

Spam: from a curious nuisance to a devastating, global problem.

By:
Avv. Dr. Felix Hofer¹

Hofer Lösch Torricelli - www.htlaw.it

If you talk to an American, he'll tell you that most of the spam that daily floods his e-mail inbox comes from Europe or Asia. On the same topic a European will say that 90% of the spam he gets originates from the United States².

While both of them could easily be right or wrong, as junk mail might be transmitted from servers located in some obscure place, but actually could be sent on behalf of companies from the areas mentioned above³, it is hard to believe that spam in just a few years developed from a disturbing phenomenon, to a true nuisance, to a intensely debated issue, and an immense, critical problem, that seriously affects a number of businesses and sometimes threatens their survival⁴.

Spam is simply everywhere, it hits e-mail communication badly, however we can hardly do without such communication technology, and – despite periodic announcements about new miraculous software, able to prevent the inconvenience of spending significant time each day on cleaning our incoming messages – currently amounts to almost 80% of all electronic communication circulating on the Internet⁵.

As spam became a serious problem, calls for appropriate remedies and strong reactions became louder and louder. Legislators started looking into the issue as did the courts, prompted by business owners suffering economic losses⁶ from spammers and by private citizens angry about a practice they find to be highly intrusive in their privacy sphere.

¹ *Felix Hofer, a founding partner of the Florence (Italy) based law firm "Hofer Loesch Torricelli", is author or co-author of a number of books and articles on advertising, marketing and sales promotions, data protection and on company law. Felix is also a frequent speaker at conferences and seminars on these topics (in Italy and Europe as well as in the United States). Felix is the country representative for Italy in the European Advertising Lawyers' Association (EALA – www.eala.net) and in the Global Advertising Lawyers Alliance (GALA - www.gala-marketlaw.com), two networks that link legal offices located throughout Europe, America and Asia, having expertise in marketing law, trade promotions and advertising. He has served as EALA's General Manager in 2001 and 2002. Contact Felix Hofer at fhofer@htlaw.it.*

² With respect to Europe a research from CipherTrust, a company specialized in messaging security, identified nearly 86 percent of all spam sent between May and August 2004 originated in the United States; in general terms, specialists from Sophos have elaborated the following ranking list as to origin of unsolicited commercial communication: 56,74% from the US, 6,80 from Canada, 6,24% from China and Hong Kong, 5,7% from South Korea, 2,13% from the Netherlands, 2,00% from Brazil, 1,83% from Germany, 1,50% from France, 1,31% from the UK, 1,21% from Australia, 1,19% from Mexico, 1,05% from Spain (Italy ranks on the 21st place of the list with 0,54%) . The survey also estimates that a huge amount of bulk email spreading around the Web is actually generated in Russia (which ranks only on place 28 of the list), but diffused through servers located in third countries.

³ e.g. by using 'hijacked' zombie PCs or insecurely installed proxy servers.

⁴ A study by anti-spam company Commtouch indicates that in year 2004 spam messages spread around the world primarily originate from websites located just in five countries: China, South Korea, the US, Russia and Brazil.

⁵ As to the incredible development of the spamming phenomenon, according to a Brightmail survey conducted in July 2002 "unsolicited bulk email made up a whopping 36 percent of all email travelling over the Internet, up from 8 percent about a year ago".

⁶ Research conducted in the UK found that already in year 1998 people interviewed received an average from 5 to 25 junk mails per day, with an estimated cost for business of £ 5 billion a year; another survey from Nucleus Research Inc., Wellesley, Mass., among 82 Fortune 500 companies showed (in May 2004) that in the US "The cost of spam has more than doubled for enterprises in the past 10 months, costing an average of \$1,934 per employee a year based on lost productivity"; with respect to Europe, Radicati Group (an IT consulting firm) estimates that in the period 2004 – 2008 "estimates that spam will account for 46 percent of emails in 2004, increasing to 71 percent by 2008 and will cost European companies EUR 85 billion over the period 2004 - 2008".

Initially privacy laws appeared to offer a suitable approach to solving the problem, especially in Europe, where protection of personal data had been ruled both through a specific Directive⁷, aimed at harmonizing the domestic legislations of the EU member states, in general terms, as well as through an additional Directive⁸, meant to govern privacy in the context of electronic communication.

As a matter of fact the second Directive contains specific rules and provisions⁹ concerning 'unsolicited communications', that:

- require prior consent for approaches performed, for purposes of direct marketing, through automated calling systems, faxes or e-mail,
- impose, with respect to electronic contact details obtained legitimately, to offer a free and easy opt-out system for customers not more willing to receive messages,
- prohibit the practice of distributing electronic messages without clear disclosure of the sender's identity and without indication of a valid address to be used for opt-out choices.

In addition, also another Directive¹⁰, governing electronic commerce, focuses on unsolicited commercial communication and establishes¹¹ that:

- such communication, when performed via e-mail has to be "clearly and unambiguously identifiable as such as soon as it is received by the recipient",
- "service providers" ... "are held to "consult regularly and respect the opt-out registers in which natural persons not wishing to receive such commercial communications can register themselves".

Nevertheless until now neither Community Law¹² nor the national implementing provisions¹³ could succeed in stemming the tide of spam constantly circulating on the Internet and more and more interfering with business in a disturbing and detrimental way.

In an attempt to get some control on the phenomenon by involving the providers¹⁴ and by loading liability burdens on the particular industry with respect to what's 'hosted' and what's 'transmitted', no significant results were achieved. On the contrary, confronted with huge protests from the particular industry as well as from freedom of speech advocates, the Committee of Ministers of EU¹⁵ issued the "Declaration on freedom of communication on the Internet", recommending that:

- the Internet should not become subject to restrictions, which go further than those, applied to other means of content delivery,
- self-regulation or co-regulation should be widely encouraged for ruling content dissemination on the Internet,
- in principle (and save achievement of goals of public interest as protection of minors), public authorities should not, through general blocking or filtering measures, deny access by the public to information and other communication on the Internet, regardless of frontiers,

⁷ See 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).

⁸ See Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

⁹ See Section 13.

¹⁰ i.e. Directive no. 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce').

¹¹ See Section 7 of the Directive.

¹² i.e. the directives and regulations issued by the European Union.

¹³ Adopted by the countries members to the EU.

¹⁴ The "guys easy to get", not able to disappear in the Internet universe.

¹⁵ In a meeting held in Strasbourg, on June 28th, 2003.

- existing barriers for accessing Internet communication and information services should be removed,
- freedom should be granted with respect to providing services via the Internet,
- no general obligation should be imposed on service providers to monitor the content, which they give access to or they transmit or store; neither should service providers be held liable for content on the Internet when their function is limited to transmitting information or providing access to the Internet, while co-responsibility may hit them where they do not act expeditiously to remove or disable access to information or services as soon as they become aware of their illegal nature or, in the event of a claim for damages, of facts or circumstances revealing the illegality of the activity or information,
- for enhancing the free expression of information and ideas, the will of users of the Internet not to disclose their identity should be respected as long as no responsibility for criminal acts is involved.

In earlier times, prior to that Declaration, several EU member states (among them Italy¹⁶), while implementing the Directive on E-commerce, felt that simply transferring the problem on the providers would not result in a suitable solution, apt to control spam, and therefore some specific criteria were introduced in order to rule provider liability.

According to those criteria¹⁷:

- a provider does not bear a general obligation to control the information transmitted or memorized; unless he's called to investigate facts or circumstances indicating illegal acts; on the contrary he's required to report such illegal acts, when acknowledged, to the competent authorities; finally, on request of the competent authorities, he has to comply with instructions for immediate access to blocking illegal content,
- an identical exemption from content control and from liability applies to "mere conduit" providers, save the following cases: (i) when the transmission of the message originates from the provider itself, (ii) when the provider selects the receiver of the message, (iii) when the provider selects or modifies the information transmitted,
- from the same exemption, services benefit as automated, intermediate or temporary memorizing (caching) as long as the provider: does not modify the information's content, complies with terms and conditions for access and updating of the information, does not interfere with the client's use of technology for profiling or data collection purposes, and promptly removes the information once it's no longer present in its original location,
- the liability exemption also covers permanent or long term information storage as hosting services performed by a third party (therefore housing clearly does not benefit from such provision), save the case in which the provider is aware of illegal acts conducted or illegal information supplied by its clients and does not promptly remove such content or block access to it.

At the end of the day the European Union and its member states had to acknowledge that their efforts to force unsolicited commercial communication into specific legal patterns and to achieve, on a domestic level, control on spamming had failed in determining a turnaround with respect to the widespread, incorrect and extremely harmful practice of "mass mailing".

Have Courts been more successful in fighting junk-mail? During the last two years the international press has repeatedly reported on lawsuits filed against spammers, who disseminate millions of electronic promotional messages on a daily basis.

¹⁶ See Legislative Decree no. 70 dated April 9th, 2003.

¹⁷ See Sections 14, 15, 16 and 17 of Legislative Decree no. 70/2003.

US companies have taken the lead in choosing courtrooms as the battlefield and are experiencing the effectiveness of 'economic weapons' (i.e. claiming for huge amounts in damage compensation) in the war against spammers¹⁸.

Also in several European countries spam victims have decided to take their cases into the courts and to seek proper protection of their interests through legal action.

In Spring 2003 a first instance court in Munich (Germany)¹⁹ had to deal with a complaint filed by a lawyer against the business practice of a marketing company. The company allowed all visitors of its website to send a free promotional e-mail message to an address of their choice. The lawyer received 16 messages (some with images) on his business e-mail address and felt disturbed by such practice. The company argued that it had simply offered a service, but could not be considered liable for actions performed by the senders. The Court did not agree with this defense, it found that on the company's side there had been at least co-liability and issued a temporary injunction, ordering the company to halt its practice and set a fine up to 250.000 Euro in case of non-compliance.

In Fall 2004, a German²⁰ second instance court partially revolted a lower court's decision and held²¹ that, even after the coming into force of the new Act on Unfair Competition, one single "cold"²² message transmitted via e-mail could result in an incorrect business practice. In addition, the Court of Appeal stated that the receiver was not bound to rely on the sender's promise to restrain from transmitting future e-mail messages and to cancel the receiver's address from its database and mailing list, but legitimately could insist on obtaining a binding obligation from the offender (assisted by sanctions for cases of non-compliance). Interestingly the Court also explained that, while a single commercial communication theoretically did not exceed the level of "a simple nuisance", the issue had to be considered not just as an isolated fact, but in the broader context of spamming as a phenomenon of illegitimate interference with business and, therefore, as an incorrect practice to be opposed according to common perception and understanding.

In the Netherlands the local watchdog on telecommunication services²³ started clamping down on spamming practices and applied²⁴ fines to companies performing such practices²⁵.

Microsoft recently claimed to have taken legal action in 17 cases throughout Europe in order to halt bulk-mail practices and to have directly contacted companies involved in such

¹⁸ In February 2004 EarthLink approached the U.S. District Court of Atlanta and succeeded in achieving a desist order, first, and forced the defendants to an out-of-court settlement, afterwards; in December 2004 the service provider CIS Internet Services was awarded with a more than 1 billion USD judgement from the U.S. District Court of Iowa against several companies performing illicit spamming; Microsoft has filed a consistent number of lawsuits – in some cases in close cooperation with public prosecutors, e.g. the AG of New York – seeking millions of USD in damage compensation from spam companies (from the U.S. District Court for the Central District of California MS was awarded with a \$3.95 million verdict; in another case a company was forced to bankruptcy after a court had ruled in favour of MS); in January 2005 the State of Texas filed a civil lawsuit in a federal court in Austin against spammers. America Online and Yahoo have also lawsuits pending in federal courts, in February 2005 Pfizer and Microsoft have jointly taken legal action against spamming relating to pharmaceutical products before courts in New York and Washington.

¹⁹ Landgericht München I, order dated April 15th, 2003, case no. is: Az. 33 O 5791/03

²⁰ Oberlandesgericht (OLG) Düsseldorf, case no. is: Az. I-15 U 41/04.

²¹ Judgement dated September 22nd, 2004.

²² i.e. unsolicited commercial communication.

²³ OPTA, i.e. a governmental body and non-departmental agency of the Ministry of Economic Affairs that operates as an Autonomous Administrative Authority. For details see <http://www.opta.nl/asp/en/>.

²⁴ In December 2004, after having collected, on a dedicated section of its website, a consistent number of complaints filed in the previous 6 months. The Authority's reaction is based on the provisions of a new law (in force since May 2004), which prohibits affecting consumers with unwanted commercial communication.

²⁵ One person, involved in four companies held liable for spamming was fined with Euro 42.500, a small printing house with 25.000 Euro.

practices in another 70 cases. In the UK – where two lawsuits have been filed²⁶ - Microsoft assumes that spammers achieved the targeted e-mail addresses through ‘harvesting’ the company’s computers and grounds its claims on the Misuse of Computers Act of 1990.

In Italy Microsoft has filed a claim²⁷ before a local first instance court²⁸ against a defendant, who had previously accepted (in an out-of-court agreement) to restrain from sending mass mails, but then had continued in such practice, in blatant breach of the obligations he had undergone.

Another Italian first instance court²⁹ had been approached by a consumer association complaining about mass mailings disseminated, in absence of prior consent from the targeted subjects, with the purpose to promote fitness and sports products. The association asked the civil court to provide compensation for both, immediate damages as well as moral ones, and obtained a decision³⁰ awarding 1.000 Euro in damages and 750 Euro in legal fees; in addition the judge ordered the decision to be published (on behalf of the defendant) in four leading national newspapers and one weekly magazine. In this case, spamming was found to be illicit on the grounds of unauthorized handling of personal data and of undue intrusion into the targeted subjects’ privacy sphere.

Nowadays such a court action would benefit from the new provisions introduced by the Italian “Privacy Code”³¹; those provisions not only entitle³² the local Privacy Commissioner to require providers of electronic services to adapt filtering/blocking systems against IP addresses from which originate unauthorized mass mailings, but also state³³ that illicit spamming may result in a criminal offence³⁴, while damage compensation may still be sought by the offended subjects.

So, could we assume that going to court is a proper remedy for fighting spam? The question deserves a – at least partly - affirmative answer, provided that:

- the economic losses derived from spamming practices impose a concrete and strong reaction,
- the legal framework of the country, where court action has to be taken, offers valid, reasonably quick and not excessively costly remedies against such practice,
- the offender is located in a place, where effective enforcement is granted to court decisions, ruling against subjects performing illicit mass mailing.

The problem still stays and remains when spammers are difficult to locate or have their companies (and assets) established in places where enforcement appears to be problematic.

So, while major companies and industry sectors have started gathering and coordinating on a national level, joining forces in the struggle against bulk-mail³⁵, it’s quite clear that a global

²⁶ in 2003, with the Royal Courts of Justice in London.

²⁷ in February 2005.

²⁸ Tribunale civile di Torino.

²⁹ Giudice di pace in Naples; the claim was filed in September 2003.

³⁰ Dated June 10th, 2004.

³¹ a Consolidated Act, that came into force in January 2004.

³² See Section 130 of the Code approved through Legislative decree no. 196 dated, June 30th, 2003.

³³ So Section 167 of the Code.

³⁴ Punished with imprisonment from 6 up to 24 months.

³⁵ In the US top companies have coordinates their initiatives; the Austrian providers’ association ISPA has prepared a joint strategy and come up with a specific “Spam Code of Conduct” since 2003; in Japan a number of companies including leaders in the mobile phone and computer industry sector have recently – in 2005 - set up an ‘E-mail Anti-abuse Group’, meant to perform research on how to fight spam not only on a legal, but also on a technical level.

phenomenon like spam calls for action on a higher level and implies necessary international cooperation and multi-national treaties³⁶.

Precisely in that direction several initiatives and efforts have been put into place recently. The UN has become aware of the seriousness of the problem and is promoting a harmonized set of rules for controlling spam. In this area the UN act through the International Telecommunication Union (ITU)³⁷, having its headquarters in Geneva /Switzerland). The ITU hosts the World Summit on the Information Society (WSIS), which is structured in two distinct phases: the first took place in Geneva December 10 - 12, 2003, where 175 countries adopted a Declaration of Principles and Plan of Action; the second is due in Tunis, on November 16-18, 2005. The Action Plan adopted in Geneva explicitly lists among the targeted goals the following: "Take appropriate action on spam at national and international levels"³⁸. Recently, at ITU's fifth annual Global Symposium for Regulators (GSR)³⁹ a breakout sessions was specifically dedicated to the topic "How to combat spam".

The Organization for Economic Co-operation and Development (OECD) already a couple of years ago set up a special task force, dedicated to study the phenomenon of spam and to come up with a common, international strategy for fighting illicit practices.⁴⁰

The EU's Commission is also quite sensitive towards the problems implied by spamming practices and during the recent Asia-Europe Meeting⁴¹ 38 countries⁴² agreed "to take action to fight spam nationally and to promote anti-spam efforts in international organizations and by industry" (the outcome of the meeting appears to be of particular importance as the agreement was reached with the participation of China and South Korea, two countries from which approximately 30% of all mass mailing circulated on the Internet originates).

The International Chamber of Commerce (ICC), through its Commission on E-Business, IT and Telecoms, has issued a policy statement on "spam", according to which the fight against "spam" consider "a multi-faceted approach" and involves action through or by:

- **Education and cooperation** (business and government will have to make joint efforts, in public-private partnership, for educating users and businesses with respect to mass mailing practices),
- **Technology** (developing technological solutions to spam is crucial; therefore industry, governments and consumers should cooperate in promoting awareness of technological progress),
- **Industry** (self-regulation through code of conduct and other tools helps business to best manage legitimate commercial communication),
- **Government enforcement** (proper enforcement of existing legislation is an essential factor for preventing harmful, fraudulent, misleading or illegal messages).

³⁶ France's consumer protection council (CNIL), UK's Office of Fair Trade and several other legislative and governmental bodies (among those the US Federal Trade Commission) have met in London in Fall 2004 in order to discuss a common front for action against unsolicited electronic communication; in addition France's CNIL and the respective Dutch authority (OPTA) have prepared a special memorandum, aimed at granting cooperation between European countries for handling trans-national complaints against illicit electronic communication (such memorandum up till now has been approved by Austria, Belgium, the Czech Republic, Cyprus, Denmark, France, Malta, the Netherlands, Latvia, Ireland and Italy).

³⁷ an international organization within the United Nations System, where governments and the private sector coordinate global telecom networks and services.

³⁸ See Section C5. "Building confidence and security in the use of ICTs", no. 12, point d.

³⁹ held on December 8th - 10th, 2004 in Geneva, Switzerland.

⁴⁰ At OECD's workshop held in Busan, Korea, on September 8-9th, 2004 spam was the key argument, and a previous OECD workshop on the same issue was hosted by the European Commission in Brussels on 2-3 February 2004.

⁴¹ Which took place in London, on February 21st-22nd, 2005,

⁴² 25 from Europe and 13 from Asia (among those: Cambodia, China, Japan, South Korea, Vietnam).

In conclusion, it appears clear that just like any other tricky and problematic issues (just think about; money laundering, tax havens, counterfeiting and piracy) proper solutions depend widely on the possibilities of timely and effective enforcement of laws and court decisions. Given the characteristics of electronic communication, such goal can be reached only in the context of intense and extensive cross-border cooperation. In other words, only if we succeed in allowing offended subjects to “go after the bad guys” in as many geographic locations as possible, there will be a chance to obtain at least some control on a devastating phenomenon called “spam”.