

Contact Network of Spam Authorities (CNSA)

Cover note

Title of the document: « Results of the initiative taken by the CNIL in relation with unsolicited electronic communications »

Origin and author: The French Data Protection Authority “Commission nationale de l’informatique et des libertés” (CNIL)

Date: February 2003

Version number: 1.0

Language: English

Contact person: Leslie Basse, Legal Department, CNIL (l.basse@cnil.fr)

Scope: This document presents the results of the CNIL « spam box » operation.

Action : /

Complementary observations: /

RESULTS OF THE INITIATIVE TAKEN BY THE CNIL IN RELATION TO UNSOLICITED ELECTRONIC COMMUNICATIONS.

February, 2003.

In July 2002, the Commission announced the opening of an electronic mailbox (spam@cnil.fr), so called 'spam box', allowing Internet users to transfer unsolicited electronic mails which they received known as 'spam'¹.

This initiative demonstrates the desire of the Commission to manage with the phenomenon of 'spamming' and to provide Internet users with means of dealing with this nuisance. It must be specified that this initiative never aimed at resolving the problem of spamming as a whole.

This report concluded this operation which lasted 3 months and consisted in managing and analysing the messages that arrived every day at the Commission.

1. AN OBSERVATION: EDIFYING RESULTS WITH REGARD TO THE EXTENT OF 'SPAMMING' IN FRANCE

The opening an e-mail address dedicated to receiving the messages that burden the letterboxes of French Internet users received a particularly favourable response from the public. As an example, from July to October, more than **325 000² spams** were received.

This figure demonstrates how many users have rallied the operation 'spam box'. A probable reason for this is that Internet users have found with the CNIL an institution that took over the problem of 'spamming' faced with which they are usually helpless, both from the technical and legal perspective.

It is important, however, to point out that all of the messages received may not be considered to be real spams.

'Spamming' or 'spam' is the massive and sometimes repetitive dispatch of unsolicited e-mails to individuals with whom the sender has never had any prior contact and whose e-mail address has been obtained irregularly.

¹ The term *spam* is used to designate unsolicited e-mail that is often of an advertising nature. This expression comes from a Monty Python sketch in which the word *spam* (contraction of 'spice ham', an English brand of pork meat) is constantly repeated in order to push the listeners into becoming consumers.

² This figure is a conservative estimate, as the internauts often attach to their message an attachment that includes several spams.

Since 1999, the CNIL adopted, within the context of a report on “Electronic Direct Mail”, recommendations relating to these new practices of marketing via electronic bulletin boards.

“Spams” are messages sent on the basis of irregular collections of e-mails, either by means of search engines in public internet spaces (web sites, discussion groups, distribution lists, chat...), or where email addresses have been communicated to third parties without prior information of individuals on this communication and irrespective of their right to oppose this communication . Such collection is unfair and therefore illegal under the terms of Article 25 of the Law of 6 January 1978.

Usually, these messages do not have a valid dispatch or “reply to” address and the “unsubscribe” address is non-existent or invalid.

Not all the messages received and considered by the users to be spam meet this definition. For instance, some Internet users considered to be victims of ‘spam’ when they received a humorous e-mail or a message dispatched to another recipient from a relative or friend. Likewise, some users considered as unsolicited electronic communication a newsletter sent from a site to which they had subscribed previously but which they had forgotten (this is the case, for example, of an Internet user complaining about receiving a newsletter from the newspaper *Le Monde* or from the Senate).

Certain Internet users have also interpreted regular electronic solicitation operations to be ‘spam’. Under current law and with regard to the Law of 6 January 1978, such operations are legal on condition that they comply with traditional requirements : fair collection of the e-mail address, notification of the list used for the operation and possibility, for the person solicited, to exercise his right of opposition. Some Internet users however considered that such operations fell within the category of ‘spam’ and some recipients therefore transferred the messages received to the email address opened by the Commission.

The cases analysed above are, however, marginal and the immense majority of the messages received well deserve the qualification of ‘spam’.

The first task carried out from the messages received was to analyse the content of these to allow classification and therefore a better understanding of the phenomenon of ‘spamming’ in France.

1.1 The lessons

The idea of suggesting to French Internet users to transfer the messages that they considered to be spam resulted, in part, from the Commission’s desire to understand the full extent of this phenomenon, both quantitatively and qualitatively. In other words, in order to provide elements of reflection in the debate on this practice, it was important to provide reliable figures and data. This operation was the first occasion on which figures related to spamming in France were produced by a public authority.

The messages received have been classified by the services of the Commission. Firstly, the operation was done in using the basic functions of automatic classification (for

example, using key-words in the message). Secondly, this automatic classification was supplemented by manual classification when necessary to sharpen the results.

In application with this method, the mails received have been classified, initially, according to **their supposed geographic origin** which led to the conclusion that **84.8 % of spams are drawn up in the English language, 8 % from Asian origin** whereas **7 % are drawn up in the French language**, while the proportion of messages in another language (German, Spanish, etc.) was negligible.

'Scams' (fraud) of indeterminate origin, and which are usually drawn up in the English language, have been classified in a specific category.

Each category - with the exception of Asian spams - was then further classified according to the **content** of the message and therefore of the targeted recipient. This choice was made in order to determine what type of Internet user was really aimed at since, by definition, a 'spamming' operation does not carry out targeted dispatching.

It appeared that individuals, as opposed to companies, are the main targets of spams: **85%** of spams propose products or services that would be of interest to individuals whereas **15 %** of spams were aimed at companies.

Spams in English were classified according to the following themes set out in ascending order: Legal assistance (lawyer, civil procedure, etc.) - (0.2% of the messages received), Games/casinos (1%), Tourism (1.4%), Health (Viagra, dietary products, nutritional supplements, etc.: 12.9%), Financial products (credits, reimbursement of debts, loans, miscellaneous investments, etc.: 40%), and finally, messages of a pornographic nature or proposing encounters represent the largest theme (42%).

A more precise classification was applied to **spams in French**. In order to be able to obtain more information, the messages were divided into major categories according to the target public:

- *Messages intended to canvas individuals*

Spams intended to solicit individuals (commercial solicitation, invitation to visit a Website, proposition of varied services, etc.) were included in this category. Certain sectors of activity could be identified that grouped together a substantial number of companies issuing spams. These sectors are therefore at the origin of substantial solicitation operations. According to this procedure, and again in ascending order, the following sectors were identified:

The *Health* sector is the weakest, representing not even 1% of the messages received.

The *Property* sector is at the origin of 0.9 % of the messages.

The *Employment* sector represents 1.1% of the messages.

The *Clairvoyance* sector, 2.3 % of the messages.

The *Entertainment* sector accounted for 2.3% of the messages received, including, for example, spams encouraging individuals to visit a humorous site.

One category, '*Fraud*'/*Chains/Miscellaneous*, was created in order to classify atypical messages and/or messages proposing doubtful offers, accounting for 3.3% of French spams received.

The *Credits/finances/insurance* sector is at the origin of 5 % of spams received.

The *Games/Casinos* sector represents 6.2 % of spams received by Internet users.

The *Tourism/Travel* sector represents 6.5 % of spams received, Suniles being the company at the origin of the greatest number of messages.

The *Offers of goods and services on-line* sector (purchase on-line of mass consumption goods and services linked to the internet) is responsible for 12.3 % of the spams received.

Finally, *spams of a pornographic nature* is at the origin of 55 % of the spams received. The 'X Top 50', promoting the best "X" sites on the web, being the origin of the greatest number of messages.

A last category entitled *Other offers of goods and services* was created in order to group together offers that do not correspond to any of the sectors identified above. This represents 4.7% of messages received.

- Messages offering services to companies

The two main sectors identified are:

The *Training/Employment/recruitment* sector, that represents 5 % of spams received.

Above all, the *products and services linked to information technology* sector, in which offers relating to e-mail/ mailing list extractors ("robot mails"), represents 74 % of spams received. Several companies were responsible for the sending of such messages, ABS being at the origin of the greatest number of messages.

Finally, another category is set aside for *newsletters* which one imagined were requested by the Internet users (newsletter from the newspaper *Le Monde*, from the Senate, from the newspaper *La Provence*, etc.).

1.2 What conclusions can be drawn?

In the first place, this operation has unsurprisingly confirmed that the great majority of spams were anglophone, which can be explained by the fact, firstly, that nearly 80 % of the content published on the internet is available in English and, secondly, that the use of the internet is more extensive in the United States than elsewhere. Finally, the United States

does not have federal legislation on the protection of personal data - although some states have passed anti-spam legislation .

As for the content of the messages, the analysis of the subject matter of the messages received pointed to notable differences between messages drafted in French or in English .

Firstly, a substantial percentage of the anglophone spams concerned the financial and health sectors, respectively 39.4% and 12.9%. This proportion is not to be found within French 'spams' and can be explained by a legislative and regulatory framework for these sectors that is much stricter in France and in the European Union than in the United States, as well as by consumption habits of households and individuals that is significantly different on both sides of the Atlantic.

The proportion of spams of a pornographic nature, not surprisingly, is the largest and equally concerns messages in English or in French.

Secondly, it appears that the practice of 'spamming' in France is essentially the work of small companies, which use the internet and its characteristics as a privileged means of communication. As a matter of fact, unlike other types of solicitation, the capture of personal data on the internet is easy, while the final cost of the solicitation is mainly undergone by the persons canvassed, as the receipt of such messages increase the network connection time. In summary, the internet is the ideal medium for companies with limited resources or for companies which offer services and products at the edge of legality, to gain access to a very vast group of people at the least cost.

Further, in addition to providing a 'spam box', a test was made which consisted in opening various accounts with the main suppliers of free email services. The electronic addresses thus created were never used to send any message and their existence was not disclosed outside the CNIL. It appeared, after a few days, that one of them, located with Hotmail, was full of 'spams'. The choice of one's e-mail supplier is not, therefore, without consequence in relation to the receipt of unsolicited electronic messages.

Some of the messages could have content of a paedophile nature. In these cases it was decided that all messages that could contribute to allowing identification of their senders would be transferred to the legal authorities specialised in combating this type of criminality.

2- A DOUBLE RESPONSE TO BE MADE

The spectacular mobilisation of French Internet users on the occasion of this 'spam box' operation gave rise to great expectations. The initiative taken, however, never had the objective of resolving the problem of 'spamming' in its entirety. What remains is the expectation that the Commission should at least take an unequivocal position. Thus, an initiative based on two main ideas appeared necessary.

Firstly, an educational part should help Internet users understand the main characteristics of the 'spamming' phenomenon and supply them with the means of protecting themselves from the receipt of unsolicited messages.

Secondly, a deterrent part - referring certain cases to the Prosecution Department - should allow prosecution of some of the more substantial authors of unsolicited e-mail.

2-1 An indispensable pedagogical initiative

One of the merits of the 'spam box' operation has been to stigmatise the practice of 'spamming'. Thus, a sizeable number of Internet user spam victims are unaware of its main characteristics (its illegal character, its costs, how to protect oneself against it, etc.). Some even have the feeling that receiving unsolicited advertising messages is inherent to use of the internet.

From a pedagogical point of view, it appeared indispensable in the eyes of the Commission to carry out **hearings** with the main actors concerned by the problem of 'spamming', and in general by direct e-mail, that is, the access providers of Internet, professionals in marketing, e-business and electronic publishing, consumer and institutional associations.

2-1-1 Auditions and working group

A **working group**, composed of the French Association of Access Providers (*AFA - Association française des fournisseurs d'accès*), the National Consumer Institute (*INC - Institut National de la Consommation*) and the magazine "60 million consumers" and the On-line Service Publishers Group (*GESTE - Groupement des éditeurs de services en ligne*), was established. The National Union of Direct Communication (*SNCD - Syndicat National de la Communication Directe*), the Federation of Distance Selling Enterprises (*FEVAD - Fédération des Entreprises de Vente à Distance*) as well as the Association for On-line Business and Services (*ACSEL - Association pour le Commerce et les Services En Ligne*) were also associated to this consultation. Finally, the Interministerial Family Committee were included in this working group (*DIF - Délégation Interministérielle à la Famille*).

This working method is not without precedent, as a similar consultation was carried out on the occasion of the summary report on e-mailing and the protection of personal data, presented by the CNIL in 1999.

These hearings essentially aimed at enriching and having the actions of the CNIL taken over by these groups on the occasion of their joint campaign against 'spamming', namely by providing a new "module" called "Stop spam!" (see below) published on the CNIL site.

The lively debates raised by the phenomenon of 'spamming' also lead the Community authorities to adopt, on 12 July 2002 a directive relating to privacy and to electronic communications³ that have the interest of clarifying the rules applicable to this sector, notably by retaining the principle of prior consent for the direct solicitation of persons by electronic means.

The provisions are to be transposed into French Law by a bill dedicated to trust in electronic economy ("Projet de loi pour la confiance dans l'économie numérique")

³ Directive 2002/58/CE of 12 July 2002 concerning the processing of data of a persona nature and the protection of privacy in the electronic communications sector.

The Commission therefore welcomes this legislation, which unifies the rules applicable to electronic solicitation and will therefore allow an efficient campaign against the senders of unsolicited electronic messages, without the need to rely on alternative legal provisions.

In any event, it is obvious that this legislation will only have full weight once it is transposed into national law and when criminal sanctions are established in this respect.

Finally, it also seems important to inform those involved with electronic solicitation (companies and individuals) of the impact of this new legal framework on their activities.

2-1-2 The educational module

An educational module called *Stop spams!* was put online on the CNIL Website on the same model retained by the Commission as to inform Internet users on the possibility that individuals are traced on the internet (See the module “*Your traces*”) or to inform them on the specific protection that must attach to minors (See the module “*Junior Space*”), . This module is only accessible in a French version.

In brief, this module is built around the following points: the action of the Commission following the opening of the address spam@cnil.fr (deliberations relative to the cases referred to the Prosecution Department and corresponding press release), information on the characteristics of ‘spamming’ (definition, statistical analyses and state of the law) and practical advice for the attention of Internet users and professionals (technical and legal assistance, “anti-spam” reflexes).

2-2 A deterrent section expected

The Commission did not wait for the introduction of the ‘spam box’ operation to start working on the phenomenon of ‘spamming’. Thus, from the time of its report “Electronic Direct Mail” of 1999, the Commission had worries that events did not refute. The opening of an electronic letterbox specially dedicated to receiving this type of message has, through its media repercussions, provoked a strong mobilisation that the Commission is now trying to reflect in the stance that it takes. Thus, the interest in this operation, apart from the statistical aspect referred to above which does not specifically fall within the powers of the CNIL, allows identification of the biggest ‘spamming’ campaigns and prosecution of these practices that are clearly contrary to the provisions of the law that the Commission has the task of enforcing.

The Commission, from the moment this operation was launched, indicated that it would not be able to give an individual response to each case, but that it would use them to prosecute fraudulent actions that they became aware of.

It must be pointed out that referring to an infringement of data protection legislation can be but very rarely relied on by the recipients of the unsolicited messages who, however, are their main victims.

2-2-1 Assessment of the practice of ‘spamming’ under the Law of 6 January 1978

Paradoxically, although the practice of ‘spamming’ is highly resented by the Internet users whose privacy is thereby breached, very few legal actions have been brought under the provisions of the Law of 6 January 1978.

There is no shortage of grounds for such an action, however.

From the outset the Commission has constantly admitted that an electronic address is personal data, so that the persons holding title to it benefit from the protective provisions of the law.

The practice of ‘spamming’, taken as a whole, breaches the provisions of the French data protection law on at least three points.

In the first place, the method of collecting addresses that serves the ‘spamming’ operations is clearly illegal.

Persons who are victims of this practice have not, by definition, communicated the e-mail address to the various companies who seek them for the purposes of solicitation. The analysis of the spams received by the Commission and the various practices observed show that the companies at the origin of these, in the immense majority of cases, use tools called ‘mail extractors’ (*robot-mails*), allowing collection of the electronic addresses published in the public spaces of the internet (discussion forums, personal or company pages, etc.) to make up solicitation files at the least cost.

Secondly, the persons or companies that are at the origin of sending unsolicited messages for purposes of solicitation do not allow effective use of the right of opposition.

Just as Article 26 of the Law of 6 January 1978, Article 14 of Directive 95/46 acknowledges that every person has the right to oppose the commercial use of its data or the transmission of these to third parties.

As highlighted in the above-mentioned report of 1999, the collection of the e-mail addresses of persons for the purposes of commercial solicitation without proper prior information of the latter ignores the guarantees offered by the general directive of 24 October 1995.

Further, upon receiving ‘spam’, no option is offered to Internet users to object, in the future, to receiving similar messages. Where such “unsubscribe” links exist, either they are inefficient, or they only serve to ‘validate’ the e-mail address used, that is, to classify this address as still being valid as effectively used by the holder. Many messages from Internet users have informed the Commission of these problems.

Finally, an operation of commercial solicitation relying on the constitution and the use of automated processing of personal data – i.e. the e-mail addresses used – “*must, prior to its implementation, be notified to the National Commission on Data Processing and Liberties*”, in accordance with Article 16 of the Law of 6 January 1978.

In conclusion, ‘spamming’ clearly infringes French data protection rules, as it infringes the principles of fair and legitimate collection of personal data

The Commission then has decided, by means of referring several cases to the Prosecution Department, to play its role as the main authority in charge of checking the proper application of data protection law in France, where its provisions have been deliberately ignored.

This position shall serve as an example for all companies involved in the practice of ‘spamming’ at the same time as it will provide Internet users with the legal means for any actions brought by them in court.

The action of the Commission will not stop at this point. Contacts have been taken with some of the French companies identified as being at the origin of ‘spams’ so as to remind them of the terms of the law and to demand that they cease such practices. The Commission hopes that the exemplary nature of the prosecutions will certainly result in a better response from the companies concerned than a simple reminder of the applicable legal provisions. Clearly, these prosecutions will not put a stop to the phenomenon of ‘spamming’, in very large part of North American origin. It is however an attempt to put a brake on the practices of small French companies that think they have found a slot to increase their turnover by collecting e-mail addresses for the purposes of commercial solicitation irrespective of the law.

2.2.2 The content of the denunciations to the Prosecution Department

The practice of ‘spamming’, as shown above, is contrary to the provisions of the Law of 6 January 1978.

The study of the messages received as well as various cases referred to the CNIL - both by postal and electronic means - have allowed identification, as far as possible, of a certain number of companies that are the source of massive and repeated sending of unsolicited e-mail.

Some examples of these messages were transferred for analysis to the IT department of the CNIL in order to determine their origin, together with various elements allowing to assess these deliveries as illegal. On this basis, several companies have been identified as practising ‘spamming’ due to the number and frequency of the messages sent and, consequently, transferred by the Internet users to the services of the Commission which excludes the possibility of a classic marketing operation.

On the other hand, the diversity of the recipients of these messages (individuals from diverse origins, professionals from multiple sectors of activity) lead to the conclusion that the addresses of these individuals were collected using a “robot mail” type tool, as certain Internet users sometimes expressly indicated that they had never been in contact with the sender.

Furthermore, for each of the cases considered, the recipient’s possibility to opt for not receiving such messages in the future is non-existent or inefficient, this latter situation also being expressly confirmed by certain Internet users.

Finally, concerning the French companies identified, no prior notification of the relevant processing of personal data had been made to the Commission on the date when these messages were sent.

Consequently, on the basis of this report, the Commission referred 5 companies to the Prosecution Department:

- **Alliance Bureautique Service (ABS)** (design and sale of ‘robot mail software),
- **Suniles** (tourism),
- **The ‘X’ Top 50** (promotion of pornographic sites),
- **BV Communication** (promotion of a minitel internet site and dating services),
- and **Great-Meds.com** (on-line sale of pharmaceutical products).

The decision to refer these specific cases arises from the will to identify certain companies that are the origin of the largest deliveries of unsolicited messages while at the same time carrying out a selection according to the content of the messages.

Taking into consideration the big amount of pornographic spams, the Commission referred to the Prosecution Department the case involving the company BV Communication, which was precisely identified by the CNIL’s IT Department, and the person or company at the origin of the messages promoting the ‘Top 50 X sites’ which represents the greatest volume of messages in this category. In this latter case, it was left to the legal authorities to precisely identify the authors of the infringement.

Also, as the origin of the spams largely comes from abroad, the Commission also decided to refer the case of a company located in North America. In effect, as recalled above, close to 85% of the spams received came from the United States. Consequently, it seemed necessary that the French judiciary authorities should hand down a decision on breaches of the provisions of the national law by a company established abroad, and more specifically in the United States.

3 TERMINATION OF THE ‘SPAM BOX’ OPERATION

The objectives of the ‘spam box’ operation have been achieved: the receipt of more than 300,000 messages in 3 months - 100,000 messages per month - demonstrates the extent of what must be considered to be a veritable scourge. Far from constituting an anecdotal curiosity of the internet, the practice of spamming is extremely vivid in France.

The CNIL has undertaken unprecedented action: 5 cases referred to the judicial authorities concerning companies that had carried out massive deliveries of unsolicited commercial messages, whereas the Commission had to date made only moderate use of its power to refer cases to the Prosecution Department (20 cases from 1978 to 2001). The exemplary character of these cases should put a brake on the practices of some French companies that think they can infringe the law with total impunity. As the origin of the ‘spams’ largely extend beyond the French borders, the Commission has also referred a case involving a company located in North America.

The CNIL has henceforth closed the 'spam box' to replace it with an 'anti-spam tool box', on-line on the CNIL Website, that can inform Internet users as to solutions, both legal and technical, that can help them to protect themselves against, and to react to, the receipt of unsolicited e-mails. Professionals have not been forgotten and have issued practical advice on how to lawfully carry out electronic prospecting.