

## Can We Legislate Spam?

Can we legislate spam? Declan McCullagh doesn't think so. In September 2003, Declan was ready to call it quits: "It's time for the tech community to realize that turning to the federal government for help in this area is simply not productive. It's like trying to teach a cow to configure BGP routers: You won't succeed, and you'll annoy the cow."<sup>1</sup>

I disagree. I prefer Dave Crocker's opinion: "Spam is a syndrome, not a disease. . . . I think that spam is a permanent condition. And so we need to look for multiple ways to control it, just as we need multiple ways to control cockroaches. We need good infrastructure, proper hygiene and good chemicals to deal with infestations."<sup>2</sup>

I think what Dave understands and what Declan forgot is that spam is not just a technology issue. It is a social issue, and

it threatens something very dear to most of us: the viability of e-mail. Campuses struggle to support solutions that will control the costs of filtering spam, keep "false positives" to a minimum, and not diminish their own marketing use of mass e-mails. The openness of the Internet, long touted as its greatest strength, also presents a threat—the problem of anything that is valued, free, and easily available. The only known cure for this problem, known as the "tragedy of the commons," is private ownership or government regulation. Clear and meaningful standards, rules of use, and methods of enforcement are required if the Internet is to retain its value. The technology community, on its own, can't save e-mail. In fact, "proper hygiene and good chemicals" could make the job of the technology community much easier.

Six years since being first introduced,

federal spam legislation was finally signed by President Bush on December 16, 2003. The CAN-SPAM Act will take effect on January 1, 2004. In general, Congress followed Dave's advice. It identified what it was after, set e-mail standards to help clean up the environment, and established rules of enforcement. But will the legislation work? Will Congress actually be able to control the "cockroaches" of the Internet?

### Separating the Good from the Bad

When an exterminator sprays for cockroaches, you don't expect the demise of the family cat. With a few exceptions, federal legislation uses three criteria to clearly differentiate spam from benign e-mail: intent, quantity, and existence of fraud. Congress agreed to the most basic definition of *spam*, referred to as a "commercial electronic mail message." Spam is "any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service (including content on an Internet website operated for a commercial purpose)." This does not include transactional or relationship messages, such as confirmation that something was ordered or that a flight is delayed. The key term in the definition is "commercial." Private, political, and non-profit e-mail speech remains protected. (This is the same concept that is being challenged in the "do-not-call" registry court cases.)

Quantity is also important. How many commercial e-mails can someone send before becoming a spammer? In California, the answer is one e-mail; in Virginia, the cut-off point is 10,000 e-mails in a 24-

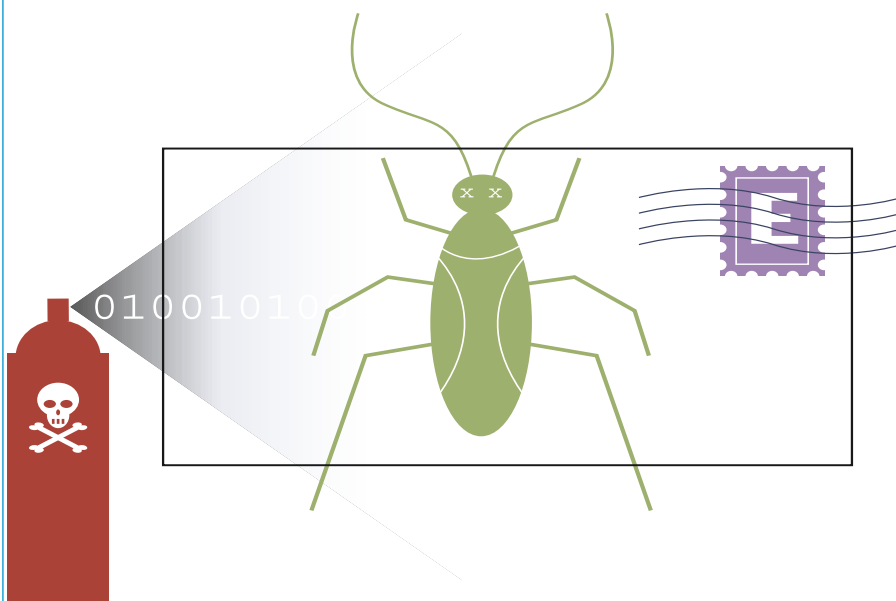


Illustration by Scott Roberts, © 2004

hour period or 100,000 e-mails in a 30-day period—and only if the message contains fraudulent information. Congress ended up with a more moderate definition, somewhere between the two extremes: more than 100 electronic mail messages during a 24-hour period, more than 1,000 in a 30-day period, or more than 10,000 during a one-year period.

For the most part, anti-spam advocates agree on what constitutes fraud. Fraud within the content of a commercial message is already well covered by law. But the standards for fraud in the subject and header of an electronic message were not clear. Remedying this gives law enforcement a new set of tools. The following “best practice” criteria developed by the Direct Marketing Association (<http://www.the-dma.org/>) and the Association for Interactive Marketing’s Council for Responsible E-mail (<http://www.imarketing.org/councils/CRE/>) served as a guideline in developing the new law:

1. The e-mail must contain an honest subject line that does not mislead readers about the content of the message.
2. The e-mail must not falsify the sender’s domain name or use a nonresponsive IP address or any other technological deception.
3. The e-mail must include the identity of the sender, including return address and/or physical address.
4. E-mail addresses must not be “harvested” with the intent to send e-mails without consumers’ knowledge or consent.
5. The e-mail must contain “ADV” or a similar label in the subject line.
6. The e-mail must contain an easily found, easily understood opt-out feature that works.

Opponents of this approach complain that it basically defines a legal way to spam. Proponents feel that law-abiding bulk e-mailers will be easy to control by market forces and technological measures without putting their civil liberties at risk.

### Right of Action, Enforcement, and Preemption of State Law

Once an e-mail is determined to be spam, who has the right to press charges? Does

federal law preempt existing state law? What are the penalties? Based on reports that 90 percent of spam is generated by less than two hundred individuals, there is optimism that heavy penalties and jail time for a few key players will be a strong deterrent. The California law (effective January 1, 2004) allows individuals to sue for up to \$1,000 per e-mail. But this approach faces serious criticism. By nature, spammers are difficult to track down and have few traceable assets. Experts believe that most citizens lack the will or the resources to pursue them. However, there *have* been several successful lawsuits brought by Internet Service Providers. Although it took four years, AOL won a \$7 million lawsuit against CN Productions Inc. in Virginia courts.<sup>3</sup> In only fourteen months, EarthLink was awarded \$16 million in an Atlanta court against a New York State man accused of using illegal means to send out 825 million e-mails.<sup>4</sup> Some of the most outspoken opponents to federal legislation have been attorney generals who fear that, after championing the passage of tough state laws, their efforts will be mute in the face of federal jurisdiction. The CAN-SPAM Act will allow for federal preemption except in the case of fraud or theft. Since, according to the FTC, two-thirds of spam involves fraud, it appears the states would retain significant power to prosecute.

Spam has traditionally been covered under civil, not criminal, law. Many spammers simply pay the fines, change their location, and continue to spam. As a result, there was pressure at the federal level either to significantly increase civil penalties or to make spamming a criminal offense. The CAN-SPAM bill originally allowed fines up to \$1.5 million and jail time up to one year. In order to win approval, the act added elements from the proposed Criminal Spam Act, which makes spamming a criminal offense and allows up to five years in prison. The result quelled the criticism that the CAN-SPAM Act would be too weak to make a difference.

### Patience, Persistence, and Cunning

In the same article in which Declan McCullough compared Congress to cows, he stated: “Washington’s torpidity has spurred state legislators into action.”<sup>5</sup> Is

that true? Or did state legislators react to their constituents ahead of Washington in a fairly normal process—one in which the states act as research activities for an eventual federal law? Even if the state laws have proven ineffective, they were a valuable test-bed for solutions that demand not only federal but international cooperation. Spammers move off-shore and ply their trade across national borders. Fortunately, the world community is just as frustrated and just as anxious to get spam under control as is the United States. Australia, Korea, Japan, the United Kingdom, and Italy have already passed anti-spam laws. A report issued in October 2003 by parliamentarians in London said it was “essential that co-ordinated global action be taken against spam.”<sup>6</sup> There has been increasing pressure on the United States, where a majority of the world’s spam originates, to adopt laws that satisfy not only all fifty U.S. states but the world community as well. This is a work in progress. The CAN-SPAM Act requires a report on progress within twenty-four months and includes provisions for changes based on the results. This is a serious diplomatic mission.

Can we legislate spam? Yes. But just like controlling cockroaches, legislating spam will require patience, persistence, and cunning.

### Notes

1. Declan McCullagh, “Spam Déjà Vu,” *CNET News.com*, September 2003, <[http://news.com.com/2102-1028\\_3-5083311.html](http://news.com.com/2102-1028_3-5083311.html)> (accessed November 30, 2003). McCullagh is the chief political correspondent for *CNET News.com*.
2. Quoted in Katharine Mieszkowski, “E-mail Is Broken,” *Salon.com*, October 2, 2003, <[http://archive.salon.com/tech/feature/2003/10/02/e\\_mail/](http://archive.salon.com/tech/feature/2003/10/02/e_mail/)> (accessed November 30, 2003). Crocker, a principal in Brandenburg Consulting, was part of the original Arpanet research community.
3. Todd R. Weiss, “AOL Wins \$7 Million Award in Antispam Case,” *Computerworld*, December 16, 2002, <<http://computerworld.com/governmenttopics/government/legalissues/story/0,10801,76821,00.html>> (accessed November 30, 2003).
4. Paul Roberts, “EarthLink Wins \$16 Million Settlement in Spam Case,” *MacCentral*, May 8, 2003, <<http://maccentral.macworld.com/news/2003/05/07/earthlink/>> (accessed November 30, 2003).
5. McCullagh, “Spam Déjà Vu.”
6. Bernhard Warner, “UK Lawmakers Call for International Anti-Spam Laws,” *Computer Cops*, October 8, 2003, <<http://www.computercops.us/article3502.html>> (accessed November 30, 2003).

Wendy Wigen is a policy analyst for EDUCAUSE.