



To print this page go to your File menu and select Print (or use Ctrl (Control) + P on your keyboard)

[< Return to Previous Page](#)

September 16, 2002

A Bounty on Spammers

By Lawrence Lessig

According to Merriam-Webster's dictionary, a vigilante is "a member of a volunteer committee organized to suppress and punish crime summarily (as when the processes of law appear inadequate)." He or she is "a self-appointed doer of justice."

The Internet has had a long history of digital vigilantism, the most common being spam vigilantes. These well-meaning souls fight to rid the Net of unsolicited commercial e-mail, sent mostly by direct marketers eager to get your attention, whether you want it or not, at work and at home. Such groups attempt to fight these intrusions by building lists of sites that don't obey "proper" e-mail etiquette and then by organizing automated boycotts of the sites on the list. If your company's e-mail server finds itself on one of these lists, then a significant number of your e-mails will be routed into a virtual black hole.

If California Congressman Howard Berman has his way, soon these spam vigilantes will be joined by a new rank of lawless law enforcers—copyright vigilantes. In July, Berman, a Democrat, introduced a bill to deputize the recording industry and other copyright holders to help fight copyright violations. Through his bill, these vigilantes would be granted immunity from liability as they deployed tools to hack peer-to-peer systems that they "reasonably believe" violate copyright laws. Run a Morpheus server with content that recording industry executives think is theirs, and you may find your machine doesn't run much content at all.

Citizen involvement in any war on crime is not necessarily a bad thing. There's a long tradition of people helping cops, especially where cops are hard to find or fund. But somehow, the Internet always seems to use vigilantism in the worst possible way. Berman's idea is an extreme example, but it shares important features with spam vigilantism as well.

Both forms depend ultimately upon code—the ones and zeros of digital nervous systems—doing the dirty work. The spam vigilantes first decide upon the spam policies they will require of e-mail servers across the Net. They then use tools to identify servers that violate their policies. Desperate e-mail administrators then subscribe to their list of policy-violating servers, and block e-mail from the servers on the list.

Once added to the list, there is no way to appeal the blocking or to fight such policies. Sometimes, the spam vigilantes offer people a way to appeal, but not always. Spews.org, for example, blocks without any appeal allowed. Its FAQ helpfully informs administrators who want to know "How...one contacts SPEWS?" Answer: "One does not. SPEWS does not receive e-mail—it's just an automated system and Web site."

Spam Vigilantes

Berman's bill is not much better. To its credit, the bill would require copyright owners to notify the U.S. Attorney General of the specific technologies it intends to use. But there is no obligation to notify the target of the attack before the attack begins. Once the attack occurs, the target would, under the bill, have the right to demand an explanation. (I never knew denial-of-service attacks came with return e-mail addresses.) The bill would also let targets complain to the Attorney General about wrongful attacks, though the Attorney General is not allowed to release the names of those behind the wrongful attacks (yet another secret list being kept by the U.S. Department of Justice).

No doubt, the motives of the spam vigilantes are pure. These are talented coders doing a public service. But there's also no doubt that the effect of their work is to make e-mail worse. They looked at the open and flexible system of e-mail that gave birth to much of the Net and decided that this system created too much freedom—at least for spammers. Their response was to find a mix of code and norms to restrict the freedom of e-mail. The result of their good intentions is a much less flexible e-mail system but not much less spam. Indeed, it's hard to believe that this conspiracy to cripple e-mail has done anything except make e-mailing more difficult.

But at least with the spam problem, there is a much simpler solution that, so far, Congress has failed to see. Imagine a law that had two parts—a labeling part and a bounty part. Part A says that any unsolicited commercial e-mail must include in its subject line the tag [ADV:]. Part B says that the first person to track down a spammer violating the labeling requirement will, upon providing proof to the Federal Trade Commission, be entitled to \$10,000 to be paid by the spammer.

The aim of Part A is to enable simple filtering. If all spam were tagged, then it would be extremely easy to choose whether to receive it or not. Spammers say there are lots of people out there who love to receive spam. Good for them. They can tell their Internet service provider or e-mail client to deliver all e-mail, regardless of the subject line. But those of us who actually work for a living can choose to ignore this class of junk on the Internet by filtering all e-mail with the subject line [ADV:].

The aim of Part B is to make Part A effective. The vast majority of proposals before lawmakers to regulate spam has made enforcement depend either upon an action by the state or by lawsuits filed by ISPs. This is not an accident; it is a product of effective lobbying by direct marketers and other commercial spammers. These people know that attorneys general and ISPs have better things to do than track them down. By making them the only enforcers, spammers know that any law aimed at stopping them will likely not be enforced.

But if the vigilantes who are working so hard to keep lists of offending e-mail servers were to turn their energy to identifying and tracking down spammers, then this passion to rid the world of spam might actually begin to pay off—both for the public and for the bounty hunters. If we deputized the tens of thousands of qualified people out there who are able to hunt offenders, then a large number of offenders would be identified and caught. Pretty soon the message to spammers will be delivered quite effectively: Label or pay.

Making Distinctions

No doubt it would be tough to draw a line between, say, "unsolicited commercial e-mail" and political e-mail. But we shouldn't exaggerate that problem. Go through the spam in your inbox and ask yourself whether there's any ambiguity about the spam you receive. Maybe it's just me, but my inbox is not filled with unsolicited political speech.

No doubt, too, it would be hard for the bounty hunter to actually discover who the spammer is. But this difficulty is also overblown. The one thing we know about the vast majority of spammers is that they are in business to make money. And the only way to get money from the sap who received the spam is to provide a simple way for the sap to link back to the spammer. If there's a way to buy something from the spammer, there's a way to charge the spammer if you catch him. And if enough of these spammers are charged, then the economics of dumping junk into inboxes will change enough to stop e-mail pollution.

Now sometimes, of course, the alleged spammer would be innocent. But that's exactly why we need people imposing punishments, not code. The difference between systems like SPEWS and systems like the one I'm proposing is that in the end, a person—not a machine—is in charge of deciding whether or not the law has been violated. Human judgment is required. With the Berman bill, and with automated black holes, no judgment is required before the harm is done, nor do the victims have any effective appeal. Scream all you want at a DOS attack or black hole; it will function just the same.

Removing human judgment is just what the copyright extremists want. It shouldn't be a part of the antispammer's campaign. The good souls who fight spam on the Net should embrace the rule of law over the reign of code, and then turn their coding efforts toward assuring this law actually rules.

Lawrence Lessig is a professor of law at Stanford Law School and the author of *The Future of Ideas: The Fate of the Commons in a Connected World* and *Code and Other Laws of Cyberspace*. His next column will appear in December.