

# NO LAUGHING MATTER

*Fight Spam by Using Law and Technology*

by TIM HEADLEY

**S**PAM, as in spiced pork and ham, is the registered trademark of Hormel Foods Corp. But any Internet regular will tell you that this product name has given way to another, far more onerous definition — unsolicited bulk e-mail.

In *Verizon Online Services Inc. v. Ratsky* (2002), the U.S. District Court for the Eastern District of Virginia noted that the term "spam" was given to unsolicited bulk e-mail after a sketch by the British comedy troupe Monty Python, where a group of Vikings chant "SPAM" in a cafe where the only breakfast item on the menu is Hormel's famous loaf. But

action, because many Internet service providers (ISPs) have been unable to stem the tide on their own. As the popularity of spam began to rise, ISPs began trying to counter spam by installing filters to block all e-mail messages that came from a certain domain name.

Unfortunately, savvy spammers got around filters by resorting to "forged spamming" and "domain-name hijacking." Forged spamming is transmitting spam using false, non-existent domain names. Hijacking occurs when large amounts of spam are relayed through an unsuspecting server, thus making the spam appear to originate from an approved, unfiltered server.

Forged spam can cause even bigger problems than ordinary spam. As employees come and go, e-mail addresses do, too. When a business' server gets a message to an out-

dated e-mail address, it kindly attempts to inform the e-mail sender that it no longer exists. (Although spammers don't care.) If the sender is a forged domain name, the server nevertheless keeps trying to get its message across, which can slow the whole system to a crawl. Delays of up to 12 hours and an inability to page key employees is not unusual.

Luckily, there are myriad Web sites where IT professionals can find programs to help combat spam.

- Declude ([www.declude.com](http://www.declude.com)) offers spam-fighting software products and free resources, such as a list of anti-spam databases; the colorful SamSpade ([www.samspade.org](http://www.samspade.org)) is full of technical tools useful in fighting spam.

- The Spamhaus ([www.spamhaus.org](http://www.spamhaus.org)) includes a

▶ *continued on page 26*

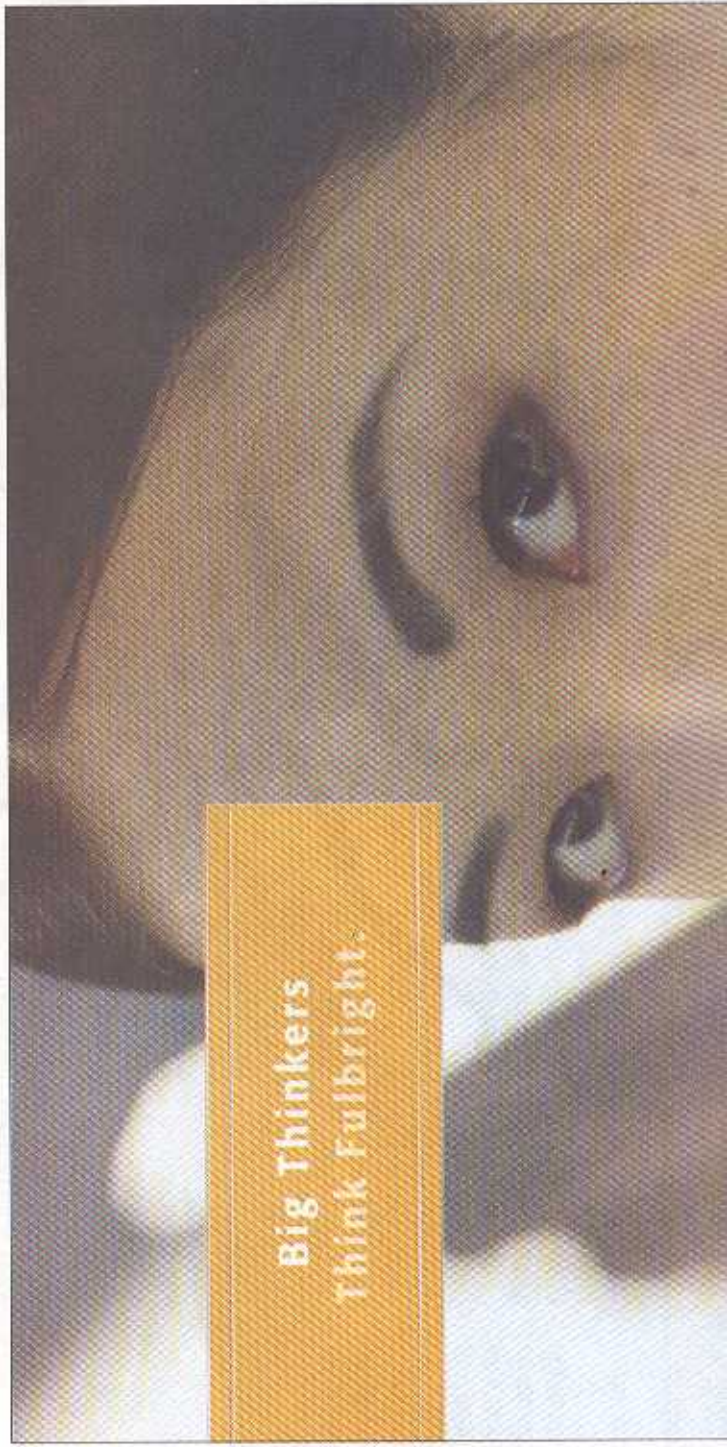


any business owner will tell you that there's nothing funny about spam.

Spam is more than just annoying. When multiple spam messages are sent to multiple e-mail addresses within one e-mail network, the whole system gets gummed up. Slowed e-mail service affects employee and business efficiency.

A business reeling from a barrage of e-mail doesn't have to sit back and take it. Businesses can arm themselves by becoming familiar with what spam is and isn't, who sends spam, and what legal remedies and technical resources are available to fight spam.

In fact, businesses *should* stand up and take



**Big Thinkers**  
Think Fulbright.

◀ continued from page 25

"Block List," which is a real-time database of addresses of verified spammers, spam gangs and spam services. The site also includes "ROKSO," a register of known spam operations that have been thrown off ISPs three times or more. As the site informs us, many of the ones who make this list of shame may be responsible for more than 90 percent of American and European spam.

To take aim against spammers in general, check out the SpamCon Foundation ([www.spamcon.org](http://www.spamcon.org)). This foundation was formed when some anti-spammers banded together to fight on their own and to encourage the passage of new laws; it bills itself as "a public benefit corporation that advocates for the mitigation of spam." The site serves as a forum for Internet users, administrators, marketers, anti-spam businesses and activists to collaborate and develop strategies that encourage responsible e-mail marketing.

### The Legal Arm

Although no federal or Texas statutes directly address

spam, there are some indirect statutory methods for fighting it. The Computer Fraud and Abuse Act, 18 U.S.C. §1030, makes it a crime, among other things, if anyone "knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer."

Section 1030(g) allows for civil actions by "any person who suffers damage or loss by reason of a violation of this section" to obtain "compensatory damages and injunctive relief or other equitable relief."

Arguably this statute could be used against spammers, because spammers overload the e-mail system and cause lost employee productivity. The Department of Justice, however, says the statute is not a slam-dunk. First, §1030(a)(5)(A)(i) requires proving that the spammer "intentionally causes damage," which may be difficult, and second, §1030(a)(5)(B)(i) requires showing that the spammer caused a minimum of \$5,000 harm.

To counter the first problem, businesses should consider having a standard form letter ready to send immediately

to the spammer stating that the spam is harming the system by slowing it down. To counter the second problem, businesses should consider tracking all time spent by their employees and consultants to combat spam.

The Texas Computer Crimes Statute, 7 Texas Penal Code §33.02, "Breach of Computer Security," that "[a] person commits an offense if the person knowingly accesses a computer, computer network, or computer system without the effective consent of the owner." Texas Civil Practice and Remedies Code §143.001 allows a person to file a civil cause of action for that crime. Arguably, a spammer "accesses" a business' computer network when it sends spam to that network, particularly if the business acts as its own ISP.

Three federal district courts — the Eastern District of Virginia in *America Online v. LCCM*, the Northern District of California in *Hotmail Corp. v. Van Money Pte Inc.* and the Southern District of Ohio in *CompuServe Inc. v. CyberPromotions Inc.* — have held that under certain circumstances, spam constitutes the tort of "trespass to chattel."

David Sorkin, a professor at the John Marshall Law School in Chicago, maintains a Web site ([www.spamlaws.com](http://www.spamlaws.com)) that tracks federal legislation against spam, state anti-spam statutes and international efforts. He lists 26 states as having anti-spam statutes.

As we wait for state and federal lawmakers to come up with constitutional ways to curb spam, spammers will keep on spamming. But creative technology managers and lawyers can protect themselves and will undoubtedly find new ways to put pressure on spammers on behalf of their clients. It would be a relief to get back to the days when spam was something to laugh about.

◀ ▶ ▶ ▶

*Tim Headley is a partner in the intellectual property section of Gardere Wynne Sewell in Houston. His practice includes litigation, patent prosecution, management of worldwide trademark programs and software licensing.*

