FTC Spam Forum - Record Supplement, P024407

Françoise Becker
Chief Technical Officer
L-Soft international, Inc
8100 Corporate Drive, Ste 350
Landover MD 20720
francoise@lsoft.com

Thank you for putting together a very interesting and useful forum. I have just a few comments to make on subjects that either were not addressed at all or did not receive the emphasis they deserve. So that my comments may be understood in context, I have also provided a short background on my company at the end of this document.

Public Education

This topic was barely touched on if at all, yet I consider it to be the most crucial step in curbing the proliferation of spam.

Funds **must** be allocated for public education. Spam proliferates because it works. When people stop buying from spammers, the spammers who are in it for the money will stop sending their spam. The buying public needs to get the message: “Never spend money in response to an e-mail from a company with which you have had no previous contact”.

Ad campaigns on television, in the print media, and – yes – in legitimate, opt-in e-mail newsletters, will do more to curb spam than expensive litigation.

A Do-not-spam Registry

At the forum, there was a lot of discussion about the technological ease or challenge of maintaining such a registry. Unfortunately maintaining it is the easy part. The difficult part is providing access to legitimate e-mail list operators so that they may use it to remove e-mail addresses from their lists. The challenge is to accomplish this **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?)

Labeling Laws

Thankfully, the prevailing opinion expressed by the experts at the forum was that “ADV” labeling is a bad idea.

Unfortunately, several of the current anti-spam state laws do require labeling, as do two of the three federal legislation proposals that we heard about (Schumer’s and Lofgren’s

– the only one that did not include labeling was Burns-Wyden though several of the panelists were confused on this subject). It appears that the lawmakers are not soliciting the advice of the experts before going off and making their proposals.

There are many reasons why the labeling laws are a bad idea, but although the panel was clear about the fact that they considered it a bad idea, they were not clear on why. If our legislators are going to benefit from this forum, they need to clearly understand this.

Labeling laws are a bad idea because:

- Labeling all commercial e-mails with “ADV” (or a symbol as proposed by one panelist) does not help the recipients distinguish between the commercial e-mails they want to receive (and have opted in to) and those that they do not want to receive. They still have to go through every e-mail in their in-boxes or (more likely) filter it all out and miss the 10% off coupon from their favorite bookstore that they really would have liked to receive.

- Spam is in the “eye of the beholder”. What one person sees as a “business communication” may be seen by another as an “advertisement”. If a software company sends e-mail to its customers about the new features in the latest version of the software, is that an advertisement or useful information?

- The definition of what qualifies is ambiguous. Should a newsletter that accepts advertising (example: ZDNet Tech Update Today) have an ADV label? If not, what percentage of the message must be non-commercial? Whatever percentage it is, the spammers will find enough filler text to qualify.

- There are other reasons (such as the slippery slope of censorship) which I will not restate here, since they were given sufficient airtime at the forum.

Litigation Challenges

I asked a question during the Q&A at the end of the “Litigation Challenges” panel, which not only was not satisfactorily answered, but the inability of the panelists to answer it raised many more concerns.

If you are a legitimate list operator, using the “golden standard” of “double opt-in”, what information should you maintain for each subscription to protect yourself from frivolous or fraudulent lawsuits?

One of the challenges for a scrupulous litigator ought to be not only to go after the bad guys, but also to make sure you are *only* going after the bad guys. So this seemed like the appropriate panel to address this question. What evidence provided by a defendant would sway one of these litigators to drop an action? Surely if these panelists were willing to take up a lawsuit against a spammer, they would also have given some thought to the circumstances under which they would *not* take one up.

Unfortunately, it appears that this was not something that any of the panelists had given any thought to. Not only that, but the one panelist who finally ventured an answer even questioned the legitimacy of the question.

With laws that allow “private right of action”, what is to stop an individual from signing on to a list and then claiming to be spammed? Even if the company can prove to the satisfaction of the court that the individual did request the subscription, the company will still be required to spend time and money to get to that point. What is to stop an unscrupulous company from engaging people to start such actions against its competitors? The damage from such frivolous or fraudulent lawsuits may be enough to put a small company out of business, even if in the end they win the suit.

Blacklists

There are several problems with blacklists, which the panel did not do enough to shed light on:

- They put the decision in the wrong hands. Corporate e-mail administrators may well use such lists if company management has made a *business decision* to accept the risks of lost e-mails. However, in the case of ISPs, the consumers should have a choice about whether to use the lists for their personal e-mail accounts. Generally, ISPs use the lists in a blanket fashion, blocking mail for all their customers, and often without even informing their customers that they are doing so. When a subscriber complains to me that they are no longer receiving their messages, I tell them to switch to a provider that does not take it upon itself to decide what messages their customers should or should not receive.

- They punish the victims more than the actual offenders. Open relay lists do not list the IP addresses of spammers, but of sites whose resources have been abused by spammers, and in some cases of sites that have never been abused by spammers, but simply have the *potential* to be abused. Some of the more ethical blacklist providers give the owner of the IP addresses the opportunity to correct their open relay before listing them. The less ethical ones will not only immediately list the IP address that has the open relay but *every* IP address owned by the same organization.

- There is often little or no accountability. If your IP addresses are listed incorrectly, you cannot redress the problem by sending e-mail to complain because your e-mails are being blocked, and the sites typically do not list any other contact information. They are often guilty of the same hiding tactics as the spammers they revile.

- There is no standard. Blacklist services are an immature industry dominated by a handful of individuals operating under their personal views about the right way to behave. Therefore there is a great variation in the level of professionalism and thoroughness they bring to the service. Because of the lack of accountability, there is often little that the blacklist’s consumer can do to determine the quality of the blacklists or whether the philosophy behind the listing is concordant with the consumer’s organizational goals. *Caveat emptor.*

- The blacklist maintainers make the assumption that the individuals putting the blacklists to use are skilled mail administrators. As Mark Burgess wrote in *Principles of System Administration*, “Because the number of local networks has outgrown the number of experienced technicians, there are many administrators who are not skilled in the systems they manage.” Even experienced system administrators are not necessarily knowledgeable about the intricacies of mail administration. The blacklists typically do not have documentation that is accessible to novice mail administrators. I even had a run-in with an administrator who had us blocked because he did not understand the difference between a blacklist and a whitelist, despite the instructions on the blacklist service’s web site.

- The negative impact of collateral damage and false positives was not sufficiently emphasized at the forum. The assumption behind the casual acceptance of “collateral damage” is that e-mail is not important, and therefore losing a few legitimate e-mails for the sake of catching spam is acceptable.

  Many organizations and individuals would not share that assumption: much e-mail is not frivolous communication, but necessary and vital for many people. For them, losing a few messages is simply not acceptable on a variety of fronts: work, information, research, personal…

  Many companies rely on e-mail to conduct business. Telecommuters use e-mail for communication with co-workers and business contacts, saving millions of dollars annually through cleaner air, less traffic, commuting time, and so on. Many individuals rely on e-mail for news, especially in repressive countries where unbiased and uncensored news is hard to come by. E-mail makes it possible for some disabled people to communicate in ways that are not possible otherwise, and in some cases opens up avenues of employment to them. Individuals with health problems use e-mail for support. Internet communities are formed through e-mail discussion lists. Researchers share ideas across the globe.

Finally, the panel did not at all address the concept of “whitelists” – individually maintained lists of addresses from which you want to receive mail to the exclusion of all others. These lists are a very good tool for home users who only want to use e-mail to correspond with family and friends. Unfortunately, they are not helpful for people who want to subscribe to newsletters and discussion lists, participate in Internet communities, or simply to conduct business on the Internet, so they are not sufficient to stop the spam problem.

ISPs should continue to offer whitelist capabilities to their customers, but would do well to move the blacklist capabilities away from the mail server and put them in the hands of the individual recipients: let each recipient decide whether they want their own mail processed through the blacklists, and clearly explain the consequences of either choice.

Legislation

Any anti-spam legislation must cover fraudulent claims, falsifications, and so on. I agree with all that was said on that subject at the forum. I only want to address the issue of who can be mailed to: the only legislation that can work is an “opt-in” legislation.

If you require “opt-in”, there is no need for expensive and technologically challenging registries, dubious labeling laws, or blacklists. Most of the complications in the currently proposed legislation stem from the fact that the proposed laws are attempting to curb spam while still legitimizing “opt-out” mailings. Any attempt to formulate such a paradoxical law will necessarily riddle it with complications and loopholes making it unenforceable and ineffective.

Prior business relationships should constitute an implied opt-in unless the recipient has specifically stated otherwise. This should also be extended, in the case of business-to-business communications, to prior relationships between the businesses rather than to the individual sender and recipient.

Legislation must be worded so as to discourage frivolous or fraudulent lawsuits, which is a danger that comes with “private right of action”. The real challenge of legislation is to define what constitutes proof that a communication was unsolicited. Due to the nature of the SMTP protocol, even records of a double-opt-in confirmed subscription are trivially easy to fake, and therefore unreliable as proof, and it becomes the word of one individual against another. Since most of the accepted definitions of spam refer to the “bulk” nature of the offending e-mail, the legislation should require a certain critical mass before a lawsuit may be filed. Then it is no longer the word of one individual against another, but that of many individuals, lending it credibility. This would make it easy for ISPs and anti-spam coalitions to file a suit against the real spammers while making it difficult to engineer frivolous or fraudulent lawsuits.

Finally, the laws need to address all unsolicited bulk e-mail, not just commercial e-mail. Spam is a problem because of its volume and its indiscriminate and inappropriate distribution, not because of its content. If the legislation addresses the method rather than the content, it will avoid charges of censorship as well as allow the pursuit of spam from the so-called “script-kiddies” who send spam out of mischief rather than for profit. This is yet another example of why “opt-in” is the better solution.

Misuse of Trademark

Several of the panelists misused the registered trademark “LISTSERV” as a generic, and I would be remiss in my duty to uphold this trademark if I did not point this out and ask that the FTC refrain from extending the panelists’ mistakes into subsequent discussions and especially in official documents.

Company Background

L-Soft specializes in the development of software and services for professional e-mail communication management. L-Soft pioneered the e-mail communication industry with its flagship product LISTSERV®. Introduced in 1986, LISTSERV® was the first and most

widely used software for e-mail list management. Since its foundation in 1994, L-Soft has expanded its portfolio of products and services to include e-mail delivery, outsourcing and consulting services.

With offices in the U.S. and Europe, the company serves more than 2,500 customers across the globe, including the Federal Trade Commission, AOL, Microsoft, MCI, Symantec, The New York Times, The Wall Street Journal, CNET, the New York State Department of Criminal Justice, The United States Senate and the United Nations.

Worldwide, public LISTSERV® servers send more than 30 million messages a day to over 100 million list subscriptions.

L-Soft's official policy on spam can be found at http://www.lsoft.com/spamorama.html. The first incarnation of the LISTSERV® software's spam filter was added in 1995, and has been continuously improved since then. L-Soft has hosted the SPAM-L Spam Prevention Discussion List since 1995.