Short Commentaries on the Can-Spam Act

Mário Antônio Lobato de Paiva

President Bush signed (on December 16th, 2003) a bill that will prohibit unsolicited commercial e-mails. Called CAN-SPAM Act (an abbreviation for Controlling the Assault of Non-Solicited Pornography and Marketing Act), the statute was passed in both houses of American Congress by a large number of votes in its favor. In the Senate, the bill was approved unanimously (1), indicating a collective conscience about the importance of it implementation. Despite this demonstration of consensus, the Congress has been debating a law to fight spam for over six years.

The receiving of unwanted e-mails is more than a simply annoying thing; in fact it can cause serious problems to Internet Access Providers (ISP), flooding their informatics systems with millions of junk messages and, consequently, producing real damage in terms of reducing the speed of communications (2). According to some statistics, the number of unsolicited messages has increased by 77 percent compared to last year. Today spam messages represent about two-thirds of the total of electronic communications received by American enterprises.

The bill, which came into force in January 1st this year, is the first federal statute regulating spam. In the USA, various states had already enacted their own legislation regarding this issue; some were stricter than others, but all of them have tried to impose sanctions on spammers in an attempt to solve the massive problem that unsolicited electronic messages have turned into, for example, messages containing pornography, advertisements of viagra, diet pills, get-rich-quick schemes and the like.

Some critics argue that the bill will not induce a decline of junk e-mails. On one hand, we could say they are correct. The problem of spam control involves other types of initiatives, such as technical developments of filter soft-wares and educational policies for the Internet user community. But, on the other hand, a bill like this one enacted was a essential instrument in the fight against spam. Firstly, because the spammers now know they will face punishment. With a bill, describing in a previous way the sanctions one could suffer as a result of spam, the heads of enterprises who used to do that sort of thing will now think twice. The simple existence of the law serves as a crime-reducing factor. Secondly, the bill is a real proof that the Government is concerned with this matter and is tackling this problem seriously. Before it was enacted - except the state laws -, the problem of spam was treated only by private organizations, like media associations and consumer defense entities. The joining of state enforcement structures will bring a decisive long arm to catch and punish the spammers. Thirdly, a federal statute, at least in theory, will resolve a confusion caused by the diverse state legislation. Each of these laws adopts diverse requirements and imposes various standards for the businessman, who never knows which of them he has to comply with. Knowing that in an electronic communication the sender has no idea about the geographical location of the recipient, the former will also not know

which state legislation he must obey. Legal treatment of commercial e-mail on a nationwide basis will bring more legal certainty for all e-commerce participants.
But, although the bill has these merits, there is still room for concern regarding some of its provisions. For example, the bill balanced in favor of the "opt-out" approach, that means, every e-mail marketer can send commercial electronic messages to everyone they want to, until they are asked to stop sending the messages. This possibility causes alarm among spam fighters, who have claimed that the bill will in fact promote the practice of spam. Of course, the bill only authorizes the sending of non-fraudulent commercial messages, but its critics insist that the approach adopted will not work. Imagine every on-line marketer sending a countless number of e-mails until the recipients ask to be removed. There are 22.9 million small businesses in USA, and each one will be able to take advantage of this new legal right.
Another concern resides in the circumstance that the federal law will supplant state legislation, which is, in some cases, tougher than its own provisions. At least 34 states have enacted regulations on bulk e-mail, with strong provisions. California (3) and Delaware for instance, have adopted the "opt-in" approach, that is, a marketer who wants to send an electronic message must ask for prior permission from the recipient. Washington legislation, by its turn, confers to individuals (recipients) the right to directly sue spammers, a right that is not foreseen in the new (federal) statute.
It is also unclear what effect the statute will have outside the USA. It is recognized that the most prolific spammers are based on American soil, and, according to some estimates, they are responsible for sending tens of millions of messages each day. The adoption of the bill will have some impact on their activities, but the extension of this impact is not foreseeable.
Below we will discuss the main provisions of the bill, offering separating comments for each of them:

Definitions (Section 3)

One of the first sections of the law (Section 3) includes specific definitions to some expressions relating to e-commerce and electronic communications as well. These definitions offered by the bill serve to facilitate the interpretation and application of its provisions, giving the law-abiding businessmen a more detailed idea of its general context.
The term commercial electronic mail message, for example, is defined as "any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service". The definition expressly includes "content on an Internet website operated for a commercial purpose" - Sec. 3 (2)(A). That means if a message is sent with the sole purpose to advertise the content of a website, it is considered a commercial message and, consequently, its transmission shall observe the rules now implemented. However, the simple mention in an e-mail about a commercial entity or its website address is not considered a violation of the Act terms, if the content or context of the message indicates another purpose than commercial advertising - Sec. 3 (2)(D).
The prohibitions contained in the Act will not apply to "transactional or relationship messages" - Sec. 3 (2)(B). If the sender has previously "transactional" contact or any kind of commercial "relationship" with the recipient, the acting of sending an e-mail is not considered a legal violation. A transactional or relationship message is defined as a message whose primary purpose is other than to promote or advertise a product or a service. Specifically, an e-mail could enter the concept of a "transactional or relationship

message" if it is transmitted with the purpose: a) to facilitate, complete or confirm a commercial transaction that the recipient has previously agreed to enter into with the sender; b) to provide warranty, product recall or safety information with respect to a commercial product or service used or purchased by the recipient; c) to provide notification concerning a change with respect to an ongoing relationship, such as a subscription, membership, account, or comparable ongoing commercial relationship; d) to provide information directly related to an employment relationship or related benefit plan in which the recipient is currently involved; or e) to deliver goods or services, including products updates or upgrades, that the recipient is entitled to receive - Sec. 3 (17). These are some situations where the "primary purpose" of the sender is not to promote or advertise its products or services, on a first time basis, as we mentioned before. On the contrary, in all of these situations the sender has previous contact with the recipient, as part of businesses transactions, in which the recipient has before agreeing to involve himself in it.

Criminal offenses (Section 4)

Section 4 amends Title 4 of the United States Code, by introducing a new section called "Fraud and related activity in connection with electronic mail". It defines five types of crimes (Subsection a). It is considered a violation whoever in or affecting interstate or foreign commerce, that knowingly:

"(1) accesses a protected computer without authorization, and intentionally initiates the transmission of multiple commercial electronic mail messages from or through such computer,
(2) uses a protected computer to relay or retransmit multiple commercial electronic mail messages, with the intent to deceive or mislead recipients, or any Internet access service, as to the origin of such messages,
(3) materially falsifies header information in multiple commercial electronic mail messages and intentionally initiates the transmission of such messages,
(4) registers, using information that materially falsifies the identity of the actual registrant, for five or more electronic mail accounts or online user accounts or two or more domain names, and intentionally initiates the transmission of multiple commercial electronic mail messages from any combination of such accounts or domain names, or
(5) falsely represents oneself to be the registrant or the legitimate successor in interest to the registrant of 5 or more Internet Protocol addresses, and intentionally initiates the transmission of multiple commercial electronic mail messages from such addresses,

The term multiple, for purpose of crimes defined above, "means more than 100 electronic mail messages during a 24-hour period, more than 1,000 electronic mail messages during a 30-day period, or more than 10,000 electronic mail messages during a 1-year period" - Subsection d(3). For purpose of crime described in paragraph 3, header information is defined as "the source, destination and routing information attached to an electronic mail message, including the originating domain name and originating electronic mail address, and any other information that appears in the line identifying, or purporting to identify, a person initiating the message." - Section 3(8). For purpose of paragraphs 3 and 4, header information or registration information is materially falsified " if it is altered or concealed

in a manner that would impair the ability of a recipient of the message, an Internet access service processing the message on behalf of a recipient, a person alleging a violation of this section, or a law enforcement agency to identify, locate, or respond to a person who initiated the electronic mail message or to investigate the alleged violation" - Sec. 4, Subsection d (2).
Subsection b provides for criminal penalties. There are two types of penalties: a fine and imprisonment, which can be applied together or separately, depending on the circumstances, such as: a) the existence of previous conviction; b) committing one of those crimes defined above in furtherance of any other felony; c) the number of messages transmitted; d) the number of user account or domain registration used to commit the crimes; e) the size of the material loss imposed to the victims; and f) the number of persons assembled to commit the crimes. The imprisonment sanction ranges from one to 5 years.
Subsection c foresees the forfeiture of any proceeds obtained as a result of crime and any equipment (the software or other technology) used to commit it.

Civil provisions (Section 5)

False or misleading header information

Section 5 sets forth some rules for all commercial e-mail, that is, even a transactional or relationship message must comply with its rules. As we have discussed before, if the sender has previous transactional contact or a commercial relationship with the recipient, the act of sending a commercial message to the latter is not deemed a violation. However, no one has the right to send an e-mail containing false or misleading header information, for example. The bill expressly prohibits, for any person, to initiate a transmission of a message whose header information is "materially false or materially misleading". For purpose of this section, "materially false or materially misleading" header information is one "that is technically accurate but includes an originating electronic mail address, domain name, or Internet Protocol address the access to which for purposes of initiating the message was obtained by means of false or fraudulent pretenses or representations" - Sec. 5(a)(1)(A). Header information is also considered "materially misleading" if it "fails to identify accurately a protected computer used to initiate the message because the person initiating the message knowingly uses another protected computer to relay or retransmit the message for purposes of disguising its origin" - Sec. 5(a)(1)(C). A "from" line (the line identifying or purporting to identify the sender) that accurately identifies any person who initiated the message shall not be considered materially false or materially misleading" - Sec. 5(a)(1)(B).

Deceptive subject headings

The Act also includes a provision regarding the "subject line". The first part of Section 5, as we already examined, is related to information regarding the origin of the message. As it is known, all types of electronic messages (e-mail) are sent according to a standard model. All e-mail manager programs function using a standardized frame for the electronic messages, which contains a space for the header information, usually located at the top of the body´s message and containing data related to the name of the sender, the name of the recipient, the date when the message was transmitted and the subject which the message purport to

related with. In general, the header information of an electronic message is divided in 04 "lines". The first one is reserved for the information that indicates the origin of the message (the "from" line) and contains the name (electronic mail address, domain name or IP address) of the person who initiates the transmission. The second indicates the date the message is transmitted. The third contains the name of the recipient, the person the message is sent to (the "to" line). And the fourth is the "subject" line, that is, the line (at the top of the message) that indicates or purports to indicate the subject that constitutes the main topic of the message or the purpose of its transmission. Paragraph 2 of subsection a (Section 5) contains a discipline for the "subject" line, as long as deceptive subject headings are prohibited. These are considered to be any message whose subject heading "would be likely to mislead a recipient, acting reasonably under the circumstances, about a material fact regarding the contents or subject matter of the message". It is indispensable, in this case, that the sender "has actual knowledge, or knowledge fairly implied on the basis of objective circumstances, that a subject heading of the message would be likely to mislead a recipient".
The provision on deceptive subject heading, like most of other provisions of the bill, does not apply to transactions or relationship messages.

Inclusion of a return address (the opt-out provision)

The bill does not prohibit sending an electronic message. Solicited or non-solicited, a businessman or a marketer can send a commercial message to a targeted person, as long as the former inserts an "opt-out" system in the e-mail, that is, a mechanism that the recipient can use to reply communicating his intention to not receive future commercial messages. It can be a "functioning return electronic mail address or other Internet-based mechanism, clearly and conspicuous displayed" - Sec. 5 (a)(3)(A). The bill requires that "opt-out" system remains functioning for no less than 30 days after the transmission of the original message. The original sender of a message also complies with this rule by providing the recipient a list or menu from which he may choose the specific types of electronic messages he wants to receive, as long as the list includes an option to not receive further messages - Sec. 5 (a)(3)(B). A temporarily and unexpected inability in the system, due to technical problems, des not fail to satisfy these requirements, if the sender correct s the problem "within a reasonable time period" - Sec. 5(a)(3)(C).
The bill prohibits sending further commercial e-mails to those who exercise the "opt-out", that is, to those who communicate their wish to receive no more messages, "more than 10 business days after the receipt of such request" - Sec. 5(a)(4)(A). It also prohibits the sender to sell or transfer the e-mail address of the recipient after receiving the "opt-out" communication.

Required disclosures

One of the most sacred principles in consumer protection is the ability to be well informed. The consumer has the right to get all information he needs to act in the market, and, in turn, the supplier has the duty to provide such information. It seems that the bill hs transferred that principle to the cyberspace arena, in order to give the recipient - who in some cases is the actual consumer - the necessary information he needs to avoid unsolicited e-mail. Based

on this presumption, the bill requires the sender to put some indispensable information in the message, such as:
a) advertising notification: it is unlawful to transmit an electronic message unless the sender provides "clear and conspicuous identification that the message is an advertisement or solicitation" Sec. 5(a)(5)(A)(i). The bill does not provide where the notification must appear, in order to comply with its provisions. Therefore, a message could not be treated as unlawful only because the notice is given in the body, not in the space placed for the header information. The requirement is that the message contains a "clear and conspicuous identification", wherever that may be located. However, the common business practice suggests that the notice of advertisement might be placed at the top of the message, more exactly in the "subject line".
b) notice of opportunity to opt out: the bill does not only require the sender to provide an opt-out mechanism; it also demands he gives a notice by which the recipient knows about the possibility to decline to receive further commercial e-mails. Sec. 5(a)(5)(A)(ii). Like the other provision discussed above, regarding the duty the sender has about giving the recipient notice relating to the advertisement nature of the message, this last one does not specify in what location such a notice of opportunity to opt-out has to be placed. However, this kind of notice is usually placed at the end of the message.
c) physical address: not only is an e-mail address required from businessmen and marketers to put in commercial electronic messages; the bill also demands a "valid physical postal address" of the sender. There is an explanation for this sort of requirement: in commercial transactions, it is important for the consumer to know the physical address of the supplier, in order to make complaints or to solicit more information, especially when he could not get in contact using electronic means. Sec. 5(a)(5)(A)(iii).

Aggravated violations

Subsection b of Section 5 provides some rules embedded under the title "Aggravated Violations Relating to Commercial Electronic Mail". It is considered an aggravated violation to initiate a message that is unlawful under Subsection a, if the sender had knowledge that the address of recipient was obtained by:
a) address harvesting: the electronic mail of the recipient is extracted (harvested) using automated means from a website or online service operated by another person, who included a notice stating that the address is not given for the purpose of initiating messages;
b) dictionary attacks: the electronic mail of the recipient is created using automated means that generates possible addresses by combining names, letters, or numbers into numerous permutations.

It is also an aggravated violation:

a) to use automated means to register for multiple email accounts from which to transmit a message that is unlawful under subsection a;
b) to engage in hijacking: the message that is unlawful under subsection a is relayed or retransmitted through a computer or network without authorization (unauthorized access).

The bill provides that the FTC shall, by regulation, specify other activities or practices to those subsection b will apply, if "those activities or practices are contributing substantially to the proliferation of commercial electronic mail messages that are unlawful under subsection "a". Subsection c (2).

Warning labels (on sexually oriented material)

Subsection d requires to any person who initiates a electronic message that contains sexually oriented material (4) to include a mark or a notice in the subject heading ("subject line"). Subsection d(1)(A)
The "marks and notices" mentioned are required in order to inform the recipient about the material ("sexually oriented") included in the message and to facilitate filtering of such message. These "marks and notices" are not provided in advance by the bill, which reserve for the FTC the power to prescribe and publish them in the "Federal Register", and give notice to the public.
The act of including these "marks and notices" does not absolve the sender from obeying the primary rules regarding information in transmission of commercial e-mails. In order for the sender not to be considered as an offender in this subsection, he must comply with the other requirements set by preceding subsections, such as the information identifying the message as an advertisement or solicitation, a notice of opportunity to opt-out and a valid physical address. Besides, the sender shall provide that the matter in the message, initially viewable by the recipient, when it is opened by him and absent further actions, contains only "instructions on how to access, or a mechanism to access, the sexually oriented material" Subsection d(1)(B)(iii). Thus, as we can see, the provisions of Subsection d are not merely a labeling requirement, but a prohibition on including lawful sexually oriented material directly in a commercial e-mail. Whoever violates these rules could be fined or imprisoned for up to five years, or both. Subsection d (5).

Businesses knowingly promoted by electronic mail (Section 6)

Section 6 of the bill is intended to make companies liable for messages sent on their behalf. It prohibits a person from promoting, or allowing the promotion of, that person's trade or business in an e-mail message the transmission of which is in violation of section (a)(1) if:
a) that person knows, or should have known, that it's business or trade were being promoted in such a message;
b) received or expected to receive an economic benefit from such promotion; and
c) took no reasonable action to prevent the transmission or to detect it and report it to the FTC. (Section 6, Subsection a)

Section 6 also gives limited enforcement against the person (referred to as the "third party") who transmits commercial messages on behalf of another person's trade and business. In general, the "third party" is not liable for the transmission of a message in violation of section 5, unless:
a) that third party owns, or has a greater than 50 percent ownership or economic interest in, the trade or business promoted by the infringing message;
b) has actual knowledge the message is in violation of section 5 (a)(1);
c) receives, or expect to receive, an economic benefit from such violation;

Enforcement (Section 6)

A violation of the Act is treated as if were an unfair or deceptive practice prescribed under the Federal Trade Commission Act. However, it provides enforcement by other agencies in certain cases. Also the Internet Service Providers (ISPs) adversely affected by unlawfully commercial e-mail can bring an action to enjoin further violation or recover damages. In actions brought by ISPs, they can recover damages equal to the actual monetary loss. Statutory damages range from US$ 25 to $100 per email, up to a total of $ 1 million. Treble damages are available if the court considers that the defendant infringed the statute willfully and knowingly, or it activity included one or more "aggravated violation
As one can see, there is no provision allowing a civil action directly filed by a physical person against a spammer. Even if being targeted by a message in violation of the Act terms, a physical person can not sue the person of which trade or business were promoted. The victim has to rely in an enforcement action brought by the FTC or other agency (5). Many non-profit organizations that work to protect cyber rights (6) advised the Congress about the validity of including a means in the bill to allow an individual right of action, based upon verification that this would be the most effective way of enforcement (7). But the Congress did not include such a provision.

Preemption of state law (Section 8)

As mentioned above, in the introductory part of this work, the new federal bill preempts state law. For some critics, it's a cause for concern, as long as a good number of state bills are stricter than the new federal one. The opt-in approach, adopted by California and Delaware statutes, will be no longer a valid rule because this clause is now supplanted, just to point out one example of certain aspects of the new bill that does not favor the recipient of commercial messages.
Apart from any state ruling that prohibits falsity or deception in any portion of a commercial message or information attached to it, the new federal bill (which came into force in January first of this year) supplants all other statutes or regulation regarding the issue of commercial electronic messages - Sec. 8, Subsection b(1). Legislation that does not specifically regulate electronic messages will be not affected. For example, the Can-Spam Act does not preempt state laws related to trespass, contract, tort law, to acts of fraud or computer crime. Subsection b(2)(A)(B). The Federal Act also does not affect policies of providers of Internet Access service regarding the act of declining to transmit, route, relay, handle, or store certain types of electronic messages. Subsection b(C).

Do not mail registry (Section 9)

Within six months after the enactment of the bill, the FTC has to present to the Senate a report containing a plan establishing a nationwide "Do-Not-E-Mail registry", a system which is expected to function in a similar way of the widely known "do-not call list". The FTC may establish and implement the plan, but not earlier than 9 months after the enactment.

Reporting provisions (on rewards for information about violation and ADV labeling)
Within 09 months after the date of enactment of the Act, the FTC shall present to Congress a report that sets forth a system for rewarding those who supply information that helps to identify the person in violation of the Act or leads to the successful collection of a civil penalty. Section 11(1)(A). The reward shall be no less than 20 percent of the total civil penalty collect by the Commission.
Furthermore, within 18 months of the enactment, the Commission has to present another report, this one foreseeing a plan for requiring commercial e-mails to be identifiable with the use of characters "ADV" in the subject line, or another comparable identifier, or a recommendation against such plan.
Of course, these report provisions are an attempt to strengthen the enforceability of the Act.

Wireless communications (Section 14)

The Act confers power to the FCC - Federal Communication Commission to regulate specific type of commercial electronic message, those which are transmitted directly to a wireless device that is utilized by a subscriber of a commercial mobile service. Within 9 months after the enactment of the Can-Spam Act, the FCC has to promulgate rules to protect subscribers of mobile services of unwanted commercial messages.

Effective date

The act came into force on January 1, 2004, with the exception of Section 9 (do-not-email registry).

Notes:
(1) The Senate previously voted 97-0 to approve the bill.
(2) In a statement attributed to Department of Justice and Commerce, of the American Government, the costs to companies was estimated about 9 billion dollars.
(3) The californian legislation was expected to take effect in january first, 2004.
(4) The term "sexually oriented material", as it is provided by the bill in another provision, means any material that depicts sexual explicit conduct (as the term is defined in section 2256 of title 18 United States Code), unless the depiction constitutes a small and insignificant part of the whole, the remainder of which is not primarily devoted to sexual matters.
(5) The Act contains a report provision - Sec. 11(1)(B), stating that the FTC has to submit to the Congress, within 09 months after it enactment, a report with a plan to settle a system to minimize the burden of submitting a complaint concerning violations of its terms. The report must include procedures to allow the electronic submission of complaints.
(6) Like, within others, CDT - Center for Democracy and Technology.

(7) A good example of bill which provides means for direct individual enforcement is the TCPA - Telephone Consumer Protection Act.

Disponível em http://www.cbeji.com.br/br/novidades/artigos/main.asp?id=2830 Acesso em.: 17 set. 2007.