By Françoise Becker, CTO, L-Soft

CAN-SPAM and the EU Directive

October 31, 2003, ushered in the new “opt-in regime” for the European Union. Member states of the EU are now required to enact and enforce laws that include, at a minimum, the following provisions with regard to direct marketing e-mail messages:

- Direct marketing e-mail messages may be sent only to subscribers who have given their prior consent.
- A business relationship in which contact information was obtained constitutes prior consent as long as a means to opt out was provided at the same time and continues to be provided with each such message and each message is about similar products or services by the same company.
- All other unsolicited direct marketing communications are prohibited.
- In all cases, concealing the identity of the sender is prohibited.

On October 22, 2003, the U.S. Senate passed “Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003,” or the “CAN-SPAM Act of 2003”. The Act is currently awaiting approval by the U.S. House of Representatives, and may soon become law.

How does the EU directive 2002/58/EC compare with the CAN-SPAM Act of 2003? The Act recently passed by the U.S. Senate does not meet the minimum standards that the European Union requires of its member states. On the other hand, the proposed U.S. law includes many provisions that are not in the EU directive, some of which will be valuable in the fight against spam. However, CAN-SPAM is a decent first step in the right direction. Although it goes through some contortions that would have been unnecessary had it simply adopted an “opt-in” stance, it may be used to pave the way to later federal opt-in legislation.

How the CAN-SPAM Act falls short

- **Opt-out versus opt-in**

  The EU directive requires prior consent from the recipient before any direct marketing e-mail messages can be sent (“opt-in”). The CAN-SPAM Act allows direct marketing e-mail messages to be sent to anyone, without permission, until the recipient explicitly requests that they cease (“opt-out”).

  While both provide for existing relationships to represent an implied consent, the EU directive requires that every message include opt-out instructions, whereas the CAN-SPAM Act exempts “transactional or relationship” messages from the opt-out instructions requirement.

  Even the EU directive is not strict enough. For individuals (“natural persons” in the language of the directive) the rule is “opt-in”, but for business e-mail addresses (“legal persons”) the member states are free to make the rule “opt-out”. Europeans can still expect to get spam at work.

- **What types of messages are covered**

  The CAN-SPAM Act covers only *commercial* e-mail messages. The EU directive covers all direct marketing e-mail messages, including charitable and political messages. Do the senators want to make sure that they CAN SPAM you when they run for re-election?

  In fact, the definition for “commercial e-mail messages” is so narrow in CAN-SPAM that it would be legal to send e-mail unsolicited, as long as the *primary* purpose is not the advertisement contained within it. Should we be shedding a tear for the poor spammers who must now spend valuable minutes coming up with enough non-commercial content so that their e-mails are not considered “commercial” under the Act?

L-Soft is a proponent of opt-in, to the exclusion of any and all opt-out compromises, and regardless of the content of the message. Both documents attack the content of the message when the true problem with spam lies in its abundance. Both the EU directive and the CAN-SPAM Act fall short of the ideal.

Other differences

The EU directive is not meant to dictate a particular law. Its purpose is to direct all member nations to enact national laws that meet certain criteria. The rules in the EU directive are, hence, necessarily broad, without spelling out details. Each nation must enact its own laws within the boundaries prescribed by the directive. Therefore, there are many provisions in the CAN-SPAM Act that are not specifically covered in the EU directive, though member nations of the EU would be free to include them in their national laws. Some will be helpful in curbing the proliferation of spam. Others cause more problems than they solve.

- **Fraud in sending e-mail**

  The EU directive merely states that “disguising or concealing the identity of the sender on whose behalf the communication is made” is prohibited. The CAN-SPAM Act is more specific and prohibits open relay abuses, falsifying header information, generating multiple e-mail addresses to send from, deceptive subject headers, address harvesting and dictionary attacks, and other fraudulent ways of sending spam. These provisions clearly identify acts of concealment that are considered fraudulent and establish specific penalties for such fraud. As such, this Act will make it easier to pursue spammers who use these techniques and should have a positive effect.

- **State Laws**

  The EU directive specifies a minimum legislation for its member states. Individual member states are free to add their own requirements. CAN-SPAM, if enacted, will supersede all state laws. This is positive because having a hodge-podge of disparate statutes makes it difficult for a law-abiding business to do the right thing. Unlike a postal address or a phone number, an e-mail address carries no information about what state the recipient inhabits.

  It is an unfortunate consequence that good state laws will be invalidated. One example is the recently passed California law set to go in effect on January 1,

2004, which requires all commercial e-mail to be opt-in. However, there are many state laws regarding commercial e-mail that are poorly written, and it's a good thing to have them invalidated.

The most important point is that because an e-mail address carries no geographical information, any state law that is more restrictive than the federal law is in effect mandating that law on all of the United States. In the absence of geographical information, e-mail marketers are forced to adhere to a standard that meets all the state laws. It is against the principles on which the U.S. was founded for one state to impose its laws on other states. Therefore, it is right and fitting for legislation regulating e-mail to be enacted and enforced at the federal level.

- **Identification and Labeling**

  In addition to opt-out instructions, CAN-SPAM also requires "identification that the message is an advertisement or solicitation" and a valid physical postal address. It also requires the FTC to produce a report on the feasibility of a subject-line "ADV" labeling law, but fortunately falls short of requiring it. Labeling of any kind opens up all sorts of problems, among which are:

  - It's a first step onto the slippery slope of censorship, with the government requiring a "brand" on certain types of content.
  - It does not help the recipients distinguish between commercial e-mail that they have opted in to and unwanted, unsolicited commercial messages.
  - Spam is in the eye of the beholder: What the sender sees as a business communication may be seen by the recipient as advertisement. A law-abiding business that believes they are correct in omitting the label may encounter difficulties due to the subjective nature of the "what is spam" assessment.

  On the positive side, this can be viewed as a roundabout means of implementing an opt-in regime for commercial e-mail messages. If all law-abiding unsolicited commercial e-mail carries a label, it will be easy for spam filters to recognize them. Legitimate e-mail marketers will be forced to adapt by keeping the addresses of those who opted in to their mailings in separate lists from the others so that they can omit the label for those recipients (to counter the second bullet above). A few encounters with the "subjectivity" problem (third bullet) along with the low delivery rates of labeled e-mails may convince marketers to eventually convert to an opt-in regime anyway. Instead of mandating opt-in straight out, the Act could slowly and painfully force legitimate e-mail marketers to adopt an opt-in strategy. In the meantime it won't help the load on the mail servers that will still have to process and filter the spam.

  This is not an *efficient* way of implementing an opt-in legislation. If that is the intent, it would be simpler to just make the law require opt-in to begin with – that way there is no need to bother with labeling rules at all. Even if that was not the original intent, it will be the effect.

- **Do-Not-E-mail registry**

  The CAN-SPAM Act directs the FTC to develop a plan for a Do-Not-E-mail registry, and authorizes it to implement it, though it does not mandate it. It's a nice dream, but not practical.

  L-Soft is among the many who think that a do-not-spam registry is a bad idea. There has been a lot of discussion about the technological ease or challenge of maintaining such a registry. However, maintaining it is the easy part. What is

difficult is providing access to legitimate e-mail list operators so that they may remove e-mail addresses from their lists **without** providing unethical spammers with a guaranteed source of addresses – or at least an easy way to validate the addresses they harvest from the Web or generate through dictionary and brute-force attacks. Why connect to individual mail servers to validate e-mail addresses when the FTC provides you with one-stop-shopping?

It has recently been claimed that a do-not-spam registry based on hashing technology would permit the removal of e-mail addresses while preventing spammers from gaining access to the raw addresses. But this is the same kind of technology commonly used to store computer passwords. "Password crackers" – programs that guess or reconstruct a user's password from its hash value – abound on the Internet, and they are quite successful with "weak" passwords. Passwords based on common English words or other predictable strings are generally considered to be weak. Unfortunately, most e-mail addresses contain predictable strings, such as AOL.COM or the user's surname. Addresses such as jsmith@xyz.com are particularly vulnerable.

Unlike passwords, e-mail addresses do not change very often. Unscrupulous individuals could "crack" the do-not-spam registry and later sell the addresses to other spammers. These addresses would be more valuable than harvested addresses because they would be valid and would presumably reach a large number of busy professionals and other decision makers, who typically do not put their e-mail addresses on the Web.

An opt-in law would make such a registry unnecessary.

- **Bounty Hunters**

  The Act directs the FTC to come up with a system for rewarding those who supply information about violators. We can only hope that the FTC will have the wisdom to come up with a system that will not initiate a witch-hunt.

A ray of hope

While the CAN-SPAM Act falls short in several ways, it is better than what is currently in place in the United States: a hodge-podge of state laws that are in many cases poorly written and unenforceable, and in some states non-existent.

Most importantly, the Act would provide a baseline that can be improved upon. It provides some protection that is not yet available and stops short of mandating dubious remedies such as "ADV" subject-line labeling and a Do-Not-E-mail registry – instead requiring that these be examined more closely.

One of the provisions in the CAN-SPAM Act is that the FTC will perform a study and produce a report within 24 months on the effectiveness and enforcement of the Act and provide recommendations on improvements, including addressing spam from other nations. Let us hope that this study will discover that EU's new opt-in laws will have been successful in curbing spam (and California's opt-in law as well, if it has any opportunity to take effect before CAN-SPAM is enacted).

There is hope that the next version of this Act will be opt-in.