COMMISSION OF THE EUROPEAN COMMUNITIES

Unsolicited Commercial Communications and Data Protection

Summary of Study Findings (*) – January 2001

Serge Gauthronet & Étienne Drouard

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 presently 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 commercial sale of personal data, the creation of vast databases of personal profiles, aggressive advertising, increasing use of unfair practices and serious infringements of privacy.

The Commission has been looking at these issues for a number of years and has taken a particular interest in the phenomenon of unsolicited commercial e-mail, more commonly known as "spam". It commissioned ARETE consultants Serge Gauthronet and Etienne Drouard to produce a comprehensive report on the matter.

The study consists of two parts: an industrial part and a legal part. In the industrial part, spam is looked at in its various manifestations, the way it has evolved over recent years, the technology it draws upon and the practices followed by its exponents. This part of the study was carried out in the US, with a view to obtaining more meaningful results. This allowed ARETE to observe how American society has gradually responded to the pressure from the Internet community to devise ways of fending off the tidal wave of marketing messages inundating the nation's in-boxes. The discussion of the situation in the US also looks at the rise to prominence of new permission-based e-mail marketing strategies which are now being practised worldwide by a number of leading e-commerce players. Such privacy-friendly strategies change the parameters of the privacy protection issue without offering a completely satisfactory solution. The legal part of the study 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 rec-

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

ommendations 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 .

I) – The industrial aspects of e-mail marketing and spamming: general situation, practices and services offered

The findings of this study may be summarised in six main points which cover the economics of e-mail marketing, its history, current practices in the industry, its technological evolution and the new forms of permission-based marketing.

I.1) – The Internet has proved very fertile ground for interactive marketing as is demonstrated by the shift in advertisers' spending patterns in the United States. Already, direct marketing accounts for 50% of the overall advertising spend in the US. There are three main factors behind the rise in popularity of the Internet as an advertising medium:

- the costs of an advertising campaign on the Internet are a fraction of those for 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 postal campaign.

- sales conversion ratios for e-mail marketing range between 5 and 15% as compared to between 0.5% and 2% for conventional mailings.

- there is a significant gap in response rates between e-mail marketing – which achieves click-through rates (1) in the region of 18% - and banner advertising where rates have fallen steadily and have levelled off at 0.65%, according to Forrester Research; other sources (Nielsen Netratings – March 2000) report a drop from 2.5%, in the mid-90s to 0.36% in March 2000.

It is therefore highly plausible that over the next few years we will witness an increasing shift in spending towards direct marketing via the Internet and towards e-mail marketing in particular.

I.2) – Spam: the teething trouble of e-mail marketing. It is safe to say that the spam phenomenon, which emerged in the mid-90s largely in the United States, is now in decline. This is borne out by the various spammer black lists posted on the Internet which reveal that the phenomenon had its heyday between 1995 and 1998; the number of blacklisted spammers has been falling for about two years now. This recent development is due to four factors:

- **1st factor**: **action taken by ISPs** who have acquired considerable control over traffic passing through mail and news servers and have set up rapid reaction

1) 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.

mechanisms: the MAPS-RBL system for the Internet (the Mail Abuse Prevention System and the Realtime Blackhole List) (2) and UDP for the Usenet world *(Usenet Death Penalty).*

- **2nd factor**: **new laws passed in the USA** (3), which, while not without shortcomings, provide stiff penalties for spammers; the average being $10 per message up to a maximum of $25,000 per day; for small-scale operators with limited financial resources, this may represent a serious or even a massive deterrent.

- **3rd factor: action taken by trade associations**, in particular by the AIM – an autonomous subsidiary of the very powerful DMA – which took an outright and clear opposition against spamming, on the strength of some hard-nosed research which showed up the ineffectiveness of UCE by comparison with e-mail marketing based on a prior customer relationship; now, this year, the AIM has adopted a series of very clear guidelines condemning the kinds of practices engaged in by spammers. The DMA, whose own deliberations are at a less advanced stage, is now offering a stop-list service (e-MPS - *Electronic Mail Preference Service*) (4).

- **4th factor**: **the e-marketing counter-culture** which is increasingly espousing the principles of "permission marketing" as a reaction to the kind of saturation mass marketing which creates confusion in consumers' minds. Permission marketing means communicating with consumers on a voluntary basis, gradually evolving from a relationship based on interest to one based on trust. As trust is built up, the

---

2) Nowadays, the vast majority of ISPs hound the spammers remorselessly; one step they have taken has been to organise a network of voluntary administrators known as The Mail Abuse Prevention System (MAPS – Redwood City, Calif.) which operates the Realtime Blackhole List (RBL). This list is a mass boycott mechanism; through it, the system administrators of the ISPs who between them control thousand of routers and mail servers can share information regularly on spam attacks and ostracise the IP addresses and domain names which are known sources of UCE. Every terminated spammer subscription is posted to the list so that other ISPs – all 2,000 ISPs around the world who subscribe to the RBL, representing about 1/3 of the total market – are immediately aware if approached by the spammer of their prospective subscriber's true nature and can refuse to provide service. Apart from this basic information-pooling function, the MAPS system also acts as a filter which uses algorithms to automatically block messages from known spammers and from the ISPs hosting them, which are deemed to have failed in their duty to the online community as a whole to help keep the network free of junk.

3) Without waiting for Congress to act, more than twenty US states have already enacted or are in the process of enacting anti-spam legislation. These statutes have already been used to bring a number of lawsuits. Many of them also cover junk faxes. Their main provisions require opt-out registries to be set up and opt-out requests to be complied with, while they outlaw the key 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 the states, spam is defined as the sending of messages to Internet users without an express prior request on their part.

4) This is a free service which allows users to register their e-mail addresses in the stop-list, stating the categories of messages for which they wish to exercise an opt-out (business-to-consumer, business-to-business, or both). Direct marketers, for their part, can clear their e-mail address lists against the e-MPS system (non-members of the DMA are charged a fee of $100 for this service). The process is carried out online and takes only a few hours. The scheme has been fiercely criticised by American anti-spam campaigners, including representatives of MAPS, Junkbusters Corp. and CAUCE, and many DMA members are also strongly opposed to the DMA's approach. A central criticism is the fact that the DMA chose not to make the e-MPS system accessible to ISPs wishing to exercise a global opt-out in respect of their entire domain name and subscriber list. The DMA has defended its approach arguing that the scheme operates on the basis of the individual's right to opt out.

consumer is induced by customised and, of course, genuine offers (incentive marketing) to give permission for an ever-wider range of marketing activities: permission to collect more data on his or her lifestyle, hobbies and interests, permission to be sent messages advertising new products or services, permission to receive loyalty points, air-miles, free samples, trial subscriptions, etc. As this process unfolds, the anonymous individual becomes first a contact, then a prospect, then one day a customer and finally a loyal customer. Building a relationship of this kind demands time and regular contact, while keeping costs to a acceptable level if possible. What medium other than the Internet offers the same scope for interaction and stepwise 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, continuous contact can be maintained with prospects without overstretching advertising or consumer relations budgets (provided the process can be sufficiently automated) and printing costs are nil. The whole concept is vividly explained by Seth Godin, vice-president of Yahoo. More and more direct marketers and online businesses are buying into the permission marketing approach and discovering the power of the new concept of advertising campaigns targeted at willing and consenting audiences. In the United States today ***opt-in e-mail marketing*** is the talk of the industry***.***

II.3) – Spam still persists however, as can be seen from the **presence on the market of relevant products (spamware) and services**, supplied in the main by small-time operators. There are two categories of spamware: *pull* tools, which harvest e-mail addresses, and *push* tools, which carry out bulk mailings. The various harvesting programs on the market are quite simple to 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. All these products are claimed to beat the spam-traps set for them. The push tools, on the other hand, are engines capable of sending bulk e-mails without going through a specific mail server or a particular ISP. These widely available products turn the spammer's PC into a fully functioning mail server, avoiding the risk of being accused of hogging the ISP's bandwidth. These systems are powerful enough to break through the mail servers' anti-spam filters and forge message headers to perfection. It is somewhat paradoxical that such products are to found openly on the market, sold by apparently official distributors, given that their functionality includes mechanisms designed to divert Internet traffic, which is now outlawed in an increasing number of US states.

The services available can be divided into two main categories: campaign hosting, or host-spamming, and brokering of e-mail addresses. Hosts offer the complete range of services required to organise a spamming campaign; there are many small operators openly plying this trade on the Internet; their rates vary from $5 per 1000 for a straight mailing to $20 per 1000 if the client wants the addresses as well. Some specialise in providing a "bullet-proof" service, which is supposed to thwart the countermeasures taken by the ISPs. Address brokers are also numerous. Many offer three different membership packages, featuring different subscriptions to address lists. 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. Others offer lists of addresses online for immediate downloading: from $19.95 for 300 000, for example, to $49.95 for 1 000 000 Internet addresses and from $19.95 for 300 000 to $99.95 for 4 000 000 AOL addresses. The availability of so many lists of e-mail addresses inevitably raises the question as to the quality of the addresses concerned and their validity, not to mention whether genuine permission was obtained prior to their 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.

The spammers themselves, those still engaging in this risky and generally not welcome activity, tend to be amateurs or opportunists trying to peddle their ideas on the Internet. Many recent spam cases have been studied closely and the few cases known to have occurred in Europe show the spammers to be people who think nothing or very little of breaking the law but who now face a real risk of having substantial damages awarded against them – 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.

I.4) – In fact, **e-mail marketing is where the real action is. This is the busiest and most promising market,** in which strict application of privacy policies and the use of e-mail lists based on full consent are now de rigueur. The e-mail marketing model is far more powerful in financial and technological terms. The key features of the model are honesty 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 trend for the Internet marketing of tomorrow. It is worthwhile taking a closer look at their concept of privacy protection, based on ***opt-in e-mail lists***.

Some fifty companies currently serve this market, some of them international players with offices in Europe, where they hold a substantial share of the market in direct marketing by e-mail. These include 24/7 Media, NetCreations Inc., YesMail.com, Exactis.com Inc., MessageMedia, BulletMail and Axciom, together with incentive marketing companies such as MyPoints, Netcentives**,** Beenz, CyberGold, ClickRewards and Freeride. Portals such as www.xoom.com are also entering the market, leveraging their databases of tens of millions of subscribers who regularly receive customised e-mail advertisements for online promotions. Finally, advertising agencies such as DoubleClick and Flycast are now also branching out into e-mail marketing. Many of these companies are listed on Nasdaq and have all the hallmarks of net economy businesses: rapid growth, high market capitalisation, negative income. Most of them have adopted an external growth model, in which expansion is achieved by taking over other firms in the same sector. The other factor common to all these companies is their commitment to the principles of permission-based marketing and opt-in e-mail – albeit with varying degrees of conviction.

These e-mail marketing firms carry on a very wide range of activities: personal data acquisition, administration and operation of cooperative databases, address brokering, e-mail marketing campaign design, push services, CRM (Customer Relationship

Management) (5), monitoring, reporting, collecting campaign fees and paying commission to websites for purchases made by prospects referred by them.

In a permission-based system, data are acquired by placing opt-in forms on a network of 100 or 200 popular sites. Visitors are required to complete these 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. The data entered on the form is passed on to the relevant company (6) and then fed into a database of between 15 and 20 million e-mail addresses. ARETE estimates that on average about a quarter of these addresses belong to Europeans.

Within this model, the practices followed vary in terms of fairness, ranging from the pre-checked box (7) at one extreme to the double opt-in at the other. Double opt-in entails confirming registration by sending an automated message to the visitor's mailbox (8).

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. Some companies receive several opt-out requests a day. They also receive in-

---

5) 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, creating a relationship of trust, developing customer loyalty, 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).

6) There are two main methods for transmitting the data – real-time transfer and periodic batch transfer of data aggregated in the cooperative database. Some e-mail marketing companies also offer a hosting service for their clients' opt-in forms.

7) Some permission marketing programmes do indeed contain pre-checked boxes 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 commercial messages sent to such visitors will be perceived as spam, since they will have no recollection of having requested them.

8) The double opt-in approach is exemplary in terms of the quality of the consent obtained and the transparency of the procedure followed. When a user subscribes to a newsletter from CNET, for example, a pop-up window appears containing a series of boxes to be checked if the user wishes to receive advertising messages in relation to the areas specified; at the bottom of this list is a link to CNET's privacy policy. This policy is very comprehensive and contains a notice to those wishing to subscribe to the newsletter explaining clearly the involvement of a third party, the e-marketing company Netcreations which gathers the data. 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 instantaneous confirmation message by Netcreations, 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. 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 the site on which he or she has registered to receive the newsletter. 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. Finally, when the opt-in confirmation is received by the e-mail marketing company, the subscriber receives an automated welcome e-mail.

quiries 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. In order to be able to respond to these queries, some e-mail marketing companies keep historical records of their relations with subscribers, including information as to when and how the opt-in was exercised.

Addresses are marketed by brokering or by campaign hosting (ESB: E-mail Service Bureau). 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. 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 the personal interests criteria, but ultimately these do not more than reflect the precision of the information gathered from the registration forms. From the standpoint of data protection, some record attributes are undoubtedly sensitive in that they allow identification – without exceeding the scope of permission – 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 business where the purchase was made. For each additional selection criterion and narrowing down of the target audience a higher rate per thousand is charged and the more sophisticated the selection criteria specified the higher the price. The most highly prized – and most expensive – criterion is propensity to shop online.

Finally, the e-mail marketing companies pay commission 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. Some e-mail marketing companies have devised a sophisticated system of 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 is common practice also for partner websites to be given advances on revenue.

I.5) – The rapid growth of permission-based e-mail marketing, which looks set to become the standard for commercial communication on the Internet, raises **issues relating to the quality of consent** and the possibility of consent being misinterpreted or misused.

Firstly, it must be borne in mind that an advertiser could be tempted to use interruption marketing techniques in order to create opt-in relationships and thereby end up spamming a list of undifferentiated and semi-consenting addressees. In other words,

the question has to be asked whether spam is not a necessary precursor of opt-in e-mail marketing. Stated in those terms, the question may appear somewhat provocative, but it needs to be asked 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 addressing the public, seizing its attention, encouraging contact by means of various forms of "appeal" well known by advertisers. 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 broker of address lists 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 not without some reservations – 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.

Another point to be borne in mind is that all the major online businesses and direct marketers are now switching to an opt-in approach, including even the pornographic sites, formerly among the most prolific of spammers. 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? 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 include 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? Is it legitimate to send an occasional online shopper several advertising messages a week? 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 as regards occasional customers.

I.6) – Finally, there is no overstating **the relevance of the recent proposal for a Directive by the European Commission** (12 July 2000) concerning the processing of personal data and the protection of privacy in the electronic communications sector, (9) because of the fact that it re-affirms the central importance of consent in e-mail marketing. We would go so far as to say that this issue is crucial to the very survival of the Internet, with the prospect of operators acquiring – as they have all announced they intend to do – equipment (servers, routers and backbones) capable of **transmitting 100 million commercial e-mails each day**.

This figure can be used as the basis for some projections of volumes and costs. There are currently some 300 million Internet users worldwide (and some 560 million mailboxes). If it is assumed that sooner or later every e-mail marketer will acquire the

9) Proposal for a Directive concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ COM (2000) 385, of 12 July 2000.

technical capacity to transmit 100 million e-mails daily, Internet users could potentially be overwhelmed by the resulting flood of messages – 200 companies 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 will help to ensure the system's survival.

Regarding the financial burden borne by web surfers, it is helpful to make a few 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 world scale, extrapolating into the future and 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.

II) - What protection in Europe ?

For almost four years, the European Union has been debating how best to protect citizens from unsolicited commercial e-mail. The debate has centred around two alternative concepts.

One approach confines itself to laying down the conditions for the sending of unsolicited messages. This is the opt-out approach. Its advocates propose that those who do not wish to receive commercial e-mails which they did not request in advance should be able to register this preference. One faction within the opt-out camp is of the view that this right should be exercisable only against the party who sent the unsolicited message. Another faction favours a system of national or international opt-out lists in which anyone can register, whether or not they have been receiving unsolicited e-mail, with an onus being placed on Europe's direct marketers to consult the opt-out lists regularly in order to comply with the wishes of those expressing that preference.

The other approach links the conditions for sending unsolicited messages with the fairness of the manner in which the e-mail addresses were obtained. This is the opt-in approach. Its supporters propose that it should be possible to send unsolicited commercial e-mail only to those who have given their prior consent to receiving such messages.

II.1) – It is worthwhile outlining the legal framework applicable to unsolicited commercial e-mail in Europe in order to mark out clearly the parameters of this debate.

First, **the general Directive (95/46/EC)** (10) of 24 October 1995 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 6.1.[a]: the data must be collected and processed fairly.*
- *Article 7[a]: processing is legitimate if the data subject has unambiguously given his consent.*
- *Article 7[f]: processing may be carried out if it "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 10: In the case of data collected from the data subject directly, the data subject must be told 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.*
- *Article 11: 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.*

10) 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.

- *Article 14: A data subject may object, free of charge, to the processing for commercial purposes of personal data relating to him or to the disclosure of his personal data to third parties, of which he must be informed in advance.*

The Telecommunications Directive (97/66/EC) (11), for its part, deals with the application of these principles to telecommunications. While it does not explicitly mention e-mail marketing it does however provide (in Article 12) 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".* As far as other direct marketing methods are concerned, the Directive leaves it up to Member States to choose between an opt-in or an opt-out approach.

The Distance Selling Directive (97/7/EC) (12) repeats (in Article 10) the requirement of prior consent in relation to marketing by automated calling systems and by fax. It also expressly includes electronic mail among the means of distance communication which may be used "only where there is no clear objection from the consumer".

Finally, **the Electronic Commerce Directive (2000/31/EC)** (13) lays down two technical requirements for the sending of unsolicited electronic mail.

- *Article 7.1: "Member States which permit unsolicited commercial communication by electronic mail shall ensure "[…] that it "shall be identifiable clearly and unambiguously as such as soon as it is received by the recipient".*
- *Article 7.2: 'Without prejudice to Directive 97/7/EC and Directive 97/66/EC, Member States shall take measures to ensure that service providers undertaking unsolicited commercial communications by electronic mail consult regularly and respect the opt-out registers in which natural persons not wishing to receive such commercial communications can register themselves".*

By referring to the existence of opt-out registers, the Directive promotes a technical facility designed to implement an opt-out approach. In the interviews which were conducted for the purposes of this study it emerged that both the supporters and opponents of an opt-out approach firmly believe that Directive 2000/31/EC favours that solution. The media coverage of the adoption of the Directive largely ignored the clearly stated intention of the Community legislators not to modify the basic rights already enjoyed by Internet-users in Europe. The resulting ambiguity is a source of serious legal uncertainty for those engaged in electronic commerce.

Directive 2000/31/EC appears to drop the link between the lawfulness of the sending of an unsolicited e-mail and the manner in which the e-mail address was originally obtained. Granted, it requires opt-out registers to be created and Article 7 refers to

---

11) 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.

12) 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.

13) Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (OJ L. 178 of 17 July 2000), to be transposed by 17 January 2002.

"other requirements established by Community law", under which personal data must be protected. But this passing reference clearly is insufficient to inform Internet operators of the full extent of the rules with which they must comply.

II.2 – The spam phenomenon has not yet invaded Europe

- **Much debate but little in the way of conflict**

In Europe as in the United States, the spam issue is seen primarily as a legal matter. Since 1997, the European press has been reporting the nature and extent of the spam phenomenon in the US. However, the relevant legislation in Europe was adopted before the rise of spam, which was unpopular in Europe before it ever existed. Even now, European direct marketers are unable to give an answer to the basic question: "how much is an e-mail address worth?", whereas in the United States, lists of e-mail addresses are priced according to highly elaborate systems of cost-pooling and profit-sharing.

The national supervisory authorities have to date had to deal with very few complaints concerning cases of blatant spamming. In one such case, however, the Spanish authority imposed a heavy fine on a company which had sent unsolicited e-mails and was unable to show that it had first obtained the consent of the recipients. The decision is currently under appeal in the courts.

In France, the CNIL (14) published a background report in October 1999 (15) in which it observed that *"the sending of electronic messages […] entails the prior collection of e-mail addresses"*, which *"constitute personal data"* and that *"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"*, and concluded that *"the automated collection for marketing purposes of e-mail addresses from public spaces 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 Article 29 Working Party (16) has adopted a formal opinion (No 1/2000 of February 2000) on unsolicited commercial communications, which was subsequently included in its formal opinion (No 7/2000 of 2 November 2000) on the European Commission Proposal for a Directive amending Directive 97/66/EC (17), and in an exhaustive report on privacy on the Internet adopted on 21 November 2000 (18). The Working Party noted that the Community's data protection legislation extends to the

14) CNIL, Commission Nationale de l'Informatique et des Libertés. See http://www.cnil.fr
15) Available (in French) at http://www.cnil.fr/thematic/index.htm
16) Article 29 of Directive 95/46/EC established a working party composed of representatives of the national data protection authorities. This group acts as an independent advisory body to the European Union on the protection of personal data. Its terms of reference are set out in Article 30 of Directive 95/46/EC and Article 14 of Directive 97/66/EC.
17) Opinion 7/2000 on the European Commission Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector of 12 July 2000.
18) These opinions can be found at http://europa.eu.int/comm/internal_market/fr/media/dataprot/wpdocs

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. In the Working Party's view, the technical requirements 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. The Working Party was of the view that the collection of e-mail addresses from public spaces on the Internet is in flagrant breach of the principles of fair collection (Article 6.1[a] of Directive 95/46/EC), finality (Article 6.1[b]) and legitimate processing (Article 7[f]). Finally, the Working Party supported the Commission's proposal that the senders of commercial e-mails should be required to obtain the prior consent of addressees.

Lastly, the **low volume of litigation** may be explained by the fact that Directives 95/46/EC, 97/66/EC and 97/7/EC have not yet been transposed into national law in all the Member States and the fact that 'spam victims' tend to turn in the first instance to their Internet access providers.

- **Consensus and caution among direct marketers**

There appears to be a broad anti-spam consensus among professional telemarketers. FEDMA (19), like the majority of national and international organisations representing online businesses, believes that "spamming must be combated". The e-commerce federations which were asked dismiss the notion that they could have a spammer among their membership, although none reports having ever expelled any member found "guilty" of spamming. Those in charge of "labels", for their part, would like to see automatic expulsion for spammers so as to uphold the credibility of their labels.

At the same time, **a multitude of opt-out lists** are being set up. These may be specific to particular trade associations or business sectors or may be national or even international in scope. In France, for example, the Fédération des Entreprises de Vente à Distance (Federation of Distance Selling Firms - FEVAD) is the first body to have created an "e-Robinson" opt-out list (20). In Belgium, the Association Belge du Marketing Direct (Belgian Direct Marketing Association - ABMD) has also created an opt-out list by aggregating the opt-out lists of all its members.

Similar opt-out lists are being set up in the UK, Germany, the Netherlands, Spain, Norway, Sweden, Finland and Italy. All represent responses by the trade to the provisions of Directive 2000/31/EC on e-commerce. They are all designed initially to cover only the particular Member State concerned but, in most cases, the trade federations behind them plan to extend them in the near future to the EU as a whole or even to countries outside the EU, in particular the United States. There are also plans for the US-based DMA and various of its European counterparts to work together on a common opt-out register (21). Furthermore, a number of Member States have recently enacted legislation in support of private initiatives to coordinate the different opt-out lists at national level.

19) FEDMA, Fédération européenne du marketing direct. See http://www.fedma.org
20) http://www.e-robinson.com
21) See http://www.e-mps.org on the E-mail Preference Service operated by the DMA.

All of this notwithstanding, **spam is still an ever-present temptation.** The apparently low incidence of spam in Europe may be due in some part to the anti-spam measures that have been put in place by ISPs in Europe and the US. This constant battle imposes an additional burden on the ISPs' financial, human, technical and commercial resources. The cost is proportional to the number of subscribers. Some of these ISPs exchange black-lists of spammers' addresses, the accuracy and lawfulness of which are open to question.

L'EuroISPA (22), which represents the vast majority of Europe's ISPs, has been fighting spam for the past two years and favours 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.

II. 3 – Confused approaches and divergent practices

- **Failure to distinguish between spam and other unsolicited commercial messages**

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, spam is by definition unsolicited advertising but not all unsolicited advertising is spam.

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 Directive 2000/31/EC, which makes no distinction according to whether the addressee of a commercial communication is a customer of the firm in question, a visitor to its website or simply an Internet user with whom the sender has never previously had any direct contact.

But while the vast majority of Europe's direct marketers avoid spamming, they remain non-committal about unsolicited commercial communications in general. 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. Yet the legitimacy of mailing an unsolicited message depends primarily on how the e-mail address was obtained in the first place.

- **Check boxes and pre-checked boxes**

On more and more European websites there is a box which visitors can tick to indicate whether they wish to receive commercial messages via e-mail. Many business associations in Europe recommend this practice, which goes well beyond what is required under Directive 2000/31/EC on e-commerce.

22) See http://www.euroispa.org

On some websites' forms, however, the box is already ticked. This practice is contrary to the requirements of transparency and fairness laid down in Directive 95/46/EC and the best that can be said about it is that it reveals the website owner's unfairness.

- **From the success of the check box to the opt-in approach**

Many Internet businesses are now coming down in favour of the opt-in approach, which they see as the most effective way to do e-commerce. This marked trend is a case of business interests coinciding with data privacy concerns.

Instead of offering visitors the opportunity to end the relationship by opting out, the advertiser invites the e-mail user to be kept informed: this is permission marketing. From a commercial standpoint, a consent-based interactive relationship of this kind has many advantages.

It means consumers are more likely to be offered services they actually want: in indicating their preferences consumers provide highly-prized information which can be packaged and sold and which is authorised for processing. Unlike opt-out registers, which cannot be sold, opt-in registers are a tradable commodity. In this way, the collection and commercial exploitation of data obtained with the consumer's prior consent represents not only a source of profit and a new financing method for electronic commerce but also the most effective means tracking the uses to which the data is put.

In this set-up, the party who collected the information receives a payment whenever a business partner 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. Businesses which thus eschew a marketing practice which is frequently indiscriminate, counter-productive and unpopular stand to win the trust of web surfers. Moreover, if a member of the public asks to be removed from a mailing list or for details of where and when the data was 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 e-mail address was supplied.

This 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). Meanwhile, Finland has adopted a code of conduct for direct marketers based on the opt-in approach.

II.4 – The need for a clarification

Given the apparent contradictions between Community directives, the lack of uniformity in trade practices and the strong trend towards the opt-in model, a clarification of the issue at EU level is now urgently required.

- **To date, five Member States have already adopted an opt-in model** for unsolicited commercial e-mail.

Four of these, Austria, Denmark, Finland and Italy implemented this model in their national legislation transposing Directive 97/66/EC. The fifth, Germany, also has an opt-in requirement, but based on other legal sources.

- **There seems to be confusion in the trade as to what is and is not legal in Europe.**

This confusion does not appear to have been dispelled by the multiple directives applicable to unsolicited commercial communications. It is exacerbated by a mistaken belief in the trade that the provisions of Directive 2000/31/EC are self-contained and all-embracing. However, both the distance selling directive of 20 May 1997 and the electronic commerce directive of 8 June 2000 are concerned only with the lawfulness of the sending of unsolicited commercial e-mail and not with the lawfulness of the manner in which e-mail addresses are obtained, which is a matter exclusively dealt with in Directive 95/46/EC.

Thus, in Europe, the sending of unsolicited commercial e-mail is governed by a combination of four directives which have to address three completely different scenarios, according to whether the recipients are:

- customers or prospective customers who supplied their e-mail addresses to the sender themselves (1);
- persons whose e-mail addresses were obtained by the sender from a third party who in turn obtained them directly from the addressees (2);
- persons whose e-mail addresses were collected in a public space on the Internet (website, directory or mailing list), without their knowledge (3).

1. Unsolicited messages are sent to persons who supplied their e-mail addresses to the sender during direct contact. The general directive (95/46/EC) provides that an advertiser can send commercial e-mails to such persons subject to their right to opt out of receiving them and/or to refuse to allow their e-mail addresses to be disclosed to third parties. Under the distance selling directive (97/7/EC), everything is allowed unless there is a “clear objection” from the consumer after receiving explicit information from the supplier. The telecommunications directive (97/66/EC), leaves it up to Member States to choose between an opt-in approach (adopted by 5 Member States to date) and an opt-out approach. Lastly, Directive 2000/31/EC requires service providers sending unsolicited commercial e-mail to their customers to clearly identify such messages as being of a commercial nature and to consult the opt-out registers on a regular basis. Paradoxically, the electronic commerce directive may have the effect of preventing businesses from engaging in normal correspondence with their customers if the latter register themselves on an opt-out list.

2. The e-mail address was supplied by the addressee to a business which subsequently supplies its e-mail database to a third party for marketing purposes. Under Directive 95/46/EC, the disclosure and use of a mailing list in this way is lawful if the party who compiled the list gave prior notice to the addressees concerned of their right to object to such disclosure free of charge. In the case of data collected online, Article 14 of Directive 95/46/EC specifically requires a check box to be pro-

vided together with a prominent notice on the electronic form advising data subjects of their right to object to the disclosure of their data to third parties for commercial purposes.

3. The e-mail address is obtained from the public spaces of the Internet (newsgroups, e-mail directories, etc.). By its nature, this practice gives no possibility to addressees to object in advance to their data being collected. The practice is outlawed by the 1995 Directive. It falls foul of the principle of finality (Article 6), the principle of legitimate processing (article 7.[f]) (probably), and the provisions of Articles 10, 11 and 14.

- **To eliminate the confusion the focus of debate must shift from the propriety of the message-sending to the propriety of the data-gathering.**

Notwithstanding its reference to "existing Community legislation", Directive 2000/31/EC appears to favour an approach whereby unsolicited commercial e-mail is lawful once it is identified as being of a commercial nature and once the recipient can avoid receiving any further messages by exercising an opt-out after the first one was received.

But by imposing the same obligations on all operators, the electronic commerce directive creates a situation where a business which takes the trouble to elicit its customers' interests and to tell them that it proposes to send commercial messages to their e-mail addresses is nonetheless obliged to consult a general-purpose opt-out list, be it national, European or transnational, which may prevent that business notifying some of its customers of its latest products and services.

Spelling out the circumstances in which data may properly be collected allows the business operator and the e-mail recipient to choose the nature and the future course of their relationship in a climate of transparency. So while none of the directives clearly imposes an opt-in system for direct contacts between businesses and their customers, 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 intrusive nature and the fact that recipients have no means of interrupting them.

It is an empirical fact that the lower the cost of a direct marketing technique the greater the risk of abuse. Direct marketing by e-mail is by far the cheapest form of direct marketing yet invented. Moreover, the protection given to consumers has always been appropriate to the risk of intrusion and breach of privacy, increasing by degrees from the right to refuse future calls (telephone telemarketing) 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 traded for profit, it promotes personalised relationships between businesses and their online customers and it is the system favoured by the web surfers themselves – on the evidence of the United States experience. It also provides a guarantee that data is not used without the subject's consent – by contrast, under an opt-out system, how can an online advertiser be certain that an e-mail addressee 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.

Under the opt-out approach, an online business sending a message to an existing customer would be indistinguishable from a spammer claiming a spurious legitimacy thanks to the opt-out registers. If the opt-out model is implemented, it is quite conceivable that in the long-term considerations of legal certainty would necessitate the adoption of binding legislation at national or Community level aimed at consolidating all opt-out requests in a single international register, the effect of which would be potentially draconian: an opt-out request directed at a handful of advertisers or even a single advertiser would apply to the entire online business community. With that in mind, it is the opt-in approach which appears more conducive to the creation – and termination – of one-to-one relations between online suppliers and web surfers.

The opt-in approach does not prohibit the sending of e-mail advertising to customers or website visitors. On the contrary, it authorises it. All that is required of advertisers is that they inform the recipient clearly of their intentions. The opt-in approach does not prohibit online businesses from passing on contacts' data to third parties, subject to the requirement of prior information and the data subject's right of objection, as laid down in the 1995 Directive. The opt-in approach does not prohibit the compilation of mailing lists. On the contrary, it is a cornerstone of the market for e-mail databases and provides a setting in which these products can be traded profitably. The opt-in approach prohibits the improper collection and use of data. By so doing, it guarantees the effective protection of personal data, provides advertisers with legal certainty, creates a climate of trust and removes the artificial conflict between the protection of personal data and the needs of e-business.

II.5 Conclusions

Since 1995 if not earlier, the European Union has been guided by the principle that the greater the threat to privacy the greater should be the level of protection provided. It is a pity therefore that the technical requirements laid down in the e-commerce directive are not better matched to the characteristics of unsolicited commercial e-mail (deceitfulness, invasion of privacy, costs borne by addressee) and that the wording of the directive lacks the clarity which in previous directives had helped to create a legal framework which was both predictable in its operation and commensurate with the mischiefs it was designed to remedy. In the United States, meanwhile, a number of states have been enacting statutes making spamming a criminal offence and e-mail marketers have been discovering the commercial benefits of permission marketing.

Today, the situation in Europe is a hybrid of the two approaches. Five countries – Germany, Austria, Denmark, Finland and Italy – have chosen an opt-in system. Meanwhile, the online industry is busy setting up opt-out registries in accordance with Directive 2000/31/EC. On the other hand, a number of European online businesses have adopted marketing models based on an opt-in approach. Coming against this background, the proposal for a directive issued by the European Commission on 12

July 2000 (23) is timely indeed. Its objective is to make the Community's data protection framework technology-neutral. The choice of an opt-in approach is the right one, in the light of the findings of this report concerning the situation in Europe and in the US. Moreover, this represents a good opportunity to reconcile national laws – which are already diverging even before the e-commerce directive has been transposed – and to establish a common approach based on the requirement of prior consent.

"Consent" in Directive 95/46 is construed as the absolute exercise by a person of his or her rights. The adepts of permission marketing take the view that once consent has been obtained everything should be possible. This attitude suggests that a two-tier system of data protection may be desirable: one level of protection for the less well off, which would diminish as the subjects granted further consents and waived their rights in response to commercial solicitations, 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, 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 of the information supplied to the data subject. Secondly, consent is always revocable.

The procedures by which consent can be given online must be spelled out. The 1995 Directive provides a strict definition of consent (in Article 2 [h]) as a "freely given specific and informed indication of his wishes by which the data subject signifies his agreement". Therefore, to make certain that the web surfer's consent to receive commercial e-mail has been given, he or she must be obliged to express his or her wishes on the matter. For example, consent could be indicated by ticking a box in a personal registration form. This specific manner of obtaining consent would satisfy the definition given in the 1995 Directive: unless the web surfer takes the active step of checking the consent box, no consent has been given. But great care must also be taken to ensure that the information provided is perfectly clear.

If a procedure of this kind is used for data-gathering, personal data can be recorded together with the conditions which the data subject has attached to their processing. This automatically promotes fairness in the collection of data, one of the core principles of the European legislation. It allows the data to be used immediately for commercial purposes and in the certain knowledge that personal rights have been respected.

The inherent transparency of the prior consent mechanism must henceforth be extended to all media and the message must be brought home to all concerned that the growth prospects of e-commerce will be damaged if prospective web shoppers are left in doubt as to the honesty and fairness of online traders.

23) 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.