tom	**EKELUND**	President	SWEDISH DMA	SWEDEN
Mr	Erick	**GRONBERG**	Secretary General	SWEDISH DMA	SWEDEN
Mr	Lennart	**HELGESSON**	Secretary General	SVENSKA POSTORDER FORENINGEN	SWEDEN
Mr	Gunnar	**RYMAN**	President	SVENSKA POSTORDER FORENINGEN	SWEDEN