Vanderbilt Journal of Entertainment & Technology Law

Volume 2
Issue 1 *Winter 2000*

Article 9

2000

How to Can Spam

Gary Miller
United States Congress

how to can spam

By Congressman Gary Miller

Receiving unsolicited commercial e-mail, also known as "Spam," is like receiving junk mail, postage due. Spam shifts the cost of advertising from the advertiser to the consumer. This imposes enormous costs on Internet Service Providers (ISPs) and their customers. The Spam problem cries out for a legislative solution, and that is why I introduced H.R. 2162, the "Can Spam Act."[1]

The source of the Spam moniker for unsolicited commercial e-mail is apparently attributed to an annoying song in a Monty Python skit. In the skit, actors dressed like Vikings sing the word "Spam" over and over again, becoming louder and louder throughout the skit, until none of the players can hear each other. Finally, the singing Vikings drown everything out and the skit ends. Unsolicited commercial e-mail is also annoying background noise that is growing louder. The concern is that Spam will finally drown out legitimate e-mail on the Internet.

Businesses have increasingly resorted to unsolicited electronic mail to send advertising and promotional materials because they are able to reach millions of Internet users at virtually no cost. Consumers report receiving dozens of unsolicited advertisements every week.[2] The problem is becoming so pervasive that Internet Service

Providers (ISPs) now hire full-time employees to screen Spam because their systems cannot handle the volume.[3] Additionally, ISPs must buy extra bandwidth so that Spam does not cause their systems to crash.[4] ISPs pass along those costs to their customers. Also, the individual consumer has the additional costs of sorting through the mail, using computer space for the mail, and paying for download time to receive the unwanted mail.

The fundamental incentives for unsolicited commercial e-mail are skewed. Spammers are encouraged to compile an enormous e-mail list because sending one message costs the same as sending a million. As a result, individuals and businesses are forced to pay for advertising they do not want.

I personally became involved in this issue when a constituent of mine had to shut down his business for a few days because he was inundated with Spam that crashed his computer system. He was understandably irate. Someone had used his Internet domain name as the false return address for an undesirable e-mail advertisement. As a result, he received almost half a million angry responses. Not only did the Spam damage his equipment and close his business, but there are now a million disgruntled consumers who hate my constituent and his business because they think he sent the message. The Spam was both a trespass onto his private computer property as well as a fraudulent use of his business name.

I am not a technology expert, but I do understand the concept of private property and trespassing. Spam is trespass.[5] In most cases, Spammers violate the policies of Internet Service Providers and cause them monetary harm through trespassing. Since Spammers are currently able to shift their advertising costs onto the recipient, there is a market incentive for Spammers to trespass. In order to craft sound legislation to fix this market incentive, I turned to the Central Hudson test for government regulation of commercial speech,[6] existing "junk fax" law,[7] and the Ninth Circuit's ruling on that law in Destination Ventures v. FCC.[8]

In 1980, the U.S. Supreme Court created the Central Hudson test to determine when the government may regulate commercial speech without violating the First Amendment.[9] Commercial speech that is otherwise legal may be regulated if: the government asserts a substantial interest in support of its regulation, the government demonstrates that its restriction on commercial speech directly and materially advances that interest, and the regulation is narrowly drawn.[10] Existing law regarding unsolicited commercial faxes builds on the Central Hudson test.[11]

Existing law regarding junk faxes is simple: if a fax is commercial and unsolicited, you cannot send it without obtaining permission from the recipient. In Destination Ventures, Ltd. v. FCC, the Ninth Circuit held that the government has a substantial interest in preventing the shift of advertising costs from sender to recipient.[12] The cost for faxes consists of the paper and toner used as well as missed faxes from phone lines being tied up.[13] The court concluded that the interest in preventing cost-shifting was legitimately advanced by a total ban on all fax advertisements.[14] Commercial electronic mail shifts advertising costs to the recipient in the same way that commercial faxes shift costs. In fact, there is potentially more recipient cost associated with e-mail than with faxes. Computer users have the costs of additional connect time charges to download unsolicited commercial e-mail, additional toll or 800 number charges for some users, and lost productivity due to wasted time filtering and deleting messages and submitting complaints. Internet Service Providers have the costs of additional bandwidth to deal with high-volume traffic, additional computers necessary to protect ISP integrity from theft of service and other inappropriate usage of ISP resources, additional storage for bulk messages, engineering staff resources to implement and maintain filtering capabilities, and system administration staff resources to deal with problems caused by bulk e-mail traffic or retaliation from frustrated recipients. My approach to controlling unsolicited commercial e-mail is less restrictive than current law for faxes. Instead of outlawing unsolicited commercial e-mail altogether, my approach gives Internet Service Providers tools to control their own property. They own the computer servers, so they can decide whether they want to bear the cost of commercial e-mail or not.

H.R. 2162, the "Can Spam Act," gives Internet Service Providers the power to control Spam by giving them a civil cause of action to recover damages of $50 per Spam, capped at $25,000 per day, for unsolicited commercial electronic messages to and from their system.[15] This keeps the government out of regulating the Internet and lets the ISPs and the market decide how to control Spam. If the ISP conspicuously posts a policy prohibiting or limiting Spam on its web-

page, or through their Simple Mail Transfer Protocol (SMTP) banner, it can use the law to protect its property and customers. ISPs have any option the market supports including: 1) banning Spam completely, 2) allowing all Spam, 3) coming to an agreement with an advertiser that the advertiser will pay a few cents per message to send it to the ISP's customers, or 4) setting up a system with e-stamps where their system will accept any messages with enough postage to make it worth their while. I am sure there are future technologies that will create more options. The crux of the issue is that advertisers must be forced to pay for their advertisements and Internet Service Providers must ensure that their customers are satisfied.

The "Can Spam Act" also has a related, but separate, provision to deal with the fraud rampant in unsolicited commercial e-mail. As in the case of my constituent, many Spammers use someone else's e-mail address as the return address so they do not have to deal with the angry replies or the return e-mail messages from inactive e-mail addresses. This is the equivalent of dumping your trash into someone else's yard, and it harms the names and reputations of others.

There are existing laws regarding fraud and trademark infringement, which the Federal Trade Commission (FTC) currently uses against Spammers,[16] but I added a provision to the "Can Spam Act" to clarify the crime of computer fraud through Spam.[17] The "Can Spam Act" would make it illegal to knowingly and without permission steal someone else's domain name.[18] The penalties would be a fine for first offense (up to $5,000) and a fine plus less than one year in prison for second offense (up to $100,000 depending on jail time).[19]

This legislation hinges on the concept that advertisers should not shift the cost of their advertising to the recipients. However, there are additional basic principles that should guide any e-mail legislation. A few months ago I handed a list to all the Members of the House Commerce Telecommunications, Trade and Consumer Protection Subcommittee during a hearing on unsolicited commercial e-mail. It outlined the guiding principles for any Spam legislation:

1. Cannot Legitimize Spam

Currently Internet Service Providers (ISPs) can sue Spammers for trespass.[20] While it is very expensive and time consuming to bring these suits, courts have recognized the property rights of ISPs.[21] Anything that allows someone free Spam before making it illegal, or in any other way recognizes Spam, would be taking away existing private property rights of ISPs and would be a step backward.

2. Cannot Regulate the Internet

The Internet is an ever-changing medium, relatively free of government regulation. That is why it works so well, is growing so quickly, and is driving our economy. We need to jealously guard the freedom of the Internet and keep the government out of it.

3. Must Protect Free Speech and Pass Constitutional Muster

The Supreme Court has outlined very specific levels of protection of speech from political,[22] religious,[23] commercial[24] to obscene.[25] These standards are already in case law. The Ninth Circuit has ruled that laws can be passed to curb commercial speech that transfers costs onto the recipient.[26] Outside of correcting cost-shifting in commercial speech, any law that regulates specific speech content may fail a judicial challenge.

4. Cannot Create a New Cost or Tax on the Internet

Most plans to stop Spam would end up costing Internet Service Providers or the government money.

5. Must Guard the Privacy of the Individual

Information is a powerful tool for law-abiding citizens and for those who break the law. Any solution to Spam cannot put personal information, including e-mail addresses, in the public domain, which would put privacy at risk.

6. Cannot Hurt Internet Service Providers

The Internet is a completely new communication tool. Unlike faxes or phones, which are person-to-person communication devices, e-mail is routed through numerous private computers and Internet Service Providers before it reaches its destination. As a result, any legislative solution to Spam must not hamstring the numerous Internet Service Providers that make up the Internet. Anything that would force ISPs to be a party to numerous lawsuits, or would force them to keep special regulated lists, would hurt the entire Internet system. A solution that harms ISPs is worse than the problem.

7. Must Work

Any solution must be usable for those who have the

ability and the desire to stop Spam. The "Can Spam Act" fits within these six guidelines. Yet there are many other issues related to unsolicited commercial e-mail legislation that have been brought up to my office over the last three years.

Some may wonder why the legislation covers only commercial speech, but not political or all unsolicited speech. One easy answer is that politicians who decide to Spam voters will probably be immediately voted out of office. But the real reason we do not address political speech is because we want to make sure this law stands up to any court challenge. By staying within the narrow guidelines of the Central Hudson[27] test, existing junk fax law,[28] and Destination Ventures v. FCC,[29] we are trying to stay on the safest legal ground possible. I am an Internet minimalist, and I want to make sure that the market incentive of Spam is corrected without creating a burden on the Internet.

Others have suggested that we regulate only bulk e-mail, since it is volume that harms the Internet. Even though it is the bulk characteristic of Spam that harms the Internet, the concept of shifting costs through each individual Spam message is the philosophical problem. I strongly believe that each unsolicited commercial e-mail message violates the property rights of the recipient, and I believe my position is consistent with existing law and legal precedent.

Direct marketers and some state and federal legislators have advocated what is called an "opt-out" solution to the Spam problem. Opt-out means that when users receive unsolicited commercial e-mail, they are responsible for notifying the sender to stop sending them messages. Legally, opt-out is a step backwards because it accepts the first Spam message as legal, thereby granting the Spammer an extraordinary legal right to the ISP's computer in the first instance. Practically, opt-out does not make sense because the worst Spammers would just change their business name each time they Spam, sell the e-mail address to their unscrupulous partners, claim they did not receive the user's request to be removed from the list, or any number of other maneuvers. Once we have granted a Spammer one free bite at the apple, we are better off with no law at all.

I have received letters and calls from people asking why e-mail filters or just hitting the delete key cannot take care of the Spam problem. I would prefer that technology and personal actions take care of this problem, but Spam is a problem of cost and scale that technology has not been able to solve. E-mail filters do block some Spam, but the cost has already been incurred by the time the Spam is filtered by the end user. A Spam that is filtered has already used bandwidth, has already passed through the ISP's staff and filters, and has already used the end user's hook-up time and computer space. Moreover, filters and hitting the delete key are not solutions that scale. By "scale" I mean that if a Spammer has fifty percent of its advertisements blocked, then it will just send out twice as many Spam messages without increasing its costs to attain the same number of successful hits. When filters block commercial content, Spam volume only increases and overall costs rise. Internet Service Providers need a new legal tool to protect their property and their customers because technology will not solve this problem.

Another concern is existing state law regarding unsolicited commercial e-mail. Many states are considering legislation to limit Spam, and a few states, including my home state of California, already have laws governing Spam. When I was a member of the California State Legislature, I authored the Spam law in California,[30] which is almost identical to the act I introduced in Congress. Even when I was working two years ago to pass the state legislation, I knew there needed to be a national solution. First of all, it is difficult for an ISP to indicate that its property is in a certain state. This causes difficulty when it comes to making sure the notice, or "no trespassing" sign, is posted without creating an undue burden on Spammers, lest a judge throw the lawsuit out. With a national law, there would be no need to demonstrate which state the computer equipment is in, making it easier for the Spammer to know they are violating a law. Also, it does not make sense to burden commerce over the Internet with 50 different state regulatory systems. E-mail has not realized its commercial potential because of the stigma created by abusers of commercial e-mail. We do not want to hurt e-mail further by creating 50 different complicated legal structures.

But a national law is not foolproof. Because the nature of the Internet is global, an American law governing Spam would not be enforceable against someone Spamming from outside the United States. The only exception would be a Spammer outside the country who has assets in the United States. Those assets could be seized to pay for a judgment granted by a U.S. court. At this point, a federal solution would be the best, but even-

tually Internet users would benefit from an international framework to stop cost-shifting on the Internet.

If the "Can Spam Act" becomes law,[31] Internet Service Providers will have a powerful new tool to stop unsolicited commercial e-mail. The property rights of computer owners and Internet Service Providers will be clearly stated in law, and it will no longer make financial sense for advertisers to send indiscriminately to huge e-mail lists. E-mail will be much more usable as a method of commerce because people will only receive e-mail messages they request, and they can complain to their ISP if that is not the case.

Once advertisers are forced to obtain permission before they send advertisements through an Internet Service Provider's system, the options are limitless. From opt-in – whereby the customer requests advertisements for products they are interested in – to future technology that allows for e-stamps, technology and the market will bring about creative uses for e-mail that we have not yet contemplated.

In sum, no one should be required to subsidize someone else's advertisements. After all, speech is only free if you do not force someone else to pay for it. ◆

---

1 See H.R. 2162, 106th Cong. (1999).

2 See Anne E. Hawley, *Taking Spam Out of Your Cyberspace Diet: Common Law Applied to Bulk Unsolicited Advertising Via Electronic Mail*, 66 UMCK L.REV. 381, 381-82 (1997).

3 See Internet Service Providers' Consortium (ISP/C), *Unsolicited Commercial Email Position Paper* (visited Feb. 9, 2000) <http://www.euro.ispc.org/policy/papers/spam.shtml>.

4 See generally Eric J. Sinrod & Barak D. Jolish, *Controlling Chaos: The Emerging Law of Privacy and Speech in Cyberspace*, 1999 STAN. TECH. L. REV. 1 (1999).

5 See America Online, Inc. v. LCGM, Inc., 46 F.Supp.2d 444, 451 (E.D. Va. 1998) (holding that the transmission of unsolicited bulk e-mails can constitute a trespass to chattels); CompuServe, Inc. v. Cyber Promotions, Inc., 962 F.Supp. 1015 (S.D. Ohio 1997) (holding that an online service provider had established a cause of action for trespass to chattels against a company that had repeatedly sent the online service provider's subscribers mass quantities of unsolicited e-mail); see also Hawley, *supra* note 2 at 392 (stating "The doctrine of trespass to chattels presents a valid cause of action against spamming").

6 See Central Hudson Gas & Electric Corp. v. Public Service Commission of New York, 447 U.S. 557 (1980).

7 See 47 U.S.C. § 227 (1994).

8 See Destination Ventures Ltd. v. FCC, 46 F.3d 54 (9th Cir. 1995).

9 See Central Hudson, 447 U.S. at 563-64, 566.

10 See id. at 566.

11 See Destination Ventures, 46 F.3d at 55-56.

12 See id. at 56.

13 See id.

14 See id.

15 See H.R. 2162.

16 See Lanham Act, 15 U.S.C. § 1125 (a)(1) (1994); see also America Online, Inc. v. LCGM, Inc., 46 F.Supp.2d at 449 (stating that "[t]he unauthorized sending of bulk e-mails has been held to constitute a violation of...section [1125(a)(1)] of the Lanham Act").

17 See H.R. 2162.

18 See id.

19 See id.

20 See America Online, Inc. v. LCGM, Inc., 46 F.Supp.2d at 451; CompuServe, Inc. v. Cyber Promotions, Inc., 962 F.Supp. 1015 (S.D. Ohio 1997).

21 See id.

22 See Cohen v. California, 403 U.S. 15 (1971); Brandenburg v. Ohio, 395 U.S. 444 (1969).

23 See Church of the Lukumi Babalu Aye v. City of Hialeah, 508 U.S. 520 (1993); Oregon v. Smith, 494 U.S. 872 (1990).

24 See Central Hudson, 447 U.S. at 566; see also 44 Liquormart, Inc. v. Rhode Island, 517 U.S. 484 (1996).

25 See Miller v. California, 413 U.S. 15 (1973); Paris Adult Theatre I v. Slaton, 413 U.S. 49 (1973).

26 See Destination Ventures, 46 F.3d at 55-56.

27 See Central Hudson 447 at 566.

28 See 47 U.S.C. § 227 (1994).

29 See Destination Ventures, 46 F.3d at 55-56.

30 See CAL. BUSINESS AND PROFESSIONAL CODE § 17511.1 (West 2000).

31 The Act is currently before the House Subcommittee on Telecommunications, Trade, and Consumer Protection. 1999 Bill Tracking H.R. 2162.