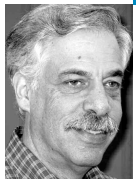
DANIEL L. APPELMAN

spam and blogs



PART 1: SPAM: A BALANCING ACT

Dan Appelman is legal counsel for the USENIX Association and practices technology law as a partner in the Silicon Valley office of Heller Ehrman LLP.

dan@hewm.com

THE EVER-INCREASING USE OF THE Internet creates new challenges for the system administrator. Many of these challenges have legal dimensions. This is particularly true of spam and blogs. By some estimates, over 75% of all email traffic is spam. In the United States and abroad, laws have been enacted to regulate spam with various remedies and varying success in encouraging compliance. Blogs are increasingly used not just for personal expression but also for commercial purposes. It often falls to the system administrator to design and enforce company policies to protect against spam, to limit personal use of blogs using company facilities, and to ensure that the company is in full compliance with all applicable laws and regulations.

This is the first of a two-part article based on a tutorial that I gave on spam and blogs at the LISA '06 conference in Washington, D.C., in December 2006. The second part, on blogs, will appear in a forthcoming issue.

Federal Inaction and the States' Responses

Spam is unsolicited commercial email. In the United States, Congress was reluctant to enact any legislation that would regulate spam even as its volume increased throughout the 1990s and the protests of the consumer lobby grew more and more audible. A reason why is obvious: The influence of the direct marketing lobby was stronger. Vendors discovered a unique tool for marketing to consumers, one that facilitates focused targeting to discrete market segments and is also ridiculously cheap per targeted recipient. They pressured Congress to do nothing that might increase the cost or impose compliance requirements on this new and very effective medium of communication.

The states were more receptive to the complaints of the consumer lobby. Federal inaction prompted a number of states to enact laws regulating spam. But these laws were inconsistent: They had different requirements and imposed different penalties from state to state. The lack of a uniform set of standards made compliance problematic, particularly for a medium such as the Internet that doesn't recognize state boundaries.

The California legislature enacted a new anti-spam law that was to be the toughest in the nation [1]. It would have become effective on January 1, 2004, and would have prohibited anyone from sending commercial email messages to any recipient who had not "opted-in" by giving his or her consent to receive spam from a particular sender in advance. Although the law could only be enforced in California, it would have had nationwide effect for all practical purposes. This is because spam campaigns can't usually tailor email messages to comply with the laws where each recipient happens to reside. Thus spammers would have had to comply with the most restrictive of the state laws in order to comply with them all—and that would have been California's. Sending spam only to recipients who had opted-in would have killed the direct marketing industry, because only a fraction of all possible recipients would ever be persuaded to opt in.

Congress Finally Acts

The direct marketing lobby found the California law to be intolerable. As a result, they changed their position on federal legislation and began to lobby Congress to pass a spam law that would supersede the very restrictive California law and that would also provide nationwide requirements. The result was the CAN-SPAM Act of 2003 [2].

CAN-SPAM regulates "commercial electronic mail messages" and not "transactional" or "relationship" messages. A commercial electronic mail message is one in which the primary purpose is the advertisement or promotion of a commercial product or service. CAN-SPAM requires that each commercial electronic mail message provide (i) a clear and conspicuous "opt-out" opportunity, (ii) a return email address for opt-outs that must work for at least thirty days after sending spam, (iii) a clear and conspicuous statement that the email is an advertisement or promotion, and (iv) a clear and conspicuous sender name and physical postal return address. It requires the sender to implement any opt-out request within ten days of receipt. It also prohibits false or misleading header or transmission information, subject lines, and content.

CAN-SPAM also contains special provisions for email messages containing sexually explicit material. The law requires senders to include a warning notice in the subject line and prohibits them from including sexually explicit material in the portion of the email that is immediately visible when opened.

Those initiating spam can be sued under CAN-SPAM if they don't fully comply with its requirements. The law also permits suit against companies providing services to spammers, such as those that assist advertisers with their campaigns for a fee. And companies whose products or services are promoted can also be sued if they (i) know or should have known about the noncompliance, (ii) benefit economically from the noncomplying spam campaigns, and (iii) do not attempt to prevent or report the noncompliance. ISPs cannot be sued under CAN-SPAM if their role is merely to transmit and they don't have a role or are not aware of the noncompliance.

CAN-SPAM gives standing to the following to enforce compliance: The Federal Trade Commission (FTC), certain other federal agencies, state Attorneys General, and ISPs. Unlike the California law, CAN-SPAM gives no private right of action. No noncompliant spammer can be sued for damages by any recipients. Recipients must convince one of the aforementioned entities to sue.

CAN-SPAM provides certain remedies in the event of a successful lawsuit. Money damages are available up to $250 per violation to a maximum of $2 million for nonwillful and $5 million for willful and knowing violation of the laws. Injunctive relief that will stop continued spamming is another permitted remedy. Those who violate the criminal provisions of the law can be sentenced to up to five years in prison. And the law provides for "bounty hunter" awards of up to 20% of the money damages assessed in a successful lawsuit.

Despite the availability of money damages, injunctions, and criminal penalties, CAN-SPAM is toothless compared to the California law and many of the other state laws that were passed before Congress finally acted. It allows spammers to send messages to everyone who doesn't opt out, rather than prohibit sending to anyone who hasn't opted in. It doesn't permit those most affected by receiving spam to sue the spammers for damages. And its compliance requirements are not all that difficult to meet. Furthermore, CAN-SPAM supersedes any state law, such as California's, that explicitly regulates commercial email messages. The only portions of the state laws that survive CAN-SPAM are those that prohibit falsity or deception in email messages or attachments.

Regulation of Spam by the FTC

Congress left the implementation of CAN-SPAM to the FTC and, in certain cases, other federal agencies. Congress gave the FTC authority to enact regulations under CAN-SPAM that have the force of law. Thus far, the FTC has developed rules further describing notice requirements for sexually explicit material [3] and establishing criteria for determining whether the primary purpose of an email message is commercial (in which case it is regulated) or transactional (in which case it isn't) [4]. It has also proposed but not finalized rules defining who is a "sender" and clarifying who has primary responsibility for responding to opt-out requests, shortening the deadline for honoring opt-out requests to three days, and prohibiting a sender from charging fees or requiring more information as prerequisites to honoring opt-out requests [5].

CAN-SPAM Compliance: Best Practices for the System Administrator

For the system administrator, there are two sides to the spamming issue: how to protect your system and its users from unwanted commercial email messages, and how to comply with CAN-SPAM if your employer uses email to market its products or services.

Of course you can (and should) maximize the protection of your system and its users against spam by installing the best filters and other anti-spam programs that become available. This is technological self-help. But you or your employer can also take legal action. Although CAN-SPAM doesn't permit spam recipients to sue spammers, you can notify your ISP, your state's Attorney General, or the FTC of any noncompliance and urge them to take action. CAN-SPAM does give these entities standing to sue violators.

The FTC uses its resources to investigate and prosecute the most egregious violators. But often it will not take action against those it views as marginal or not likely to serve as optimal test cases. ISPs are interested in providing good experiences for their customers, but they receive many complaints and have limited budgets for litigation. In my experience, clients often get best results by taking their complaints to their state's department of consumer protection or directly to the Attorney General.

My recommendation is to start by contacting the department of consumer protection in the state in which your company's computers reside. These departments will often have information you can use [6]. They can often be convinced to refer your complaint to the Attorney General, who can actually bring suit against the spammer. But you don't have to choose only one option. You can also inform your ISP and the FTC through their appropriate procedures. However, before you contact any of these agencies, be certain that the spam your system is receiving is actually violating the law, and get authorization from your employer to take the actions recommended here.

For those readers who work for companies that engage in commercial email campaigns, it is very important to comply with the law. Although compliance with CAN-SPAM is easier than with some of the state laws that it superseded, companies can still be fined, people can still be jailed, and employers can still suffer adverse publicity if they violate the law or any of the regulations that implement the law. It is therefore essential that system administrators have some familiarity with the law and those regulations and are able to work with their employers to ensure compliance.

The trend is for system administrators to participate with their employers in developing policy guidelines and templates that will ensure maximum compliance with the requirements of the law. At a minimum, companies should institute effective procedures for systematically implementing opt-out requests and for verifying compliance by its service providers. System administrators need to be aware of these procedures and should participate in their development and implementation. And system administrators should also clarify with their employers the scope of their responsibilities for monitoring and enforcing compliance.

REFERENCES

[1] The California law can be found at http://www.keytlaw.com/netlaw/caspamlaw.htm.

[2] CAN-SPAM stands for "Controlling the Assault of Non-Solicited Pornography and Marketing Act." A version of the CAN-SPAM Act can be found at http://uscode.house.gov/download/pls/15C103.txt.

[3] http://www.ftc.gov/os/2004/01/canspamfrn.pdf.

[4] http://www.ftc.gov/os/2005/01/050112canspamfrn.pdf.

[5] http://www.ftc.gov/os/2005/05/05canspamregformfrn.pdf.

[6] In California, for example, the agency is called the Department of Consumer Affairs, and it has a Web page specifically addressing what to do about spam: http://www.dca.ca.gov/ced/junkmailtips.htm.