Abusive Advertising on the Internet through Spam: Problems and Solutions*

Phaedon John Kozyris

1. Introduction: Technology and the Advent of the Internet: Blessings but Also the Curse of SPAM

The possibilities of telecommunication, including person-to-person contacts, and the gathering of information, have exploded exponentially through the Internet and this is continuing at an astronomical pace at a point of no return. As a result, and due to the simple but crucial fact that most of this can be conducted at minimum cost, the life and work of billions of people have been substantially affected for better or worse.

On the negative side:

First, electronic messaging has greatly simplified and amplified the opportunities of wrongdoers to cause harm through fraud, organized crime, pornography and undue influence.

Second, the virtually cost-free access to e-mail has enabled the marketers to flood the channels of the Internet at an accelerating pace with “SPAM”, i.e. unsolicited commercial e-mail messages sent automatically and in bulk to vast numbers of Internet users. It is estimated that, at present, close to an incredible 80% of all e-mail worldwide constitutes SPAM and the percentage is growing. Mobile phones are now becoming increasingly vulnerable to it and there is no end in sight.

Even innocent-content SPAM causes significant harm by inundating the channels of the Internet with unwanted garbage to the detriment of ordinary users but also of legitimate

* Session IIIB2. National reports received from: Denmark, K. Frost & H. Udsen; Germany, Th. Hoeren; Greece, R. Giovannopoulos; Italy, F. Giardini; Poland, B. Gadek; South Africa, J. Hofman; Spain, S. de Salas; Switzerland, B. Cottier; UK, L. Edwards; US, P. B. Maggs.
commerce. Particularly virulent is the “disguised” innocent-content SPAM, intended to avoid detection, either through misleading indicia of source or content or, even worse, through hosting of other people’s computers (zombies).

We are faced here with activity that causes relatively minor nuisance-type harm or distraction each time to each target but which cumulatively, involving hundreds if not thousands of messages to billions of persons within a relatively short time frame, approaches the level of an Internet catastrophe, a menace that requires serious attention. We are faced with a classical “Tragedy of the Commons” conundrum. There is little question that spammers at the very least (a) trespass upon the commercial property of the servers, whose access contracts typically forbid it (although servers may also profit from it through their use charges), and also upon the communication facilities of the users (b) invade the privacy of the users, mostly at home, and cost them time and money for the extra periods spent on-line and (c) even distort trade. Thus even innocent-content spamming violates both property and privacy-personality rights, including possibly unfair competition, and can be treated as a tort with possible criminal law consequences. In addition, administrative law strategies may be used. Private “netiquette” persuasion is not enough.

While we must respect freedom of expression and communication, which extends to SPAM, however despicable, its commercial nature as well as the thoughtless and indiscriminate actions of the sender minimize its social utility, and our care to make it possible and easy for the user to consent to receive it take care of his legitimate interests. We should also remember that freedom of expression stops at the door of privacy, of the freedom not to receive expression and to preserve one’s peace and personality.

Our study will focus on innocent-content SPAM narrowly defined: unsolicited, commercial, bulk, automated. SPAM as part of some other illegality is to be confronted together with such activity, although inevitably our proposed anti-SPAM package will help there as well by reducing its rate. Concentrating on commercial versus e.g. political SPAM will make our proposals more compatible with the constitutionally protected freedom of expression whereas requiring bulk and automation will thankfully leave out ordinary casual communications among users even including merchants in concrete situations. As regards the requirement of “solicitation”, we will not cover SPAM which is offered to us only after we took some inviting action, e.g. pop ups, banners or adware in web pages that we visit, although the general rules for proper methods of identifying and presenting advertising, which apply e.g. to television, should extend also to those situations, and the visit to a web page certainly should not be treated as implied consent to receive SPAM in other ways.
2. Combating SPAM

There is universal agreement that measures should be taken to limit or even eradicate innocent-content SPAM as harmful activity. Further, the lesser the availability of SPAM, the lesser the opportunity for spammers to engage in fraudulent or criminal behavior. Given the free-global-range nature of the Internet and the ability of persons to enter and use it from anywhere in the world, international cooperation is vitally needed, as recognized e.g. at the Geneva Declaration of Principles (37) and Plan of Action (12d) of 2003 of the ITU World Summit of the Information Society and reaffirmed in the Tunis Commitment of 2005. See also the Joint Statement adopted at the London Conference of February 21-23, 2005 of the ASEM, representing many European and Asian states. The OECD also set up a Task Force and has been moving forward on this front. Closer to us, 13 European Union members, including incidentally five of those covered in our national reports, agreed to cooperate and handle through a common procedure, mostly through their Data-Protection Agencies, SPAM complaints across national borders. The obstacles and difficulties of fighting SPAM effectively, however, are major, not so much on the legal as on the practical side.

Our legal analysis that follows will start with the most strict measures and end at the margin. We will then address more specifically the elusiveness of those engaged in or used for spamming and will explore strengthening enforcement by conscripting on-line service providers (ISPs, access, and ASPs, application (e-mail) providers, usually the same enterprise, sometimes called collectively “intermediaries”) as well as advertisers and their clients.

3. The Legal Front

3.1. Ban SPAM!

The European Union, especially in Article 13.1 of Directive 2002/58/EC, has come close to requiring specifically that the mere sending of SPAM for “direct marketing” to natural persons should not be allowed without the subscriber’s “prior consent”. Art. 2f and Recital 17 of Directive 58 cross-refer to Directive 1995/46/EC for the definition of consent (which requires in Art. 2h that it be “free, express and informed”), and Recital 17 further indicates that any “appropriate method” is acceptable provided that the consent is “freely given, specific and informed.” Ticking a box in a website is possible. Since the ramifications of consent have been explored in more detail in the context of the protection of personal data, we will review them there.

Civil and penal sanctions for violations are to be imposed although this is left to the member states. See Recital 47 and Art. 15.2, also cross-refering to Chapter III of Directive 1995/46/EC. However, there are no express requirements with respect to the potential liability
of the on-line providers for SPAM sent over their facilities. Indeed, it would appear that silence means that the exculpatory provisions of Articles 12-15 of Directive 2000/31/EC, the background text for electronic commerce, would apply also here, which basically negate the obligation of those who are conduits and transporters of messages to monitor their content and eliminate their responsibility for the violations of those who use the facilities unless they know or participate in them. In addition, there is no indication that the advertisers-clients of spammers are to held accountable. Finally, it appears that these providers are not themselves enabled to pursue remedies for violations. Directives 2000/19-22+77/EC, which address the details of the business operations of on-line service providers, do not concern their potential liability for carrying and delivering SPAM. The European Commission continues to be seriously concerned about the problem of SPAM and in Proposals and Communications, as set out in the Appendix below, appears intent to expand coverage and strengthen enforcement. Working Groups have been keeping the fight current and active. The Commission also recently created the European Network and Information Society Agency to keep the issues on the agenda (COM (2006)251). However, we are still faced with gaps and with serious problems of implementation.

The 2002/58/EC Directive, and the implementing measures, do recognize also the prior-business-relationship exception (Art. 13.2). Further, legal persons are relegated to lesser protections, to be decided by the states, e.g. possibly an opt-out system (Art. 13.5).

3.2. CAN SPAM!

In the United States of America, the CAN SPAM ACT, effective beginning in 2004, strikes at SPAM but, for the time being pending review, only in a limited way. Its basic approach is one-to-one opt-out, enabling the receiver of SPAM only to reject future such messages from the same source. This is quite meager considering also that the Act contains no remedies for the target but only for the ISPs and the authorities. The Act reflects the theory that an opting-out approach, if made simple and easy and if the burden of implementing it is insignificant, is more consistent with the freedom of the Internet and less bureaucratic. A further dilution of the protection appears because no overall and generic opt-out, e.g. through a National Registry, is available as yet and the user must object e.g. on a one-to-one basis to those who propose to spam. Some justify this as safeguarding information likely to be abused by illegal spammers and the creation of such a Registry has already been studied and treated with skepticism by the FCC and is not likely to be implemented.
Important features of the Act are that it requires the true identification of the source and punishes misleading headers as well as the capturing of the facilities of other users to send SPAM. Particularly as to headers, a requirement of identification as advertising, e.g. ADV, is under consideration.

3.3. Protection of Personal Data

As of now, the main legal instrument of protection against SPAM in the countries of the National Reports has been the recent legislation prohibiting, with minor exceptions, the collection and processing of Personal Data as part of the Privacy-Personality rights of the user. Within the European Union, such legislation is patterned upon the detailed provisions of Directive 1995/46/EC as supplemented by Directive 1997/66/EC now replaced by Directive 2002/58/EC.

According to the prevailing view, the electronic addresses of users are treated as protected Personal Data. Spammers need such data and they “harvest” them in various ways, electronically (Spambots or Spiders) or through other means and their activities would be seriously impeded if they were denied use of this information.

Personal Data protection laws (as well as the Directives discussed above) quite appropriately draw a watershed line between those (few!) users who want-do not mind-tolerate all messages and the rest of us and seek to utilize the key notion of “consent” to separate the two groups. Generally, the definition of “consent” here is strict: it must be “prior”, “informed”, “explicit”, “specific” and “written” either to a specific type or to a particular source of message. In these circumstances, SPAM should be considered legitimate. We should note that not only the consent itself but also the solicitation to consent to SPAM is sufficiently connected to it that it should meet these requirements. Thus, there is no “first bite” exception.

Further, a second and important exception allows the use of the electronic address where there has been a prior, especially commercial, relationship between sender-user which would justify at least the initiation of another contact. This exception, with its many details and ramifications, will not be explored further here since it is not applicable to most instances of SPAM and the related contact is not likely to be burdensome.

From the narrow scope of the “express consent” – “prior relationship” exceptions, it follows that silence means no authorization for others to collect and utilize one’s own personal data or generally to use them to spam and that an “opt-in” type regime is the most compatible.

The personal-data-confidentiality approach is partial but strong as against SPAM and an added feature is a panoply of remedies, including penalties and administrative measures as well as actions by the subscribers harmed. What also helps is the establishment of an
independent administrative agency to oversee, supervise and enforce. Further, ISPs and ASPs 
are not allowed to reveal or misuse or take advantage of personal data that come into their 
possession but, on the other hand, they are not generally required to monitor and police what 
is transported by them on behalf of their clients as explained above.

3.4. Preventing Unfair Competition

The technique of spamming has also been considered as a too aggressive and unfair method 
of trading both against competitors and against customers. Where such characterization 
sticks to particular SPAM, there are reasonable enforcement possibilities both privately and 
by the authorities but principally against the advertisers and their clients. The availability of 
collective civil suits by consumer organizations may also help.

4. Reality Check

The Internet is basically a free world of its own beyond the effective authority of any nation 
or organization where persons of any nationality or location can offer access and application 
services, including e-mail, and where anyone anywhere can enter and communicate 
anonymously or pseudonymously at will. Identity, source and location not only can be 
changed but also can be disguised or dissimulated through easily available and cheap 
software.

Spammers obviously take advantage of this environment, shopping for localities and ways 
that will enable them to send their garbage with minimal detection. Indeed, it is estimated that 
the majority of the SPAM that purports to come to US recipients from abroad originates in the 
US itself.

The complexities of jurisdiction and choice of law relating to any controls imposed in this 
global context are difficult in themselves, but this is not the main problem. Indeed, the harm 
done by SPAM both through the harvesting of addresses and the sending of messages occurs 
clearly where communication is received and this generally would suffice for purposes both of 
jurisdiction and choice of law. It should be enough that the message has been posted in ways 
that could and did reach the recipients in other localities. Further, this should extend not only 
to the spammer but also to those who transfer the message or advertise through it. In addition, 
penal or administrative provisions of course are of a public nature and apply immediately 
and totally to activities that are conducted or have effect within the jurisdiction, clearly 
SPAM. It is not possible for a spammer to hide successfully behind a potentially permissive 
law of the state of origination or of his own establishment. Within the European Union, the 
scope of anti-spamming regulation extends broadly to messages received at or sent through 
a public network within the Union (see Recital 31 of COM/2004/28 final) and this field has
been exempted from the home-rule principle (see Annex to Directive 31). The most vexing problem is that of enforcement, of identifying and localizing the spammers and bringing them to justice. The difficulties of coordinating action internationally add to the problem.

5. Avenues of Enforcement

Our earlier review of the legal front focused mainly on rules that are aimed at the spammers and at others who reveal personal data to them and the reality check made us aware of the difficulties of enforcement. We will now explore some additional measures that may also prove helpful.

5.1. Defensive Technology and Conscripting the Intermediaries

There is no question that the fight against SPAM necessarily starts with and relies heavily on counter-technology, i.e. combating it with practical countermeasures. However, the more we sharpen our anti-spamming tools, the more the spammers as prestidigitators constantly seek, and often succeed, to develop new ways to by-pass any technological controls aimed at their practices. With rapidly changing technology, we run the risk of coming second, with any solutions proposed becoming obsolete the next day.

In this situation, it appears reasonable to aim our legal devices mostly at the more visible and accessible enterprises which run and serve the Internet on line, especially the ISPs and ASPs who offer access respectively to the Internet and to e-mail. Assuming we agree that the mere providing of lines for the transportation of messages over the Internet (common carriers) should not be burdened with the responsibility of content control, and not be liable except when they act "knowingly" (see the discussion of Articles 12-15 of Regulation 1995/46/EC above), how far can we realistically conscript the ISPs and ASPs to combat SPAM? Their self-interest to eliminate the overloading of their business assets with garbage, even though they make some profit from it by charges on the use of the lines, basically coincides with the privacy interests of the subscribers, and their willingness to cooperate with public authority in this field should be assumed.

To begin with, the ISPs and ASPs are business enterprises subject to the authority of the countries where they operate and typically they are required to be licensed there. It follows that they are amenable to substantial regulation as has been done, for example, in the field of personal data protection for confidentiality as discussed above. However, two factors limit how far they can be conscripted in the anti-SPAM fight. First, it is generally agreed that control measures should not impose excessive burdens on the operation of a free Internet. Second, the nature of the Internet makes it possible for some such enterprises offering such services to operate from "offshore" locations or through divertive techniques that make them
virtually unreachable by any arm of the law. The existence of such renegade mobile operators will complicate the enforcement of any system of obligations against spammers. Still, a lot can be accomplished through cooperative intermediaries, and the antitrust rules should be moderated here to permit joint action.

Next, the rules that require these enterprises to respect and safeguard the confidentiality of the personal data of their subscribers do not limit the monitoring of such data for purposes of preventing violations of the law, including the anti-SPAM regime. Indeed, not only are they allowed but they are required to protect the safety of their networks (see e.g. Art. 4 of Directive 58) and also they must take action against and report on illegal use, including SPAM (see e.g. Art. 7 of Directive 46 and Arts. 14-15 of Directive 31). We must also remember that both the opt-in and the opt-out systems for subscribers and, even more so, the enforcement of the true-identification and true-return-address obligations of senders necessitate some screening of messages to insure compliance. This should include both traffic and location data.

A questionnaire addressed by the European Commission to the intermediaries (D(2004) 538341) in the context of Communication (COM (2004) 28), relating to the enforcement Directive 58, expects self-regulatory and technical actions by the industry to combat SPAM including (a) contract clauses with subscribers (b) filtering (c) preventing third-party mail-hosting, limiting the amount of outgoing mail per user, authenticating sender mail, payment of mail services (d) blocking SPAM from other service providers (rate limiting – maximum number per destination server within a timeframe –, reputation system – for source –, checksum – detecting bulk incoming e-mail etc.) (e) collecting personal data for “double’ or “confirmed” opt-in systems (f) labeling for opt-in compliant e-mails, etc. etc. In conclusion, intermediaries occupy the first line of defense: they are empowered and are required to use techniques to combat SPAM which involve monitoring of what comes to their systems. However, we must recognize that they should be also required both to inform their subscribers of their practices and to give them an opportunity to reject all interference with incoming messages.

5.1.1. The anti-SPAM Arsenal of the Reachable and Cooperative Intermediary

5.1.1.1 Bulk-SPAM-permit?

It appears that a technically practical way to frustrate a lot of spamming is for the particular provider to intervene at the point of dispatch and require that any sender through his system of more than e.g. 1,000 messages at a clip must obtain his prior electronic permission, which will be denied to spammers (who should be obvious). Cf. the Commission’s reference to rate limiting and checksum, above. This technique will also enable the intermediary to limit the
controls to only commercial messages. Software to identify high-volume senders is available, e.g. Senderbase of Spamcop by Iron Port. Spammers may seek to avoid this control by changing slightly the content of their messages but still this should operate as a significant obstacle to spamming.

5.1.1.2. SPAM-filters?

Intermediaries can and do provide filtering to their clients which catches a significant amount of spamming. This includes the use of “black” or “white” lists identifying respectively unreliable and acceptable sources. Cf. the Commission’s reference to a “reputation system”, above. A special white list may include only those senders who are bonded with the intermediary. Users may also so protect themselves. While filtering is improving by the day so, unfortunately, are also the techniques to by-pass it. This appears not to be a sufficient solution since a significant amount of SPAM still escapes and there are also false positives. In any event, as a matter of general principle, there is no good reason why the cost of protection should be borne, directly or indirectly, by the subscriber. It goes without saying that any subscriber who wants absolute freedom to receive any and all messages unreviewed or unfiltered should have it.

5.1.1.3. Traceable sender ID

Traditionally, to obtain a telephone number-name you had to provide full and reliable identification so someone bore responsibility for the use of this service. ISPs and ASPs do require some ID information and there is no good reason, other than some processing burden, why e-mail addresses should be created and access be made available for the benefit of shadow users. The location and ID of the equipment may also be useful to know. Privacy and anonymity are sufficiently protected by prohibiting making ID information available to others or screening the messages themselves. It is here that the law may come in to require adequate identification that will make the tracing of illegal messages, including SPAM, possible.

Most SPAM is “spoofed” as to source, i.e. the return address is phony. Spammers want to be non-traceable. Intermediaries are capable of identifying and forwarding only the messages that originate with and include a real address in the Caller-ID fashion, as already proposed by Bill Gates and in the process of implementation by Microsoft with “hotmail”. Cf. the Commission’s “authentication of sender”, above. The potential to identify and locate the elusive spammer will both deter his activities and help enforcement.
5.1.1.4 SPAM-free e-mail area

It has been reported that it is possible, through the use of a new top-level domain name of “.mail”, and with the cooperation of legitimate intermediaries, to create an additional and separate e-mail area from where unidentified and unauthorized senders will be excluded. This is known as the Spamhaus Project against the “net” or “com” names. From the perspective of freedom, this may be the best of all possible worlds in the sense that spammers may inundate one channel but subscribers will be able to limit their e-mail operations to the other channel.

5.1.1.5 Spam-stamp?

The only reason that SPAM exists is the possibility for a sender of e-mail to inundate the Internet with an enormous number, millions, of identical messages at virtually no cost. In these circumstances, even an infinitesimal commercial acceptance rate makes a profit. SPAM can be eradicated by imposing an infinitesimal cost (e.g. $0.001 on every message sent in bulk, e.g. at more than one thousand units at a time, cf. the concept articulated by Bill Gates of Microsoft). Apparently this approach is not presently considered realistic in that it will need changes in Internet telecommunication by requiring bulk senders to provide true identification and establish credit lines for their access. In addition, some agency (or ISP?) should do the collection at some location and decisions are needed on where and how to use the proceeds. The technocrats should have the final word whether we, the lawyers, can develop a practical way to enforce such a regime without handicapping the Internet. A similar and simpler idea would be to require each sender to answer an instantaneous question before being allowed to send any message. But this may be considered as overbroad and over-burdensome on all, throwing out the baby with the bathwater.

5.1.1.6 No-SPAM contract clauses

Most reputable intermediaries provide their services only to persons who agree in their connection contracts not to spam. Enforcing such clauses has been promising and can be expanded. It should also be remembered that it is here that subscribers should be informed of the safety risks of e-mail and should be requested to approve monitoring techniques to detect and eliminate SPAM.

5.1.2 The Errant and Wandering Intermediary

It is now possible for an e-mail user without identification to get access to and deliver messages on the Internet through intermediaries and servers who are or appear to be located at unknown places and beyond the reach of any regulation. Once these messages are placed on
the Internet flow, sometimes by bouncing off additional servers, they are processed together with the others and reach their destination. This method may by-pass any and all controls over SPAM, however severe, while at the same time abusing the facilities of legitimate intermediaries down the line. It appears that the major ISPs and ASPs worldwide are now banding together to develop technology which will intercept or block these messages and this should be encouraged or even required by law. Further, it may become possible to stop this practice at its inception by identifying suspect servers or locations and excluding them altogether from the flow.

5.2. Striking at the SPAM Profit

A promising target of regulation, as yet unexplored, are the advertisers themselves, and even more so their client enterprises, who together not only know what is going on but have planned and invited it and are profiting from it. The typical innocent SPAM solicits the sale of a product or service and makes a profit. Assuming the proposed transaction is not fraudulent and phony, and the seller gets paid, he should be easy to locate and identify since the transaction almost always involves charging a credit card or depositing funds in a bank account and the banking enterprises do and could be legally required to make this information available to the public authorities and even to the buyer. The advertiser can then be traced also through the seller. The origination of the product or service may also help. Of course, using credit facilities in, and shipping from, obscure locations of convenience may frustrate this tracing, but this is not the common practice.

6. Conclusion

In many ways, the infection of our lives with “unsolicited, automatic, bulk, electronic, commercials”, even if innocent “SPAM”, resembles a flu epidemic: it hits most of us stealthily, there is no fully effective vaccine and it is benign but it collectively causes enormous damage. Unlike the flu, however, it is chronic and it poses a continuing and expanding threat of harm.

The similarity to the flu extends further. For example, SPAM imposes heavy costs on our communications-care system by burdening its facilities to the detriment both of our normal use and of the adequacy of service by the providers. SPAM also, like the flu, carries with it the threat of more serious abuse, e.g. of “aggravated infection” of our system and of “complications” caused by viruses, scams, pornography and other kinds of malignancies in the hands of wrongdoers.

In the same vein, protection against SPAM starts with limiting exposure: we should “stay away” from its paths, by not making information on how we can be reached easily
available and by not visiting places through where the virus can get to us. It is here that the legislative and administrative measures for the confidentiality of personal data help, including in particular the prohibitions against the intermediaries disclosing such data to potential exploiters; and it is here that our own door-closing remedies (opt-ins or opt-outs, the distinction is not crucial) could play a crucial role if adequately enforced by making it easy for us to “just say no” once and for all generically to all SPAM.

Given the worldwide expansion of the SPAM virus and the innumerable places where it can hide and from where it can strike, we need and can conscript our communications-health-care intermediaries to reduce its incidence. The on-line service providers should not accept subscribers and users who are not sufficiently identifiable and reachable. They should be required to use available technology which makes it possible, without too much trouble, to identify typical SPAM sources, including unreliable servers, and typical SPAM content, and exclude them from the system. They should reinforce this policing through appropriate subscription contract clauses. They should close back-door alleys such as open-relay and open-proxy styles. Once the on-line service providers have instituted all the safety structures and taken all the measures that protect and clean up their facilities from SPAM, they should be granted immunity for purely transporting messages that may be infected. Yes, some of this will cost money and some of it will limit the freedom if not the license-irresponsibility of the Internet, but so be it!

Speaking of money, it is more than obvious that the major and almost exclusive reason for the SPAM epidemic is that it costs almost nothing to spread the virus and there is profit to it. Consequently, we should consider installing special financial disinfectives – disincentives in addition to the protections outlined above. The Spam-stamp for bulk e-mailings would take care of the problem fully, but it is cumbersome and the average users may object. A Spam license may be easier to administer.

On the commercial side, the “aggressive” advertising aspects of SPAM can be addressed as “unfair competition” both against competitors and against the customers themselves. Thus, the SPAM advertiser, and in particular the seller of the product or service, may be pursued both for violating the NO-SPAM regime outlined earlier and for engaging in unfair competition. What is crucial here is that both these spammers cannot claim lack of knowledge and in addition, especially the second, they are identifiable and reachable by the authorities, including in particular through the money trail of credit card and bank transactions. It follows that the anti-SPAM regime should be strengthened by strong remedies against the merchants, including criminal sanctions.

In a way, there is a similarity with terrorism: a few perpetrators are harming large numbers with garbage in the one case, with fear in the other. In both contexts, given the elusiveness
and globality of the related activity, adopting laws, however severe and comprehensive, is not enough. International cooperation on enforcement, including technological sophistication, is vitally needed and we should applaud and encourage the early efforts in this direction.

7. Annexes

Annex A

Since 7 of our 10 National Reports come from European Union States, we will include below some references to the main related documents from the Union (in reverse chronological order of legal texts).

   “Article 13: Unsolicited communications.
   1. The use of … electronic mail for the purpose of direct marketing may only be allowed in respect of subscribers who have given their prior consent …
   5. Paragraph[s] 1 … shall apply to subscribers who are natural persons.”

   See also:
   “Recital 17. For the purposes of this Directive, consent of a user or subscriber…should have the same meaning as … defined and further specified in Directive 95/46/EC. Consent may be given by any appropriate method enabling a freely given specific and informed indication of the user’s wishes, including by ticking a box when visiting an Internet website.”

   Article 2h of Directive 1995/46/EC defines “consent” as a “free, express and fully informed” action.

   Recital 40. It refers specifically to spam and explains that “it is justified to require that prior explicit consent of the recipients is obtained …”.

   It recognizes the SPAM problem (unwanted content) and proposes funding for anti-spam technologies, especially filtering, through 2008. See Art. 1.1 and Explanatory Memorandum 3.2.2 (user empowerment)

   This is a very comprehensive anti-spam document. Examples:
   [5] Spam: invasion of privacy, time consuming, increase of costs. Also often misleading, deceptive
   [8] ISPs and e-mail providers are burdened and have to create more space
   [31] Directive 58 applies to all messages received on and sent from networks in the Eu

   Art. 7 requires that, where SPAM is permitted, service providers must make certain that it is recognizable as such and also must set up and consult registers for natural persons who are unwilling to receive it.

   In Recital 30, it is stated that the “sending of unsolicited commercial communications by electronic mail may be undesirable for consumers and information society providers” and it may disturb the normal operation of the Internet.
   Reference is then made to Directives 1997/7/EC and 1997/66/EC on the needed consent of the recipient and it is stressed that such communications should not result in extra communication costs for him.

   While under Art. 3 the service providers are generally regulated only by the state of their establishment, an exception is provided in the Annex as concerns unsolicited commercial e-mail. At the same time, Art.12 frees from responsibility, for the messages handled, a service provider who merely transports them or makes available access to the Internet, and is not their source, does not select the recipient and neither chooses nor modifies their content. Similar rules apply to caching and hosting (Art. 13 and 14) and Art. 15 establishes clearly that service providers not only are under no general obligation to monitor the information that they transmit or store but are even under no general obligation to make an effort to examine whether it is related to illegal activities.
However, Recital 46 clarifies that when such service providers obtain actual knowledge or awareness of illegal activities, they must act expeditiously to remove or disable access and, further, Recital 48 preserves for the member states the possibility of imposing on them a duty of care to detect and prevent certain types of illegal activities.

5. Directive 1997/7/EC on Protection of Consumers in Respect of Distance Contracts
   Article 10(b)2 merely provides that the States may require that communications such as e-mail may be used only if the consumer has not expressed clear objection. Obviously, this limited protection is not significant in the entire anti-spam picture.

   The thrust of this major Directive is to prohibit the collection, processing, storage, use, communication etc. of personal data without the free, express and informed consent of the person concerned (Arts. 2h and 7a). There is no question that practices on the Internet are covered and that most of the information needed by spammers and harvested on the Internet qualifies as such data. See, also, Art. 14b. Arts. 22-24 and 28 contain a full range of remedies and protection for the victim and there is no doubt, also as provided in the subsequent Directives discussed above, that the on-line service provider may be liable for the collection, storage, processing or dissemination of such data except to the extent absolutely necessary for the use of such service.