

Deliver Us From Evil Spammers

By Seth Cooper

Millions of Americans begin their work day clearing their inboxes of e-mail spam, the contents of which range from mildly annoying to frighteningly obscene. More of the same e-mail spam awaits millions of workers, schoolchildren, and families on their home computers. Advertisements for miracle weight-loss supplements, porn, Nigerian prince treasure schemes, more porn, fake lottery-winning notices, and sexual enhancement products max out e-mail inboxes and user patience.

E-mail spam is a continuing source of frustration and complaints about the Internet. It bogs down networks and slows down user connection speeds. Spam is also a tool of identity thieves and scammers, and makes for a handy dispenser of computer viruses.

To fight e-mail spam we have the CAN-SPAM Act, an ironically-named piece of legislation passed by Congress in 2003. It prohibits unsolicited commercial e-mail containing materially false heading information about the subject and sender of the message. Federal and state agencies, state attorneys general, and Internet Service Providers can take spammers to court. Violators of CAN-SPAM face civil fines or even jail. Many state anti-spam laws similarly empower state attorneys general or ISPs to go after spammers.

There have been some high profile prosecutions for illegal spamming. Robert Soloway, known as the "King of Spam," was successfully sued in 2005 by Microsoft for \$7.8 million and later in the same year by an Oklahoma ISP for over \$10 million.

Soloway was able to hide his assets and never paid the verdicts against him, and even mocked them. Bad idea. Federal prosecutors caught up with him and in March of 2008 he pled guilty to mail fraud and tax evasion. Soloway is now facing a possible 26 year prison sentence and over \$600,000 in fines.

In Virginia, Jeremy Jaynes earned the distinction of being the first spammer

convicted under state law. Once considered the world's eighth worst spammer, he is now serving a nine-year sentence. Prosecutors estimated that Jaynes may have earned as much as \$750,000 per month from his "work-at-home" spam schemes.

But despite some of these notable prosecutions, enforcement of anti-spam laws has been relatively light. The electron army of e-mail spam continues to charge ahead, seemingly unabated. The money is just too good.

BUT INCENTIVES ALSO exist for keeping spam out. ISPs continue to devise their own solutions to alleviate the Internet traffic spam jam through network management technologies and other practices. Competition among ISPs has driven much of this innovation. It is they, after all, who have the greatest economic incentive to ensure that their customers are able to send and receive specific e-mails, shielded from spam.

To the average person spam is spam. It is all unwanted, and the spam filters most ISPs use are programmed to block everything that the average person might consider spam. However, federal and (most) state anti-spam laws define spam in much narrower terms due in part to freedom of speech concerns. Certainly, fraudulent e-mails meant to deceive or rob unsuspecting internet users should be illegal. But the First Amendment protects legitimate solicitations from government censorship, however unwelcome they may be.

Keeping these same constitutional concerns in mind, can ISPs legally block everyday spam, or must they be limited to filtering only "official" or fraudulent spam? In 2005, e360Insight, an online marketing company that sends e-mail solicitations and ads to millions of e-mail users, sued Comcast for blocking its services. e360Insight claimed Comcast violated

federal and state computer and consumer laws, as well as the First Amendment.

In March of this year, the case of *e360Insight v. Comcast* was decided in an Illinois federal court. Citing the "Good Samaritan" provision of the federal Communications Decency Act, U.S. District Court Judge B. Zagel ruled against e360Insight.

The "Good Samaritan" provision protects ISPs from legal liability for good faith actions "to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected." Judge Zagel found no conflict between this provision and the narrow definition of e-mail spam found in federal law.

According to Judge Zagel, Congress decreed that "compliance with CAN-SPAM...does not evict the right of the provider to make its own good faith judgment to block mailings." ISPs need not confine their anti-spam detection and filtering operations to the e-mail defined and

prohibited by CAN-SPAM. Even mistaken ISP efforts to block e-mail spam are permissible when made in good faith. Moreover, Judge Zagel noted that the First Amendment only limits the powers of government to control speech.

Anti-spam laws are necessary, but the law's prohibition of certain commercial e-mail spam only addresses a part of the problem, and prosecutions are oriented more toward punishment than deterrence. Continued strategic and technological innovations by ISPs for detecting and filtering spam are crucial to curbing the volume of unwanted e-mail that courses through the internet if we don't want e-mail spam to reach biblical plague proportions.

Fortunately, Congress and the court got it right in conferring the law's blessings upon these Good Samaritans of spam fighting.

Seth Cooper is the Director of the Telecommunications and Information Technology Task Force at the American Legislative Exchange Council in Washington, D.C. -- the nation's largest nonpartisan, individual membership organization of state legislators.