JAN KABEL*

Computer und Recht International 2003-1: 1-5

Spam: A Terminal Threat to ISPs?

The legal position of ISPs concerning their Anti-Spam Policies in the EU after the Privacy & Telecom Directive

Internet Service Providers (ISPs) all over the world face being flooded with abundant quantities of the same message to their subscribers, sent by commercial mailers of their network services. This phenomenon is known as spam and it is commonly defined as unsolicited, commercial messages sent by bulk e-mail. It has been predicted that, in the end, spam will kill off e-mail as the near-universal method for communicating with people via the Internet. ISPs suffer greatly from spam: their image as spam-free providers is dented and costly time is spent on taking measures to avoid this phenomenon. Legal responses to this problem are highly divergent. It is questionable whether the new Directive on Privacy and Electronic Communications will strengthen the legal position of ISPs. Spam litigation by providers against spammers with whom plaintiffs had no prior contractual relationship, has led to different outcomes. A recent Dutch case does not seem a cause for much jubilation in this respect.

I. The Privacy & Telecom Directive and Anti-Spam Policies

1. A Restricted Approach

The recent Directive on Privacy and Electronic Communications of July 2002[1] (the Directive) does not contain any specific provision directly protecting the interests of providers who support a spam-free policy. The Directive offers solutions for spamming problems, which are restricted to the relationship between the subscriber and the direct advertiser. Article 13, dealing with so-called unsolicited communications, allows the use of electronic mail for the purpose of direct marketing only in respect of subscribers who have given their prior consent. In this respect, the anti-spam policy of a provider is directly dependent on the attitude of its subscribers to unsolicited mail. The Directive itself therefore seems to offer no legal footing for providers to maintain an independent policy. Nevertheless, at least some attention is devoted to ISPs policy problems: Recital 40 refers to the difficulties posed by the sheer volume of unsolicited mail to electronic communications networks and terminal equipment. However, according to Recital 42, possible problems of cost shifting following from these difficulties are confined to financial costs imposed on subscribers and users rather than on providers.

2. Different Forms of Privacy Protected by the Privacy & Telecom Directive

This restricted approach is understandable from the point of view of the protection of privacy. A personal right, privacy is a right to self-determination and should therefore be enforced by the subject of the right only and not by third parties. More specifically, the right protected by Article 13 of the Directive does not regard privacy in the sense of informational privacy or that of the privacy of communications, but privacy in its relational aspects, in particular the right to determine which communications one wishes to receive or not. The relevant activity is the sending of the e-mail, not the collecting of personal data, or the intrusion on the confidentiality of communications. In this respect, relational privacy could also be seen as a category of freedom of expression that is of the right *not* to receive information. Where the informational aspect of privacy is at stake, other Articles of the Directive apply, such as Article 6 about the storage of traffic data; Article 9 concerning the processing of location data, or Article 12, which states that Member States shall ensure that subscribers are given the opportunity to determine whether their personal data are included in a public directory. These Articles express the right to informational privacy, i.e. the right of an individual to determine for him/herself which information about him or her may be communicated to others. On the other hand, where the right to privacy of communications is at stake,

---

* Professor Jan Kabel, Institute for Information Law, University of Amsterdam. Further information about the author on p. 32.

[1] Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, *OJ* 31 July 2002, L 201/37.

Articles like Article 5 concerning the confidentiality of the communications apply. Article 13 does not protect these rights, but could be considered as protecting the relational aspects of privacy, in conjunction with Article 8, paragraph 2, which gives the called subscriber the possibility of preventing the presentation of the calling line identification of incoming calls. The difference between this paragraph and Article 13 lies in the fact that a third party, the service provider, is obliged to safeguard this aspect of relational privacy. Nevertheless, this obligation is, of course, also based upon the subscriber's wishes.

II. Privacy and the Safeguarding of a Spam-Free Image

1. Tackling the Sources: A Ban on List-Broker's Activities

According to the *Article 29 Data Protection Working Party* , the legal framework of Directive 95/46, the general Directive on the Protection of Personal Data (Data Protection Directive), provides a clear answer to informational privacy issues ensuing from unsolicited electronic mail.[2] The Working Party stresses the rule that in the case of addresses being collected with a view to electronic mailing by a company directly from a person, the collecting company must inform the person of those purposes at the time of collecting the address. More important, collecting addresses in a public space on the Internet, newsgroups included, should be prohibited altogether according to the Working Party's Opinion. This method of gathering information is regarded as

(a) unfair processing,
(b) contrary to the purpose principle in that the data subject made his e-mail address public for quite a different reason, and
(c) given the cost imbalance and the disruption to the recipient, such mailing could not be regarded as satisfying the balance of interests in Article 7(f) of the Data Protection Directive.

This line of reasoning focuses the discussion not on the sending of e-mail, but on the measures to be taken before it's sending, i.e. on the collecting and further processing of e-mail addresses. The ARETE-report, a study commissioned by the EC, concurs with this line of thinking, but without any other practical consequences than the choice for an opt-in approach.[3] Developing this train of thought further, a set of rules emerges, based on the protection of informational privacy, which may or should lead at least to a ban on most of the practices of e-mail list-brokers, including a ban on messages in which millions of e-mail addresses are offered to the public, with these addresses presumably having been collected from public Internet areas unless evidence to the contrary is submitted.
Data Protection Agencies should survey the application of these bans. It is striking that most of them have not yet taken action in this field. This lack of action again probably demonstrates the often-heard reproach that the protection of personal data in the private sector for the most part is left to that same sector.[4] The only exception seems to be the recent decision of the Italian Data Protection Agency , the *Garante per la protezione dei dati personali*. The *Guarante* blocked the processing of personal data by seven companies on the ground of their having collected e-mail addresses of data subjects for commercial purposes without having obtained their prior informed consent.[5] Earlier, in January 2001, the *Garante* ruled out the possibility for a political association to use e-mail addresses gathered from the Web in order to send out political messages and information without the addressees' consent. The *Garante* pointed out that given personal data being available to a number of entities, whether on a temporary basis or not, does not imply that the data is "publicly available" in the sense set out by the Italian Data Protection Act. Indeed, the basic requirement of obtaining the data subject's consent for processing his/her data can be overridden if, *inter alia*, the data are taken from "public registries, lists, instruments, or publicly available documents."[6] The public nature of such documents is related to the existence of a legal provision laying down the general availability of the information included in them. This did not appear to be the case here, nor could any proof be obtained that the data subjects' consent

[2] *Opinion 1/2000 on certain data protection aspects of electronic commerce*, adopted on 3rd February 2000.
[3] Serge Gauthronet and Etienne Drouard, Unsolicited *Commercial Communications and Data protection*, Commission of the European Communities, January 2001, p. 109-110 (ARETE-Report).
[4] See a.o. Thomas Hoeren and Sven Lütkemeijer, 'Unlauterer Wettbewerb durch Datenschutzverstösze', in: Bettina Sokol (Ed.), *Neue Instrumenten im Datenschutz*, Düsseldorf 1999, p. 108.
[5] Decision of 26 July 2002. See the website of the Italian DPA on: http://www.garanteprivacy.it/
[6] Article 12, Paragraph 1 of the Italian Data Protection Act.

had been obtained in order to disclose their data for purposes of a political nature. Thus, the allegations made by the association were neither consistent with the Italian Data Protection Act nor with EC Directive 95/46, in particular, with Article 7 concerning the lawfulness of the processing.
This kind of action applies rather straightforwardly the rules on the fair processing of personal data. Could ISPs themselves successfully make use of such actions, given the inactivity in this field of Data Protection Agencies in many other European countries?

2.Direct Appeal to the Protection of Informational Privacy Principles by Providers

Given the individual-based protection of informational privacy, the question remains how third parties, like providers, might resort to this remedy. Providers have tried this remedy in several instances. In the Dutch *Ab.Fab v. XS4ALL* case[7] the provider, XS4ALL, claimed that Ab.Fab, an electronic direct-marketing company that provided electronic advertising services for third parties, by sending unsolicited e-mails to XS4ALL's subscribers on the basis of an opt-out system, acted unlawfully *vis-à-vis* XS4ALL. XS4ALL based this allegation *inter alia* upon infringement of the protection of subscriber's informational privacy, as laid down in the Dutch Law on the protection of personal data. Some of these subscribers joined as a party to the XS4ALL action. On appeal, the Court considered this infringement only in view of the relationship between the advertiser and the addressees, i.e. the subscribers of the provider. It explicitly refrained from taking into consideration possible separate, informational privacy related interests of the provider regarding the claimed infringement. In the Court's opinion, Ab.Fab had correctly processed the data of its addressees. When personal data have been lawfully processed with regard to the subject of these data, other parties may not use the appeal to informational privacy. This approach is the correct one. Data Protection Agencies excluded, the maintenance of informational privacy protection in principle is a matter for the data subject concerned.

3. Appeal to Relational Privacy and to Privacy of Communications

As far as relational privacy is concerned, Article 13, Paragraph 5 of the Privacy and Electronic Communications Directive restricts the application of the rules on unsolicited communications to natural persons. The same Paragraph obliges the Member States to ensure that the legitimate interests of subscribers other than natural persons with regard to unsolicited communications are sufficiently protected. ISPs are of course not subscribers. The Directive therefore does not legally force ISPs to control the behaviour of direct marketers attempting to send messages through the providers system against its spam policy. It could have done otherwise, as examples of some US State laws show. Under the Louisiana and California Statutes, it is unlawful to use the services of an ISP to send spam in violation of the policies set by the ISP. Washington, Illinois and Delaware support ISPs by not holding them liable for blocking the transmission of messages they (reasonably may) believe are in violation of the relevant State laws.[8] An appeal to privacy of communications is not an appropriate remedy; on the contrary, such an appeal is in the advantage of the defendant because privacy of communications safeguards the confidentiality of the communications and the related traffic data of the sender.

4. Result

The new Directive does not give much support to ISPs in their struggle against spam. For the moment, this support has to be found elsewhere. Case law in various countries allows for some solutions.

III. European and American Case Law on the Safeguarding of a Spam-Free Image by ISPs

1. Simple Solutions: Contractual Obligations and Netiquette

[7] Amsterdam Court of Appeal 18 June 2002 (*AbFab/XS4ALL*), *Computerrecht* 2002-5, p. 299-307 with a comment by J.J.C. Kabel.
[8] See Michael A. Fisher, 'The Right to Spam? Regulating Electronic Junk Mail', *23 Columbia – VLA Journal of Law & Arts 363*, Spring 2000, p. 403-404.

a) Netherlands

The decision in *Netwise Publications v. N.T.S. Computers*,[9] not exactly applicable in the relationship between spammers and providers, nevertheless is interesting because it demonstrates the strength of contractual obligations in this field. Netwise publishes an e-mail directory on its website *www.e-mailgids.com*. It guarantees its subscribers that their addresses will not be used for unsolicited advertising. On its website Netwise has published general conditions, which prohibit harvesting of the addresses and spamming to the holders. Defendant, *N.T.S. Computers*, collects abundant quantities of these addresses in order to sent commercial e-mail, advertising for its computers, printers, and the like. The court considers N.T.S.'s activities as contrary to its contractual obligations and decides that plaintiff has a legitimate interest in a prohibition of these activities, because of its guarantee to its subscribers their addresses not being used for unsolicited, commercial e-mail.

b) France

In *G. v. France Telecom Interactive*,[10] G's claim for the continuation of his access contract with Wanadoo, after this contract had been cancelled by France Telecom because of G's spamming activities to Public Discussion Groups, was dismissed on the ground that Article 1135 of the French Civil Code obliges parties to a contract not only to its express statements but also to what customs as a source of law in this field contain. It was established that spamming to Public Discussion Groups indeed, according to Netiquette rules, should be considered as contrary to a custom in the Internet World. In a similar case between *P.V. and Liberty Surf/Société Free,*[11] the same line was followed. The Court observed that:

> *"(L)a pratique du spamming considerée dans le milieu de l' internet comme une pratique déloyale et gravement perturbatrice, est contraire aux dispositions de la charte de bonne conduite."*

A very simple and effective solution indeed and one may wonder why most of the other cases are so complicated: sometimes this simple contractual remedy is dismissed completely, sometimes ISPs have to find refuge in quite complicated and outdated legal constructions like trespass to chattel or unjust enrichment, sometimes cases could only be won by an appeal to misleading statements of the spammer.

2. Unfair Competition

In its treatment of *Ab.Fab v. XS4ALL* (for the facts of this case see II.2. above), the Amsterdam Court did not consider the collection of the addresses by the marketing company. As we have seen before, a distinction must be made between two different ways of collecting personal data, one directly from the data subject, the other relating to information not obtained from him or her but from other sources, like public places on the Internet. According to the Working Party's Opinion, collecting addresses in a public space on the Internet, newsgroups included, should be prohibited altogether, and the authors of the ARETE-report adhere to this view. If this opinion is correct, the Court should have investigated the collecting methods used by the company. Furthermore, it should have examined the company's performance of its information duties in more detail. Did the company notify the individual holders of e-mail addresses at the time of the collection of these data of its identity, of the purposes of processing, of the possible recipients of the data, of the existence of a right of access and a right to rectify the data? It seems improbable. This is not common practice, however contrary to the rules. It does not mean that these companies could be accused of having acted contrary to the principles of data protection if one also includes in these principles the reasonable expectations people may have of the protection of their privacy. Reports show these expectations to be minimal when commercial companies are concerned. Nevertheless, the infringement of the rules stands as it is.

These rules protect the data subject and it seems difficult to construct a case in which an ISP could base its actions on an infringement of the informational privacy of its subscribers. However, one possibility must not be overlooked. Given the infringement, one may ask whether competing advertising companies or other companies like ISPs could claim damages from the company that unfairly processes personal

[9] Court Rotterdam 5 December 2002, case nr. 185313/KG ZA 02-1068, not yet published.
[10] Tribunal de Grande Instance Rochefort sur Mer, 28 February 2001. This decision is available on: www.foruminternet.org
[11] Tribunal de Grande Instance Paris, 15 January 2002. This decision is available on: www.foruminternet.org

data, according to the theory holding that unfair competition could take place by infringement of public rules thereby gaining an unfair advantage over law-abiding competitors. This theory is followed in the jurisprudence of most civil law countries of the EU. In an interesting Dutch case, XS4ALL itself took the lead by publishing an advertising campaign against free providers; in this campaign, XS4ALL quoted from the subscriber-conditions of these providers (a.o. Wanadoo and Nok Nok). The quoted conditions allowed the free providers to market the personal data of theirs subscribers, whereas XS4ALL did not market these data and did not offer free subscriptions either. The allegation by some of XS4ALL's competitors of unfair competition (disparagement) by XS4ALL was dismissed.[12] The Court did not enquire in detail into the quoted conditions. If the practice based upon these conditions would be against the rules for the protection of personal data, an action by XS4ALL against its competing providers and based on the theory mentioned above, is not altogether unthinkable.

The problem to be solved seems more complicated because it relates to companies that usually are not competing with each other: ISPs on the one hand and advertising service companies on the other. Competing issues nevertheless could arise if an ISP performs activities in the advertising market, for example by offering 'pop-up' facilities for its own services or for those of others. Depending on the relevant national legal system, actions based on unfair competition clauses could also be brought against companies by interest groups, as is the case in Germany (Article 13 UWG) or in the Netherlands (Article 3:305a en 305b Civil Code). In these cases, there is no need for a direct competitive relationship between plaintiff and defendant.

The protection of personal data in the private sector for the most part is left to that same sector. Given the weak upholding by DPA's of the actual defence of data subject's rights in this sector, one may indeed look for legal actions in the field of unfair competition. These actions could be founded on the unfairness of breaching rules that hold for all competitors alike, thereby gaining an unfair advantage in the market. As far as the processing of data is concerned, German case law on unfair competition (Article 1 UWG) contains in this respect the following conditions for a successful action:
(a) the disputed activity must be contrary to the rules on the protection of personal data;
(b) it must have an external effect;
(c) it must serve competition goals; and
(d) it must lead to an advantage in competition.[13]

These conditions could be fulfilled in cases where personal data are collected in public areas, offered for sale on the market, serve direct marketing goals and where the data-collecting company unduly obtains an advantage over its law-abiding competitors. Examples of cases are not overabundant, but some could serve as an example for the setting up of an action by ISPs.

3. Complicated Solutions: Classical Remedies

Given the lack of specific law, ISPs have to resort to more complicated, yet interesting classical remedies, like - in the Anglo-American countries - the action of trespass to chattel, or property claims and unjust enrichment claims in the continental law systems.

a) Unjust Enrichment
Actions based upon unjust enrichment may not necessarily lead to a ban on spam activities, but could however result in a shift of costs which in turn could have a prohibitive effect on these activities. These actions could be granted when the defendant has saved costs or has increased his income by making use of other people's property without their consent.[14] The conditions mentioned are, for instance, applicable to fax advertising and could clarify why the much-used cost-shifting argument in these cases indeed denotes unlawful behaviour. In the case of fax advertising, the recipient is confronted, after all, with the costs of paper and toner; unsolicited junk fax shifts advertising costs from sender to recipient. Bulk advertising by e-mail does also shift costs, but the harms presented by the use of junk fax are not present in the same way in the relationship between the junk-mailer and the recipient. If the recipient has

[12] District Court Amsterdam, 2 December 1999, *IER* 2000-2: 87-95 with a comment by J.J.C. Kabel (Euronet v. XS4ALL), confirmed by Court of Appeal Amsterdam 22 June 2000, *IER* 2000-5: 265-268.
[13] Thomas Hoeren and Sven Lütkemeijer, 'Unlauterer Wettbewerb durch Datenschutzverstösze', in: Bettina Sokol (Ed.), *Neue Instrumenten im Datenschutz*, Düsseldorf 1999, p. 119-120.
[14] See for Dutch law: E.J.H. Schrage, *Verbintenissen uit andere bron dan onrechtmatige daad of overeenkomst* (Monografieën Nieuw BW), Deventer: Kluwer 1998, p. 60-61.

access to the Internet on a flat-rate basis, he or she incurs no costs for the time it takes to delete the spam messages. If, on the other hand, the recipient's access is based upon pay-by-the-minute, he or she pays for the time it takes to download the unsolicited mail. There may be some cost shifting, but not enough on which to base actions, however. Moreover, the condition that use has been made of another's property seems difficult to fulfil. Finally, the recipient must have made clear beforehand that he or she has not given his or her consent. The individual's interest in these cases will, generally speaking, not be sufficient to start a legal action. The obvious action of a group of recipients has been rejected in the Unites States, with the judge not being able to ascertain that everyone in the group satisfies the condition of not having given his or her consent.[15] In the same way, the judge in first instance in the Dutch *XS4ALL v. Ab.Fab* case decided that the individual recipients could not claim an interest in the ban requested, because they had not protested beforehand against the unsolicited e-mail.

b) Tresspass to Chattel

The fulfilment of the condition that use has been made of a plaintiff's property seems easier to prove when the plaintiff is an ISP. In *CompuServe v. Cyber Promotions*,[16] it was accepted that the junk-mailer intentionally 'intermeddled' with another's property; the Court held that electronic signals generated and sent by computer are sufficiently physically tangible to constitute intermeddling and thereby the Court found that occupying the disc space and draining the processing power of the plaintiff's computer equipment, together with the resulting loss of goodwill, was sufficiently injurious to maintain an action for trespass to chattel. *Fisher* remarks that the Court's concern about the inherent cost shifting quality of spam has been an important factor in the Court's recognition that the public interest is advanced by allowing ISPs to block unsolicited electronic advertisements. It must be noted that the Court did not consider subscribers' prior protests against unsolicited e-mail as a necessary condition for a comprehensive ban. Therefore, ISPs claims could be granted independently from subscribers' attitudes to unsolicited messages. The case, however, is not altogether a clear-cut one, the property claim being diluted - so as to speak - by the fact that the junk-mailer, *Cyber Promotions*, had falsified the sender data in order to circumvent *CompuServe's* efforts to screen and reject the spam.

c) Property Claim

The Dutch Court in the aforementioned case *Ab.Fab v. XS4ALL* had to deal with a more 'decent' junk mailer and therefore with a more clear-cut case. Ab.Fab, according to the Court, respected the opt-out rules concerning unsolicited e-mail; its messages were recognisable as advertising and its data traffic of a modest quantity (20 to 25 KB messages to individual subscribers). The Court did not pay attention to the method of collecting the e-mail addresses. In these circumstances, the Court's considerations about the property claim of XS4ALL tended towards a more subtle approach. Firstly, it stressed the public character of the service of the provider and concluded that, thanks to that specific character, the use by Ab.Fab of the provider's property could not be considered as such to present a trespass to XS4ALL's property of its computer equipment. On the contrary, according to the Court, the public character of XS4ALL's services restricted the exercise of its property right. Lacking a legal public obligation, XS4ALL, in the opinion of the Court, did not have an obligation towards third parties to deliver their e-mail messages to its subscribers. Given the lack of such an obligation, it could nevertheless not follow that XS4ALL should be competent to prohibit third parties to offer specific kinds of messages. The Court considered that other circumstances would lead to an alternative conclusion and these include:

a) sending e-mails in bulk quantities, causing thereby a disproportionate burden to the system of the provider,
b) more than minimal costs.

The Court saw no reason to assign a tort action against Ab.Fab. as these two conditions were not fulfilled. XS4ALL's reputation could not be harmed, with spam frequently occurring all over the world, as the average user of e-mail should well know.

d) A Right to Block Spam

[15] *Kenro, Inc. v. Fax Daily, Inc*., 962 F. Supp. 1162, 1168.

[16] *CompuServe v. Cyber Promotions,* 962 F. Supp. 1015, S.D. Ohio 1997. See for the sources on American case law: Michael A. Fisher, 'The Right to Spam? Regulating Electronic Junk Mail', *Columbia VLA Journal of Law & the Arts*, Vol. 23, Nos. 3 & 4, Spring 2000, p. 363- 419; David E. Sorkin, 'Technical and Legal Approaches to Unsolicited Electronic Mail', *35 U.S.F.L. Rev*., p. 325-380; Michael W. Carroll, 'Garbage in: Ermerging Media and Regulation of Unsolicited Commercial Communications', *Berkeley Technology Law Journal*, Vol. 11: 2, p. 233-280.

Regarding these decisions, only specific circumstances seem to offer a provider the right to block spam from a spammer who is not a subscriber: disproportionate burden, more than minimal costs, misleading changes of sender data in order to circumvent providers efforts to reject spam. Decent spammers could not be blocked at all. On the contrary, they could appeal to fundamental legal defences like freedom of speech or antitrust. Defences based on freedom of speech were put forward by the plaintiff in the *Ab.Fab v. XS4ALL* case, but without result. Nevertheless, defences based on freedom of speech, used by non-commercial spammers, could probably not be without success. In the case of *Staat v. Rath* [17] the judge gave himself a lot of trouble in order to decide that the sending of bulk e-mail to members of the Dutch Parliament with the purpose of influencing these members to oppose to a certain bill affecting the trade in vitamin preparations, should be considered as commercial e-mail on account of the sender's own trade in these preparations. The Court could thereby circumvents the possible problems related to freedom of speech and unsolicited e-mail. Antitrust claims have been raised also, however without success.[18]

IV. Conclusions

According to Article 13 of the Directive on Privacy and Electronic Communications, electronic mail for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent. One may note that a user of an electronic communication service not necessarily has subscribed to this service. Therefore, the protection against unsolicited e-mail is restricted to subscribers only; that leaves users in the working place for instance for their protection dependant on their employer-subscriber who shall be in most cases on his turn be dependant of his provider. This once more calls for a strengthening of an ISP's legal position. Data protection law seems very appropriate to tackle at least the fundamental problem of harvesting and selling e-mail addresses; a strict application of the data collection principles takes the spamming tools away from the spammer. Nevertheless, the spamming itself is difficult to suppress. The Directive offers no straightforward legal actions to ISPs. However, once the Directive will be implemented (October 2003), providers could have a case when, acting as an interest group, they found their civil actions against direct advertisers on the then legal proposition that the communication as such is illegal. This proposition would allow for better possibilities with regard to claims concerning trespass of chattel, unjust enrichment and the like, the proposition being a fundamental circumstance to make the unsolicited sending of e-mails illegal against the provider. Contract law cannot be enforced against third parties, i.e. non-subscribers. Publication of ISPs anti-spam policies, however, sometimes could be considered as binding agreements with respect to third parties. On the whole, Data Protection Agencies should be more active in the field and ISPs should unite and, acting as an interest group, look forward to see spammers in court.

[17] Court Almelo 13 September 2002*, Mediaforum* 2002-11/12, p. 360-362 with a comment by Catrien Noorda.
[18] Fisher, p. 392-394.