Summer 2000


Credence E. Fogo

Follow this and additional works at: https://repository.jmls.edu/jitpl
Part of the Computer Law Commons, Internet Law Commons, Privacy Law Commons, and the Science and Technology Law Commons

Recommended Citation

https://repository.jmls.edu/jitpl/vol18/iss4/2

This Article is brought to you for free and open access by The John Marshall Institutional Repository. It has been accepted for inclusion in The John Marshall Journal of Information Technology & Privacy Law by an authorized administrator of The John Marshall Institutional Repository.
THE POSTMAN ALWAYS RINGS 4,000 TIMES: NEW APPROACHES TO CURB SPAM

by Credence E. Fogo†

I. INTRODUCTION

Before 1994, the average Internet user received little unsolicited commercial email ("UCE"), or "spam." Before large Internet Service Providers ("ISPs") offered flat-rate pricing and the World-Wide Web experienced phenomenal growth, the Internet was still mostly the province of university students and the computer literati: it was not a mass medium particularly attractive to advertisers. But that all changed in April 1994, when enterprising Arizona lawyers Laurence Canter and Martha Siegel sent UCE advertising their immigration law "services" to approximately 8,000 Usenet newsgroups. The ad reached approximately 20 million people, inspiring irate Usenet users to flame Canter and Siegel in such great volume that the attorneys’ ISP’s computer crashed. The computer overloads Canter and Siegel’s stunt caused also completely knocked out New Zealand’s Internet access. The couple remained undeterred by the flames, telephone harassment, and death threats they received after their first foray into direct marketing. After Canter and Siegel spammed the Internet again in 1995, their ISP terminated their


1. The pair was offering to fill out "green card" lottery applications for $95/person, a task that does not require a lawyer’s assistance. See also Peter H. Lewis, Unrepentant Lawyers Hit by Internet Mobs After Incident, Austin American-Statesman, May 30, 1994, at C3 available in 1994 WL 3943016.


Following in Canter and Siegel's footsteps, countless direct marketers have taken the lawyers' technique to a new level and sent their ads to thousands of individual email accounts at a time. Because this marketing technique is easier and far less costly to the advertisers than an equivalent number of direct mail solicitations, email accounts worldwide have been deluged with "make money fast" scams, pyramid schemes, and dubious chain letters. The burden millions of daily spams place on the worldwide computer network has the potential to bring down the Internet one node at a time.

A campaign against mass UCE is taking place in Congress, the courts, and state legislatures. As of October 2000, Congress is considering five anti-spam bills; thirty-three states have introduced or passed anti-spam legislation. In addition, an increasing number of ISPs have filed suit against spammers who have taken advantage of their networks. The Federal Trade Commission has even taken steps to prevent the consumer fraud spammers all too often perpetrate.

This article will analyze the spam problem under First Amendment "commercial speech" jurisprudence, including lawsuits that senders of junk faxes filed (unsuccessfully) challenging the legal restrictions that form the most sensible template for an effective anti-spam law. Part II will explore the social and technological context in which the spam problem developed, and will discuss the true financial costs of the practice. Part III will describe ISPs' and state governments' unsuccessful attempts to restrict the most destructive aspects of spamming. Part IV analyzes the First Amendment protections of spam as "commercial speech" and examines five federal proposals to curtail spam, concentrating on their legality and likely effectiveness. The article concludes that two solutions—amending the junk fax law to cover Internet solicitations, or a bill currently in Congress that provides civil and criminal penalties for engaging in some of the most egregious spamming practices—will be
the most effective and the least vulnerable to First Amendment challenges. It also suggests an alternative, model bill that would bring together the best of the current proposals before Congress and close their loopholes.

II. SPAM

A. DEFINITION

"Spam" is any unsolicited email message sent in large quantities, usually to a large number of recipients, often using forged headers to avoid bounce-backs from bad addresses and angry replies ("flames") from unwilling recipients. It need not be commercial: many netizens consider chain letters, solicitations from advocacy groups, and political ads sent in this manner to be spam.

The term also describes such messages sent to Usenet newsgroups, when the topic of the newsgroup is unrelated to the product or service the spammer is hawking. However, this article will not address the regulation of Usenet spam, such as Canter and Siegel's, because such regulation would have a significantly chilling effect on free speech. Undoubtedly, Usenet spam is destructive, annoying, and obnoxious. The havoc spam has wrought upon Usenet should not be underestimated. It is not uncommon to find some Usenet noncommercial discussion groups overwhelmingly full of spam; often the original topic of conversation, as in the Monty Python skit, the original topic of conversation is completely drowned out. "Spam wastes so much time and makes real messages so hard to find," one commentator notes, "that it can destroy the usefulness of online forums."

Nevertheless, regulation of Usenet spam would create more of a First Amendment problem than regulation of email spam for three reasons. First, insofar as the government might regulate UCE to protect users' privacy interest in their email accounts, the rationale does not translate to Usenet. Second, the government's interest in protecting Net users involved in e-commerce from business losses caused by system slowdowns is inapplicable to Usenet. Finally, the pressure Usenet spams place on system processors is, despite the havoc Canter and Siegel

10. See, e.g., Rebecca Fairley Raney, New Issue for Political Campaigns: The Spam Question, N.Y. TIMES, June 7, 1998 (describing advocacy groups' and politicians' uses of spam during 1998 campaign season); Coalition Against Unsolicited Commercial Email, About the Problem (visited Mar. 28, 2000) <http://www.cauce.org/problem.html> (detailing characteristics of "the most commonly seen UCEs.").


wrought, less intense than with email spams, because a spam that goes into Usenet only hits hundreds or a few thousand newsgroups, as opposed to email spam, which can hit many thousands (or millions) of email accounts and generate thousands of bad address bounce-backs, which clog up ISPs' central processors. Consequently, unless otherwise indicated this article will use the term “spam” to denote commercial messages sent to individual email addresses.

The use of the term “spam” to denote UCE is derived from a Monty Python sketch in which a couple attempts to order breakfast at a diner that serves nothing but SPAM.13 The link between Monty Python's beleaguered diners and email users is that, as in the sketch, inappropriate, unwanted, and exceedingly numerous spam messages can overwhelm wanted communiqués: legitimate email can become impossible to separate from the spam.14 A less well-known etymology has it that “spam” stands for “send phenomenal amounts of mail.”15

B. Scope of the Problem

Many spammers argue that their messages are just like the junk mail everybody receives in the physical world. People who aren't interested in passing on a chain letter, making money fast, or having sex with

13. Monty Python’s Flying Circus: The Spam Sketch (BBC television broadcast, Dec. 15, 1970). When the wife attempts to order her breakfast without SPAM, she is drowned out by a horde of Vikings singing the meat product’s praises:

Man: Well, what've you got?
Waitress: Well, there's egg and bacon; egg, sausage, and bacon; egg and SPAM; egg, bacon, and SPAM; egg, bacon, sausage, and SPAM; SPAM, bacon, sausage, and SPAM; SPAM, egg, SPAM, SPAM, bacon, and SPAM; SPAM, sausage, SPAM, SPAM, bacon, SPAM, tomato, and SPAM.
Vikings (starting to chant): SPAM, SPAM, SPAM, SPAM . . . .
Waitress: . . . . SPAM, SPAM, SPAM, egg, and SPAM; SPAM, SPAM, SPAM, SPAM, SPAM, SPAM, SPAM, SPAM, baked beans, SPAM, SPAM, SPAM . . . .
Vikings (singing): SPAM! Lovely SPAM! Lovely SPAM!
Waitress: . . . or Lobster Thermidor au Crevettes with a mornay sauce served in a Provençal manner with shallots and aubergines garnished with truffle pâté, brandy, and with a fried egg on top, and SPAM.
Wife: Have you got anything without SPAM?
Waitress: Well, there's SPAM, egg, sausage, and SPAM; that's not got much SPAM in it.
Wife: I don't want ANY SPAM!

Id.

14. See, e.g., Testimony of Ray Everett-Church before the Senate Communications Subcommittee (visited Aug. 12, 2000) <www.senate.gov/~commerce/hearings/0617eve.pdf> (describing inconvenience of “wading through dozens of unsolicited advertising messages” in order to find legitimate email). Everett-Church was testifying on behalf of the Coalition Against Unsolicited Commercial Email (which he co-founded), as well as the Forum for Responsible and Ethical Email. Id.

NEW APPROACHES TO CURB SPAM

2000

a virtual girlfriend should simply perform the electronic equivalent of throwing away a Publisher's Clearinghouse circular, and hit the delete key.\textsuperscript{16} Unfortunately, such a "solution" is deceptively simple and only diverts attention from the true costs of spam, which are both more expensive and widespread than direct marketers care to admit. In reality, spam has wrought incredible costs on Internet users, threatening the medium's financial and technical integrity. In terms of wasted person-hours, spam's cumulative costs are incalculable. One conservative estimate places the cost at more than $87 million per year.\textsuperscript{17} Aside from the aggregate amount of time wasted skimming and disposing of spam, ISPs' employees spend many additional hours resolving consumer complaints about spam emanating (or appearing to emanate) from their domains and attempting to track down the culprits. Of course, because spammers routinely forge their headers, many complaints fielded by an ISP's staff regard spam that originates from a completely different source. However, the cost in staff time does not end with customer service: any calculation of the true costs of spam must also take into account the not-insignificant expense of fixing servers that crash under the weight of thousands of pieces of junk mail and losses suffered by businesses that lose orders or other valuable communications due to such outages.\textsuperscript{19}

In addition to financial and technical damage, the onslaught of virtual come-ons has done what some view as irreparable harm to the social fabric of the Internet. These costs are, of course, not as easily quantified as the economic damage. Many longtime netizens (in Internet time, that's about ten years) believe that the proliferation of spam during the past several years has irreparably damaged the character of the online community\textsuperscript{20} by changing the atmosphere from Bughouse Square\textsuperscript{21} to


\textsuperscript{17} See Quarterman, supra note 12.

\textsuperscript{18} As spammers become more sophisticated, they have begun to mark their messages with deliberately innocuous subject lines designed to fool the recipient (and mail filters) into opening and reading the message, rather than disposing of it unread. See also Allan Hoffman, \textit{Digging Out From an Avalanche of Spam}, Star-Ledger (Newark, NJ), Sept. 11, 2000, at 061, available in 2000 WL 26254638.


\textsuperscript{20} See Quarterman, supra note 12.

\textsuperscript{21} Bughouse Square is a "town square" in Chicago where speakers hold forth on political and social topics during summertime lunch hours.
that of a carnival.

III. BACKGROUND: EARLY LEGAL RESPONSES TO SPAM

The most compelling argument in favor of federal regulation of spam is that, as with telesolicitations and junk faxes during the 1980s, no other measure has worked.

A. PRIVATE ISP SUITS

Initially, netizens attempted self-help through four methods. The first was vigilantism: This method included mailbombing, harassment, and imposition of the Usenet death penalty. The second, third, and fourth methods were more civilized: individuals complained, programmers raced to develop technical blocks, and ISPs terminated spammers' accounts.

Quickly it became clear that self-help would not work. ISPs and other victims of spam turned to the courts. They deployed a dizzying variety of statutory and common law legal theories. The first major category of such claims argued that spammers' practice of forging headers and displaying ISPs' logos and names at the Web sites to which hyperlinks in the spam led violated ISPs' intellectual property rights in their names, trademarks, and copyrights. Such lawsuits generally claim

22. See Jeff Bounds, Spamming Battles Lead to Nasty Fights, Litigation, DALLAS BUS. J., Dec. 12, 1997, at 1C.


24. See Shirley Duglin Kennedy, Updates on Use and Abuse of the Net, INFORMATION TECHNOLOGY, Apr. 1, 1998, at 46. See also Ken Lucke, Usenet Death Penalty FAQ (last modified Jan. 11, 2000) <http://www.stopspam.org/usenet/faqs/udp.html>. The "Usenet death penalty" is a sanction imposed by an unofficial group of systems administrators who "take it upon [themselves] to block or cancel every message posed to Usenet from a site [sic] whose administration is deemed to be "soft" on the issue of spamming by its users." Id.


that an ISP’s trademark or copyright is violated when spammers forge the service’s name onto an email header. These types of claims have also been made in cases in which the spam included a hyperlink (usually to a pornographic site) upon which the ISP’s name and/or logo appeared without its consent. These legal theories have found favor with the courts; relief, however, is only available to those ISPs with the resources to hire intellectual property attorneys.

The second major category of claims alleges violations of state and federal laws that ban fraudulent and abusive computer practices.27 These charges generally stem from actual physical damage that voluminous amounts of spam can cause to overwhelmed servers. They are often augmented by common law nuisance, trespass, and conversion claims.28


27. See, e.g., complaint filed for America Online v. Over the Air (visited Sept. 30, 2000) <http://www.ljx.com/LJXfiles/aol/aolsuit.htm> (violation of Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (1994); hereinafter “Over the Air Complaint”); Prime Data Complaint, supra note 26, at Counts 1, IV (same, as well as violation of Virginia Computer Crimes Act, Va. CODE ANN. §18.2-152.1); Bigfoot Complaint, supra note 26, at paras. 66-73 (violation of Electronic Communications Privacy Act, 18 U.S.C. § 2701-11 (1994)); Cyber Promotions Complaint, supra note 26 (Computer Fraud and Abuse Act); Concentric Complaint, supra note 26, (Electronic Communications Privacy Act and Computer Fraud and Abuse Act); Strong Complaint, supra note 26 (Computer Fraud and Abuse Act); Typhoon Complaint, supra note 26 (Electronic Communications Privacy Act).

28. See, e.g., Over the Air Complaint, supra note 27 (conversion and trespass to chattels); Prime Data Complaint, supra note 26 (conversion, trespass to chattels, and conspiracy to commit trespass and conversion); Bigfoot Complaint, supra note 26 (trespass to chattels, conversion); Cyber Promotions Complaint, supra note 26 (trespass); Concentric Complaint, supra note 26 (trespass and conversion); Complaint filed for Expert Pages v. Lawinfo.com (last modified May 31, 2000) <http://expertpages.com/anti-webpiracy/filing1.htm> (trespass); Parker v. C.N. Enterprises - Petition (last modified June 9, 1997) <http://www.jmls.edu/cyber/cases/flowers1.html> (nuisance, trespass, and conversion);
Finally, ISP plaintiffs have asserted a smattering of more novel legal theories, which have met with less success. These include libel, unjust enrichment, breach of implied covenant, interference with contract, fraud, negligence, the tort of publicity, false light, outrageousness, and the federal law against sending junk faxes.

Despite the huge amount of time, effort, and money ISPs have poured into defending their equipment and customers, it has become clear that scattershot private suits by ISPs have not worked. There are two major reasons why these private suits have failed. First, ISP enforcement is, by and large, limited to those ISPs who are large enough to afford to pursue such claims (which, as America Online's experience has shown, is an incessant task). Although the largest ISPs have such resources, they cannot file such suits unless their own servers or trademarks are violated. If the spam overloads their customers' email accounts through different servers, America Online's customers—who are injured because their email accounts are filled with junk, and because the Internet as a whole is slower and less reliable—are out of luck. Second, the spammers are, as always, a step ahead of the anti-spam ISPs and are attempting to circumvent litigation by building their own Internet backbone; the company will "pay other networks to carry its junk email." Even if such a plan never comes to fruition, spammers

Matthew Seidl, Verified Complaint (last modified May 5, 1998) <http://www.cs.colorado.edu/~seidl/lawsuit/complaint.html> (trespass to chattels); Strong Complaint, supra note 23 (trespass to chattels); Typhoon Complaint, supra note 30 (trespass to chattels); Web Systems Corp. v. Cyber Promotions (last modified June 10, 1997) <http://www.jmls.edu/cyber/cases/websys1.html> (nuisance, nuisance per se, trespass, and conversion).

29. See Bigfoot Complaint, supra note 26; Typhoon Complaint, supra note 23.
30. See Bigfoot Complaint, supra note 26; Concentric Complaint, supra note 26; Juno Complaint, supra note 26; Typhoon Complaint, supra note 26.
32. Id.
34. See Seidl, supra note 25 (negligence, negligence per se, and negligent hiring).
35. See id.
36. See id.
37. See id.
38. See id.; Strong Complaint, supra note 26.
39. An example would be if America Online's users were spammed, but not in such great numbers that AOL's servers crashed or otherwise suffered damage. In the absence of an intellectual property or some common law violation, neither AOL nor the spam recipient could take legal action.
can continue to jump from ISP to ISP or, as “Spam King” Sanford Wallace formerly did, rent bandwidth from a willing ISP.42

B. STATE LAWS

Due in part to the futility of the dozens of private suits that had been filed against spammers, some states have begun to pass laws attempting to limit the practice. As of October, 2000, thirty-three states have considered anti-spam legislation. Seventeen — Nevada, Washington, California, Illinois, Maryland, Virginia, Delaware, Iowa, and West Virginia, Louisiana, Missouri, North Carolina, Oklahoma, Pennsylvania, Rhode Island, and Tennessee—had actually passed laws: none prohibit spam outright.43

The Nevada law was a disappointment to anti-spam advocates. Although the original version of the bill would have prohibited outright the practice of sending UCE,44 the law as eventually passed requires only that the email include the sender’s address, as well as removal instructions.45 Consequently, the law will not prevent the most harmful aspect of spam: the outrageous quantities of untargeted emails that have caused so many system overloads. Furthermore, since the businesses that spam change constantly, the law, which immunizes the spammer’s ISP, will do little to reduce the traffic snarls that prompted the push for regulation in the first place. The law is not merely under inclusive, it is too narrowly tailored to accomplish anything.

Similarly, the bill passed in Washington originally would have banned spam altogether.46 As passed, the law forbids commercial emailers from putting false or misleading information in the subject line of the message, using a third party’s domain name without permission, or otherwise forging headers.47 Enforcement is by the Attorney General or private action;48 furthermore, the law specifically authorizes ISPs to block incoming or outgoing spams.49 Critics argue that spammers will

42. See Kornblum, supra note 16.
43. In sixteen states—Alaska, Colorado, Connecticut, Hawaii, Idaho, Kentucky, Maine, Massachusetts, Minnesota, Nebraska, New Hampshire, New Jersey, New York, Oregon, Texas, Vermont, and Wisconsin—anti-spam bills (or provisions within more general bills) either were defeated or are still under consideration.
47. See id.
easily evade the law by signing up for throwaway accounts and that spam will continue unabated. However, this criticism fails to consider that spammers remain accountable under the law—if not to their ISPs—whether they use a throwaway account or not.

Washington's law was strengthened in 1999 to forbid spammers from using false domain names or false or misleading subject lines and to require spammers to include identifying information in the body of the message. Furthermore, the legislature authorized the Attorney General to create an electronic registry of email addresses that spammers may search to determine whether his or her targets are protected by the new law. The new law also prohibits violations of ISPs' terms of service and provides a private right of action for violations to both ISPs and their customers.

Like Washington, California has passed two laws to restrict spam. The first, Assembly Bill 1676, is not stringent: it merely requires spammers to include opt-out instructions in the body of the spam, and the warnings “ADV” or “ADV:ADULT” in the subject line. The law only applies when both the recipient and the ISP conveying the spam are located in California. The second law is more comprehensive. Although it does not ban spamming, as the original version of the bill would have, it creates a private right of action for ISPs whose terms of service are violated by spammers. In addition, it criminalizes using a false domain name to send messages, if use of the name causes damage to a computer system. The law provides no relief for individual recipients of spam, who must continue to proceed under common law theories against spammers who have injured them.

50. Throwaway accounts are email accounts that the spammer intends to use one time only (for a spam), thus avoiding personal accountability with his or her usual ISP. See Peter Lewis, '98 Review - Preview '99, Seattle Times, Dec. 27, 1998, at C1, available in 1998 WL 24470928
52. See H. 1037, 56th Leg., 1999 Reg. Sess. (Wash. 1999), at §§ 2,3.
53. See id.
55. See id.
56. See A. 1676, 1998 Sess. (Cal. 1998), at § 1. See also Pa. SB 262 (A.1) (Banning UCEs containing "explicit sexual materials" without including "ADV-ADULT" in subject line); see also Tenn. Code Ann. § 47-18-2501 (requiring "ADV" in subject line, as well as return address information, a ban on the distribution of spamming software, and the institution of a private right of action).
57. See id. at § 1(d).
The Illinois law, titled the "Electronic Mail Act," prohibits spammers from falsifying their messages' point of origin or using false or misleading information in the subject line.\(^{59}\) It only applies to spams involving recipients or computer equipment located in Illinois.\(^{60}\) Unlike in California, in Illinois Internet users have a private right of action, as do ISPs.\(^{61}\) In addition, ISPs may block spam.\(^{62}\) The Act also adds falsifying routing information in connection with transmitting spam to the state's criminal offense of computer tampering.\(^{63}\) Iowa's law is similar, except that it relies on private lawsuits and the attorney general's civil enforcement powers, rather than criminal sanction.\(^{64}\)

The Maryland law is far more lenient than the other states: it does not prohibit or regulate spamming outright. It instead criminalizes the misuse of email with intent to harass, or the sending of "lewd, lascivious, or obscene material."\(^{65}\) The law does not apply to political speech.\(^{66}\) Because of its exclusive focus on content, the Maryland law appears much more vulnerable to a First Amendment challenge than do the other laws which states have passed, particularly given the Supreme Court's decision in \textit{ACLU v. Reno},\(^{67}\) which invalidated regulation of "indecent" speech on the Internet. Maryland's proscription of "lewd [or] lascivious" content is as vague as the invalidated sections of the federal Communications Decency Act were.\(^{68}\) Despite the less searching scrutiny the Court gives to restrictions on commercial speech, it seems unlikely that Maryland could show a substantial interest sufficient to uphold the regulation.\(^{69}\) From the point of view of ISPs and spam recipients, even if the law were constitutional, it would be unhelpful in the extreme, because it does nothing to prevent or punish the system overloads, clogged mailboxes, and other problems that UCE creates.

Virginia recently amended its computer trespass law to include falsifying or forging routing information, as well as distributing software


\(^{60}\) \textit{See id.}

\(^{61}\) \textit{See id.}

\(^{62}\) \textit{See id.} \textit{See also} No. Rev. Stat. § 207.1300 et seq. (2000) (Similarly requiring valid return address information, immunizing ISPs, and providing for $1,000 damage award in private civil actions).

\(^{63}\) \textit{See} 815 Ill. Comp. Stat. 511/10 at § 16D-3.


\(^{65}\) \textit{See} 27 Md. Code Ann. §§ 555C(1)(B), (C).

\(^{66}\) \textit{See id.}


with the primary purpose of falsifying or forging routing information.\textsuperscript{70} It permits ISPs to block spam\textsuperscript{71} and provides a private right of action for both ISPs and their customers.\textsuperscript{72}

Delaware's law, which does not provide Internet users with a private right of action, is still relatively tough on spammers. It provides that a person is guilty of “the computer crime of unrequested or unauthorized electronic mail,” a misdemeanor, when he or she intentionally or recklessly spams, falsifies headers, or distributes software with the primary purpose of falsifying or forging routing information.\textsuperscript{73}

Finally, West Virginia prohibits fraudulent or deceptive bulk email, or unauthorized email that falsifies headers, contains sexually explicit materials, or contains false or misleading information in the subject line.\textsuperscript{74} It immunizes ISPs from liability for terminating service to spammers and prohibits the sale or possession of spamming software that falsifies headers.\textsuperscript{75} It provides a private right of action to spam recipients, with nominal damages of $1,000 per spam, and authorizes punitive damages for the “willful failure to cease initiating” spam.\textsuperscript{76}

While these laws are a step in the right direction, their loopholes may doom them to failure. Even laws that provide private rights of action may not be enforceable in practice: few users are likely to pursue a court remedy against a difficult-to-trace spammer, given that statutory damages run from only $10-$1,000 and often do not provide for attorney fee awards.\textsuperscript{77} More importantly, because of the interstate nature of the Internet, state-by-state regulation of spammers’ marketing practices raises dormant commerce clause issues, which could invalidate all of the regulations. One trial court in Washington State has already come to this conclusion, holding that the statute is “unduly restrictive and burdensome and places a burden on businesses that outweighs its benefits to consumers” in a case that the state attorney general brought against an Oregon spammer who sent between 100,000 and 1 million UCEs a

\begin{footnotesize}
\begin{itemize}
\item[70.] See VA. CODE ANN. § 18.2-152.4(A)(7), (B) (2000). See also N.C. Gen. Stat. § 14-458(a) (similarly, but without software ban) and § 1-539.2A (authorizing private right of action); Okla. Stat. tit. 15 § 776.1 (similarly); R.I. Gen. Laws § 11-52-4.1 and 11-52-5-6 (amending computer trespass law, includes criminal penalties and private right of action).
\item[71.] See § 18.2-152.4(D).
\item[72.] See § 18.2-152.12(B), (C).
\item[73.] House Substitute for H.B. 242, 140th Gen. Assembly, 1999 Reg. Sess. (Del. 1999), § 1. See also La. Rev. Stat. Ann. § 73.6 (similar, except defines spam only as commercial bulk UCE distributed in violation of ISP policy; provides for $5,000 criminal fine).
\item[76.] § 46A-6G-5.
\item[77.] See e.g., Idaho Code § 48-603E94)(2000) ($1000 damages); 720 ILCS 5/16D-3(b)(4) (Illinois $10); R.I. Gen. Laws § 11-52-6 ($500).
\end{itemize}
\end{footnotesize}
week.\textsuperscript{78} Although the ruling will likely be appealed, every one of the state anti-spam laws (except possibly California's) is vulnerable to similar constitutional challenges. Furthermore, even if the appellate courts uphold state anti-spam laws against commerce clause and federal and state free speech challenges, the fact remains that regulating spam state-by-state is inefficient. This is true both from the point of view of consumers, whose rights and remedies now vary widely, and of online businesses, who have an interest in consistent regulation. Consequently, a federal solution is preferable than the current patchwork of contested state regulations.

Thus far, the legal odyssey of spam has followed in the footsteps of the junk fax. Junk faxing was once a costly obstruction to businesses' use of their fax machines. States began to pass laws against the practice.\textsuperscript{79} This did not work, because states did not have jurisdiction over interstate calls.\textsuperscript{80} It took passage of a federal law, the Telephone Consumer Privacy Act (TCPA), to cut off the junk fax problem.\textsuperscript{81} While a federal solution conceivably would still allow junk emailers to move their operations abroad, such a result is unlikely; most spammers operate from small or micro-businesses that do not have the resources to relocate. Furthermore, international mail order is complex and costly, a line of business likely to be unattractive to marketers who turned to spamming in the first place because it is easy and cheap.\textsuperscript{82}

\begin{itemize}
\item \textsuperscript{79} See Michael M. Parker, \textit{Fax Pas: Stopping the Junk Fax Mail Bandwagon}, \textit{71 Or. L. Rev.} 457, 462 (1992).
\item \textsuperscript{80} See Southern Pacific Co. v. Arizona, 325 U.S. 761, 770-71 (1945). In fact, state regulation of interstate calls might have withstood a dormant Commerce Clause challenge: the state would only have been required to show that the regulation was rationally related to a legitimate state end, and that the burden on interstate commerce was outweighed by the state interest. \textit{Id. See also S. Rep. No. 102-178, at 4 (1992), reprinted in 1991 U.S.C.C.A.N. 1966, 1968. However, the legislative history to the Telephone Consumer Privacy Act does not seriously engage the issue; it simply asserts that states do not have jurisdiction over interstate calls. Id.}
\item \textsuperscript{82} But see Robert Raisch, \textit{Postage Due Marketing, Revisited, Part II} (last modified Dec. 11, 1997) <http://www.internautics.com/article960917.htm> (suggesting Internet access provider-enforced "community standard" to stem tide of overseas spam).
\end{itemize}
IV. CONSTITUTIONAL ISSUES: SPAM IS NOT PROTECTED SPEECH

Before analyzing the various legislative proposals before Congress, it is necessary to analyze the constitutional status of spam. Spammers claim that the First Amendment protects their activities—and even that private ISPs are required to carry their missives. As we shall see, spammers' current practices are not protected by the First Amendment.

A. LEGAL BACKGROUND: COMMERCIAL SPEECH JURISPRUDENCE AND THE JUNK FAX LAW

Commercial speech does enjoy First Amendment protection, although it is unclear how “local ordinance” maps onto cyberspace in the presence of competing norms. Of course, advertising that is false or misleading is not protected by the Constitution. Commercial speech is also subject to greater constraints than “core” political speech; in particular, the government has greater latitude to impose time, place, or manner restrictions on advertising than on advocacy. The landmark case of Virginia Board of Pharmacy, decided in 1976, stands for the principle that consumers enjoy a First Amendment right to receive commercial speech. The restrictive rules of third party standing might make it difficult, however, for spammers to assert such a claim.

Virginia Board of Pharmacy’s broad protection of commercial speech was limited less than five years later in the case of Central Hudson Gas

---

84. See, e.g., Moser v. Frohnmayer, 845 P.2d 1284 (Or. 1993) (Article I, § 8 of state constitution violated by state junk fax law). Spammers may be protected by state constitutions, some of which provide more stringent protections. Id.
86. Anne Wells Branscomb, Anonymity, Autonomy, and Accountability, Challenges to the First Amendment in Cyberspace, 104 YALE L.J. 1639, 1647 (1995).
87. Virginia Pharmacy Board, 425 U.S. at 771 (“[U]ntruthful speech, commercial or otherwise, has never been protected for its own sake.”).
88. See id. at 771 (“[W]e have often approved restrictions of that kind.”).
89. See id. at 747.
90. See, e.g., Craig v. Boren, 429 U.S. 190 (1976) (allowing third-party standing where failure to let third party proceed would adversely affect her rights); Carey v. Population Services Int’l., 431 U.S. 678 (1977) (allowing third-party standing where third and primary parties had a unity of interest and there was a substantial obstacle to primary party exercising own rights). Although Virginia Board of Pharmacy was brought as a third party claim, in general it is quite difficult to assert third-party standing. Id. The Supreme Court generally requires, at minimum, that the third-party plaintiff show unity of interest with a directly affected party, as well as some substantial obstacle to that party exercising his or her own rights. In the case of spam, it would be difficult for a spammer to argue it has the requisite unity of interest with consumers, as so many have taken action to prevent spam from invading their email accounts.
v. Public Service Commission,\textsuperscript{91} which promulgated a four-part test to determine whether state regulation of commercial speech violates the First Amendment. The test inquires:

1) Is the speech protected?\textsuperscript{92} In other words, is it misleading\textsuperscript{93} or proposing an illegal transaction?\textsuperscript{94} If so, the speech can be banned completely. Although the nature of a great deal of UCE clearly fails this test, a speech category consisting only of spam would likely also contain truthful claims. Not all spam is of the “make money fast” variety. The fact that many spams advertise unwanted products or services does not make them illegal or misleading. Because that is the case, spam does enjoy some First Amendment protection and thus may be regulated only in accord with the other three parts of the Central Hudson test.

2) Does the government have a “substantial” interest to support the regulation?\textsuperscript{95} In the case of spam, there are at least four such interests: reducing the system overloads that are a demonstrably crushing burden on network capacity, preventing spammers from misappropriating others’ servers and identities, preventing consumer fraud, and reducing the heavy cost burden that spam shifts from the advertiser to the listener. Cost shifting alone, of course, does not justify regulation when the burden is minimal and publicly borne,\textsuperscript{96} such as the cost of paying government to remove litter caused by advertising handbills. However, in the case of spam, the cost burden is so crushing at both the individual and system levels\textsuperscript{97} that courts should find that it is one properly shouldered by the advertiser.\textsuperscript{98} The clutter spam creates is analogous to a situation in which handbill litter blocks use of the sidewalk and intersection for hours or days at a time: this is not \textit{de minimis} and certainly should be regulable.

3) Does the regulation directly advance the governmental interest?\textsuperscript{99} As we shall see, some proposed legislative solutions directly advance the interests asserted; others do not.

4) Is the regulation no more restrictive than necessary to achieve the desired end?\textsuperscript{100} With respect to several of the bills being considered by Congress, the regulations would not be extensive enough to solve the

\textsuperscript{92} See id. at 563-64.
\textsuperscript{93} See Friedman v. Rogers, 440 U.S. 1 (1979).
\textsuperscript{95} Central Hudson, 447 U.S. at 564.
\textsuperscript{96} See Schneider v. State, 308 U.S. 147 (1939).
\textsuperscript{97} See supra notes 15–24 and accompanying text.
\textsuperscript{98} Cf. Destination Ventures v. Federal Communications Commission, 46 F.3d 54, 57 (9th Cir. 1995).
\textsuperscript{99} See Central Hudson, 447 U.S. at 564.
\textsuperscript{100} See id.
problems spam causes. Furthermore, the Court has interpreted the “no more restrictive than necessary” prong of the text to indicate a scrutiny somewhat less searching than that under the “narrow tailoring” analysis used for some regulations involving noncommercial speech.\textsuperscript{101}

Completely banning spam may be within the government’s authority. Consistent access to the Internet is crucial to the viability of an increasing sector of the U.S. economy. The aggregate costs of spam are threatening the continued viability of the net as a reliable communications medium. Despite the fact that the Court’s most recent commercial speech decision in \textit{44 Liquormart v. Rhode Island}\textsuperscript{102} subjected regulations of commercial speech to greater scrutiny, that decision expressly addressed regulations covering advertisements that were not false, misleading, illegal, or aggressive:\textsuperscript{103} spam often displays all of these attributes at once. Furthermore, that case involved a total ban on truthful information contained in advertisements of liquor prices.\textsuperscript{104} The interest served by such a regulation, temperance,\textsuperscript{105} received much less deference by the Court than should an anti-spam regulation, which protects both privacy and property. Even if a ban covered commercial speech that was not false, misleading, or illegal, prohibiting the practice of sending hundreds of thousands of unsolicited commercial messages, at a huge expense to the recipients and countless third parties with a highly detrimental effect that threatens the survival of a medium that has become increasingly necessary to the smooth functioning of commerce, would serve an important governmental interest. The only real constitutional question with respect to anti-spam regulations is whether these regulations are written narrowly enough to satisfy the \textit{Central Hudson} test.

\textbf{B. Legal Antecedents: The ‘Junk Fax’ Problem}

The Internet is not, of course, the first new medium that shady and intrusive “entrepreneurs” have attempted to hijack in pursuit of a quick buck. The best analogy to spam is not telesolicitation, broadcast ads, or direct paper mail: it is the junk fax. Like an email account, a fax machine does not require human interaction or attention to oversee the receipt of a message. Like unwanted email, unwanted faxes can be quickly trashed. Like email technology, fax machines can be easily configured to send the same message to a great number of recipients simultaneously with very little effort by the sender.\textsuperscript{106} And fax machine owners, like

\begin{itemize}
\item 101. Board of Trustees of SUNY v. Fox, 492 U.S. 469 (1989).
\item 103. See \textit{id.} at 501 (Stevens, J., concurring).
\item 104. See \textit{id.} at 489.
\item 105. See \textit{id.} at 493.
\item 106. There are also dissimilarities. For example, unlike fax recipients, email users receive the spam at little cost to themselves. The aggregate costs, however, appear to be
email users, had a huge problem with unsolicited commercial messages that threatened the viability of the fax as a communications medium, until the Telephone Consumer Protection Act (TCPA) banned the practice of junk faxing.\textsuperscript{107}

The TCPA provides that "it shall be unlawful for any person within the United States to use any telephone facsimile machine, computer, or other device to send an unsolicited advertisement to a telephone facsimile machine."\textsuperscript{108} The law permits the Federal Communications Commission to exempt noncommercial speakers from a provision of the law banning recorded telemarketing calls,\textsuperscript{109} but not from the junk fax provision. Aggrieved recipients have a private right of action for an injunction and damages of up to $500 from the junk faxer.\textsuperscript{110} The law permits the creation of a national database of individuals who do not want to receive calls from telemarketers.\textsuperscript{111} Finally, the law requires all faxes to bear a mark of origin.\textsuperscript{112}

It did not take long for telemarketers and junk faxers to challenge the new law as violative of the First Amendment. In two cases, the Ninth Circuit held against the plaintiff telemarketers and junk faxes. The first case,\textsuperscript{113} Moser v. Federal Communications Commission, involved the TCPA's ban on automated calls. The U.S. District Court for the District of Oregon had held for the telemarketers; the Ninth Circuit reversed. Noting that the federal law was required because existing state laws were incapable of regulating interstate calls (an issue that is germane to the analysis of state laws regulating spam),\textsuperscript{114} the court found that the TCPA did not distinguish between commercial and non-commercial calls.\textsuperscript{115} Thus, it concluded, the law should be analyzed as a


\textsuperscript{109} See § 227(b)(2)(B)(I).

\textsuperscript{110} See § 227(b)(3).

\textsuperscript{111} See § 227(c)(3).

\textsuperscript{112} See § 227(d)(2).

\textsuperscript{113} See Moser v. Federal Communications Commission, 46 F.3d 970 (9th Cir. 1995).

\textsuperscript{114} See id. at 972. The court noted that the state laws had also faced constitutional challenges; Oregon's law was struck down on state constitutional grounds in Moser v. Frohmayer, 845 P.2d 1284 (Or. 1993). Id.

\textsuperscript{115} See Moser, 46 F. 3d at 973. Language permitting the FCC to exempt non-commercial callers from its regulations, the court held, was "permissive . . . [i]t in no way requires the FCC to adopt such exemptions." Id. at 972. This rather convoluted reasoning is unpersuasive; the legislative findings the court cites just a few paragraphs earlier make it manifestly clear that the TCPA is not content-neutral. Id.
"content-neutral time, place, and manner restriction" rather than under Central Hudson, but the tests are "essentially identical."116 Under that analysis, the restriction must be independently justifiable, narrowly tailored, and leave open "ample alternative channels" of communication.117 The TCPA's alleged under inclusiveness118 did not rise to the level of a First Amendment violation because it was not viewpoint-based and because the government was not required to completely eradicate the problem.119 With respect to the "ample alternative channels" requirement, the court held that such means did exist—just as a ban on spam would leave open voluntary mailings, advertisements in appropriate newsgroups, and many forms of Web-based advertising. As the court noted, "That more people may be more easily and cheaply reached . . . is not enough to call forth constitutional protection for what those charged with public welfare reasonably think is a nuisance when easy means of publicity are open."121

The reasoning in Moser provides strong support for the proposition that regulation of spam is constitutional. Congressional findings on the problems created by telephone solicitation are reasonably similar to those created by spam. Furthermore, regulation seeking to curb some of the most intrusive and obnoxious aspects of UCE—forged headers preventing the target from replying, the dissemination of thousands of messages at a time to every recipient at a particular domain, and preventing other traffic from using the server for hours at a time—should satisfy the courts as narrowly tailored enough to address the substantial government interests in protecting privacy and keeping the Internet up and running. However, the "prerecorded call" analogy does not track perfectly onto spam, as UCE does not invade personal privacy as directly as telesolicitation. On the other hand, UCE imposes direct financial costs onto consumers that telesolicitations do not, primarily the cost of access time, at least for users whose ISPs charge by the hour.122

A closer, though imperfect, analogy is found in the junk fax portion of the TCPA, which the Ninth Circuit upheld in Destination Ventures v. Federal Communications Commission.123 As noted above, the TCPA re-

---

116. See id. at 973.
118. See id. Plaintiff argued under inclusivity because, it said, pre-recorded telephone calls constituted only 3 percent of telesolicitations. Id.
119. See id. at 974 (citing City of Ladue v. Gilleo, 512 U.S. 43, 49–50 (1994)).
120. See id. at 975.
121. Id. (quoting Kovacs v. Cooper, 336 U.S. 77, 88-89 (1949)).
122. See supra notes 15–24 and accompanying text. UCE also imposes substantial indirect financial and other costs on consumers. Id.
123. See Destination Ventures v. Federal Communications Commission, 46 F.3d 54 (9th Cir. 1993).
requires faxes to bear a “return address,” the phone number from which they are sent. It also prohibits the practice of sending unsolicited ads to a fax machine.\textsuperscript{124} Unlike in \textit{Moser}, in \textit{Destination Ventures} the court focused on the government’s interest in “prevent[ing] the shifting of advertising costs.”\textsuperscript{125} Also unlike \textit{Moser}, the court analyzed the challenged provision under the commercial speech regime of \textit{Central Hudson}, which requires that the regulation “directly advance a substantial government interest in a manner that forms a ‘reasonable fit’ with the interest.”\textsuperscript{126} In \textit{Destination Ventures}, the plaintiff challenged the provision on the grounds that it was not a “reasonable fit,” since other forms of unsolicited faxes are also costly to consumers.\textsuperscript{127} Reasoning that advertising caused the bulk of cost shifting, and that mere under inclusiveness would not defeat the law,\textsuperscript{128} the court held in the government’s favor.

The best argument against directly applying a junk fax analysis to the spam problem invokes time and scale as significant differences between spams and junk faxes: it takes a consumer no time at all to receive a spam (whereas, the \textit{Destination Ventures} court noted, it takes 30-45 seconds to receive a fax), the recipient’s email account is not prevented from receiving other email during the spam transmission, and the cost of receiving a spam is minimal compared to the two and one-half cents per page the \textit{Destination Ventures} court found a recipient paid to receive each fax. Although such distinctions are valid, they are shortsighted, because they do not take into account the indirect costs borne by the ISPs in equipment burdens, server failure, and staff time. Nor does it consider the burden UCE imposes on users in the form of costs passed on by ISPs, wasted time, and, for commercial users, business lost due to system crashes or slowed response times. Because the interests involved in staunching the incessant flow of spam so closely track those that justified the regulation of telephone solicitation and junk faxes, regulation of spam on the TCPA model should be upheld by the courts.

Although amending the TCPA is probably the simplest solution to the spam problem given the law’s already proven efficacy and constitutionality, the only bill that proposed to do so died in the 104th Con-

\begin{thebibliography}{128}
\bibitem{124} See supra notes 77 and 81 and accompanying text.
\bibitem{125} See \textit{Destination Ventures}, 46 F.3d at 56.
\bibitem{126} \textit{Id.} at 55 (citing \textit{Central Hudson Gas and Electric Corp. v. Public Service Commn.}, 447 U.S. 557, 566 (1980)). This formulation of the \textit{Central Hudson} test is a slight variant on the original, which requires not that the regulation “form a ‘reasonable fit’” with the asserted governmental interest, but that it be “no more restrictive than necessary” to advance the interest. The difference is probably not material, since the Court has interpreted “no more restrictive than necessary” to require more deference to government than, for example, a narrow tailoring requirement. \textit{Id.} See also supra note 70 and accompanying text.
\bibitem{127} \textit{Destination Ventures}, 46 F.3d at 56.
\bibitem{128} See \textit{id.}
\end{thebibliography}
The bill, introduced by Rep. Chris Smith of New Jersey and titled "The Netizens Protection Act of 1997," would have amended the TCPA to ban UCE unless there is a preexisting relationship between the sender and recipient or the recipient grants his or her express consent. It also would have required UCE to include the identity and email address of the sender. Because of its simplicity, certainty, and willingness to place most of the onus on the advertiser, the Smith bill could have succeeded in finally stemming the tide of UCE. It remains to be seen whether the bill will be reintroduced in a subsequent Congress or whether this eminently sensible solution will be forgotten, and one of the current, less comprehensive bills analyzed below will be adopted instead.

C. LEGISLATIVE PROPOSALS

Currently, there are five bills pending before Congress that purport to address the spam problem. Organized anti-spammers are most enthusiastic about HR 2162, the "Can Spam Act," introduced by Rep. Gary Miller of California. The bill, which would provide ISPs with a private right of action against spammers as well as create criminal penalties for some forms of spamming, was drafted with the input of the Coalition Against Unsolicited Commercial Email ("CAUCE"), a group of ISPs and other Internet professionals. Other bills pending would extend the criminal fraud statute to the Internet, authorize the Federal Trade Commission to apply its antifraud rules to Internet commercial activity, allow ISPs to prevent their domains from receiving spam under certain conditions, and provide for civil and criminal penalties (as well as a private right of action against spammers) who falsify their identity or routing information, ignore opt-out requests, or distribute software that forges identifying information.

129. See WL 1998 CQ US HR 1748 summary (tracking bill through legislative process to its ultimate failure).
131. See id. at § 2(3).
132. See id. at § 3(3).
133. See WL 1998 CQ US S 771 (tracking bill through legislative process to its ultimate failure); 1998 CQ US S 875 (tracking bill through legislative process to its ultimate failure); 1998 CQ US HR 4124 (tracking bill through legislative process to its ultimate failure); 1998 CQ US HR 1748 (tracking bill through legislative process to its ultimate failure). None of the four bills introduced during the 105th Congress passed.
137. See id.
NEW APPROACHES TO CURB SPAM

1. S. 699/H.R. 612: The “Telemarketing Fraud and Seniors Protection Act” / “Protection Against Scams on Seniors Act of 1999”

This bill, introduced in the Senate by Sen. Wyden and in the House by Rep. Weygand, would help crack down on some of the most pernicious spamming practices but would not regulate spamming directly. Section 201 of both bills would extend the criminal fraud statute to the Internet. Section 202 would authorize the Federal Trade Commission to initiate a rulemaking proceeding to set forth the application of section 5 of the Federal Trade Commission Act (15 U.S.C. 45), and other statutory provisions within its jurisdiction, to deceptive acts or practices ... in connection with the promotion, advertisement, offering for sale, or sale of goods or services through use of the Internet, including the initiation, transmission, and receipt of unsolicited commercial electronic mail.

Although it is unclear how extensive such FTC regulation would be, S. 699 and H.R. 612 as currently written clearly pass the Central Hudson test. First, the bills target only is misleading speech; truthful claims would not be caught in their net. Second, reducing consumer fraud is clearly a substantial governmental interest. Third, the regulation involved—extending regulatory authority to the FTC, which already regulates consumer fraud perpetrated through other media—more directly advances the governmental interest the bills seek to vindicate than would other solutions, such as authorizing a private right of action. Finally, the regulation involved is, in the abstract, no more restrictive than necessary to achieve the desired end of lessening consumer fraud. This may not be true of the regulations that the FTC would eventually promulgate.

In the end, although the bills themselves are undoubtedly constitutional under Central Hudson, the regulations they spawn may not be. It is thus impossible to predict with certainty whether this particular antifraud proposal will ultimately pass constitutional muster. Furthermore, although the bills themselves are not under inclusive with respect to their professed goals, neither will they do anything to stem the tide of spam washing into users’ mailboxes. Nor will they solve system wide problems (including the havoc slowed systems wreak on legitimate electronic commerce) caused by spamming. It seems highly unlikely that S.R. 699 and H.R. 612 will have any impact at all on spam’s most destructive tendency: overloading server after server, bringing down the Internet one node at a time.

141. See S. 699 § 201; H.R. 612 § 201.

This bill, introduced by Sen. Murkowski of Alaska, is more inclusive than the Wyden and Weygand bills in that it responds, albeit in a flawed manner, to the problems spam creates for individual users. However, it also creates an unwieldy system that requires ISPs to permit spam and does not prevent spammers from reselling email addresses of who do not wish to receive UCE.

The general thrust of the Murkowski bill is to forbid the transmission of UCE if the recipient “submits to the [spammer] a request that the initiation of the transmission of such mail by the person to such other person not occur.” A user may accomplish this in any “appropriate” way, including sending a “remove” message to the email address, which all spammers must include in the body of their messages. However, in order to do so, one must receive a spam first—and the damage is done. Furthermore, making an online purchase constitutes authorization to receive spam from that business. The bill also requires UCE to include information identifying the sender.

The Murkowski bill’s provisions relating to ISPs have already sparked criticism. It permits a domain owner (who may or may not be an ISP) to opt out of receiving spam by notifying its users and the FTC, which will be required to keep a list of all spam-free domains. However, the bill requires ISPs to permit their customers to elect to continue receiving spam and to make a list of the customers opting in available to the public; yet an ISP may not pass the cost of UCE on to such customers. The bill also authorizes FTC regulation of deceptive Internet trade practices, Attorney General suits for violations of the requirements pertaining to users’ opt-out rights and the requirement to provide identifying information, and ISP suits for violations of the provision allowing domain-wide opt-outs. Finally, it preempts all state or local laws dealing with spam.

The Murkowski bill is much more comprehensive than are the Wyden and Wygand bills in that it addresses the system-wide problems that spam can create, particularly through the use of forged headers. Spammers forge headers to avoid hearing from people who are angry that they have been sent UCE, or who request removal from the mailing

---

145. id. § 2(a)(3)(B).
146. See Coalition Against Unsolicited Commercial Email, supra note 135.
147. See S. 759, § 2(c).
148. See id. § 4(c).
149. See id. § 2(c)(3).
150. See id. § 3.
151. See id. §§ 5, 6.
152. See id. § 7.
list. The practice is responsible for a large portion of the costs ISPs pay in dealing with bounce-backs,\textsuperscript{153} irate users, and lawyers prosecuting the intellectual property violations of trademark infringement and misappropriation inherent to the practice.\textsuperscript{154} The Murkowski bill probably represents the least restrictive alternative that does anything at all to advance the government’s interest in keeping the Internet open for business.\textsuperscript{155}

The Murkowski bill appears constitutionally fit under \textit{Central Hudson}. Unlike the Wyden and Weygand bills, it casts a net that catches more communications than just those that are false or misleading. Therefore, there must be a substantial government interest to support the bill. Here, that interest is preventing fraud and protecting the integrity of individual email accounts, much as the TCPA protected users’ fax machines from an unremitting flow of postage-due advertisements. The bill meets the requirement of the third \textit{Central Hudson} prong—that the regulation directly advance the government interest—by clearly targeting the destructive practice of header forgery as well as spammers’ propensity to hide from unwilling recipients who wish to be removed from the mailing list.\textsuperscript{156} Finally, the Murkowski bill clearly passes the fourth \textit{Central Hudson} prong: requiring opting-out ISPs to allow their customers to opt back in is much less restrictive than it need have been to effectively combat the system-wide slowdowns that UCE creates.\textsuperscript{157}

Despite its constitutionality, the Murkowski bill has received little support from users. The major reason for this is that it still permits cost-shifting onto ISPs and users by placing the burden on ISPs to maintain two email systems: one that permits spam and one that does not. Furthermore, as CAUCE points out, requiring companies to list its mail host names on the FTC’s public Web site could create a security risk, and the bill’s requirements interfere with the terms of the contract between an ISP and its users.\textsuperscript{158}

\textsuperscript{153} See Kimberly Patch & Eric Smalley, \textit{E-mail Overload}, Network World, Oct. 26, 1998, at 1, available in 1998 WL 17476163. A “bounce-back” is a spam sent to an email address that is not in service; the message bounces back to the return address. Staff of the ISP whose address was listed on the spam’s header are thus hit with a large amount of email which is, in effect, marked “return to sender.”

\textsuperscript{154} See supra note 23 and accompanying text.

\textsuperscript{155} See SUNY v. Fox, 492 U.S. 469 (1989). Of course, commercial speech restrictions are not required to be the least restrictive alternative. \textit{Id}.

\textsuperscript{156} See id. at § 2(d) and (e).

\textsuperscript{157} See id. at §1(c).

\textsuperscript{158} See Coalition Against Unsolicited Commercial Email, supra note 135.
3. **H.R. 2162: The “Can Spam Act”**

Like the Murkowski bill, this bill, introduced by Rep. Gary Miller (R-Ca.), preempts state and local anti-spam laws; aside from this flaw, it is the bill most likely to slow down the flow of UCE. The bill flatly prohibits using an ISP's equipment to transmit spam (where the ISP has posted an anti-spam policy)\(^\text{159}\) and provides a private right of action to ISPs (though not to individual users),\(^\text{160}\) with damages available up to $25,000 per day for each violation, as well as injunctive and declaratory relief and attorney fees.\(^\text{161}\) It also criminalizes the common practice of unauthorized use of a domain name, if such use damages a system or network.\(^\text{162}\)

The bill appears constitutionally fit. Although it targets speech that is not necessarily misleading or proposing an illegal transaction, the government’s substantial interest in regulation is the same as with all the other anti-spam bills and, for that matter, the TCPA: preventing cost shifting, preventing fraud, and protecting the telecommunications infrastructure. To this end, the Miller bill directly advances the government’s interest by targeting the practice that has resulted in the greatest amount of cost-shifting and system damage: unauthorized use of an ISP's servers and forgery of domain names. The regulation is not unduly restrictive, as it does not ban spam outright, but instead merely regulates the most destructive aspects of spam. Most importantly, the bill shifts the costs of spam back where they belong: onto the advertiser.

From a user's point of view, however, the Miller bill is underinclusive in the extreme. It does not require that spam be directed only to those users who opt to receive such messages—an important goal of many anti-spammers. Furthermore, it does not require spammers to honor opt-out requests or even require them to provide a valid e-mail address where their targets can direct such a request.


This bill, introduced by Rep. Gene Green of Texas, provides civil and criminal penalties for several of the most pernicious spamming practices. It imposes a civil fine for using false identifying information in an unsolicited bulk email message, using false router information, ignoring opt-out requests, or distributing software that forges router or identifying information.\(^\text{163}\) Spammers who misappropriate another person’s name or email address, or who send spam to a person who has previously opted

\(^{160}\) See id. § 2(c).
\(^{161}\) See id. at § 2(c)(1)(B).
\(^{162}\) See id. § 3.
out, face criminal prosecution. The bill authorizes a private right of action for any ISP injured by a spammer's falsification of router information, and one for any UCE recipient injured by any of the practices for which the spammer may receive a civil or criminal sanction. The bill only applies to commercial email, and, like the Murkowski bill, exempts messages sent to a recipient who has a "prior relationship" with the sender, as well as mail sent to a user who has "affirmatively requested to receive communications" from the sender.

Like the other bills under consideration, the Green proposal likely passes the first two prongs of the Central Hudson test. While it goes farther than the Miller bill in regulating UCE (most notably by requiring spammers to identify themselves and to honor opt-out requests), it is somewhat vulnerable on the third and fourth prongs of the Central Hudson test with respect to the opt-out requirement. Direct marketers could argue that the opt-out provision not only does not directly advance the government's cost-shifting, fraud, and system damage concerns, it unduly restricts truthful commercial speech, regulation of which receives more First Amendment protection under 44 Liquormart. However, such an argument could easily be defeated by pointing out that the aggressive speech that the opt-out requirement targets does not come under the aegis of 44 Liquormart. The resolution of this issue remains uncertain—because the TCPA cases did not involve opt-out lists.

Like the other bills discussed here, the Green bill is not perfect from the point of view of many users, primarily because it employs an opt-out rather than an opt-in system. Furthermore, some critics argue that any legislation that permits spamming to continue, as does the Green bill (and, it is important to note, all the others), is flawed because it "legitimizes" the practice. However, given that Congress does not seem inclined to ban UCE outright, the Green bill probably represents the next best alternative.


This bill, introduced by Reps. Heather Wilson (R-N.M.) and Gene Green (D-Tx.), passed the House of Representatives July 18, 2000. It contains Congressional findings of fact with respect to the critical role of

164. See id. § 2(b).
165. See id. § 4(a).
166. Id. § 5.
168. See 1999 CONG US HR 3113.
the Internet in global communication and commerce, that "unsolicited commercial email can be an important mechanism through which business advertises and attracts customers," the "significant" costs of spam, and many spammers' shady business practices.\(^1\) The bill restricts its reach to commercial spam only.\(^1\) It provides criminal penalties for falsifying routing information,\(^1\) requires UCE to include a valid return email address,\(^1\) and requires spammers to respect opt-out requests.\(^1\) The bill also purports to provide government enforcement power of ISP policies regarding UCE, provided that such policies are clear and publicly available.\(^1\) State laws are explicitly not pre-empted,\(^1\) and ISPs are immunized.\(^1\) The FTC, individual victims, and the Attorney General all have enforcement powers.\(^1\) The bill requires the FTC to study the effects of UCE and the effectiveness of the bill, should it become law.\(^1\)

This bill is similar to the Green proposal in its reach, and may cause the same Central Hudson and 44 Liquormart problems due to the opt-out requirement. The dissimilarities between this bill and the Green bill are not germane to its constitutionality or effectiveness, with one major exception. HR 3133's authorization of a private right of action for individuals—a plaintiff class much more numerous than the ISPs covered by the Green bill—would create a new pressure on the federal courts' dockets that may not be justified in the smaller-stakes context of individually aggrieved spam victims, at least those who are not alleging significant, actual monetary damages. Furthermore, if state laws do survive dormant Commerce Clause scrutiny at the appellate level, state courts may be a more appropriate forum for such cases.

\[\text{D. A Better Solution}\]

Because of the underinclusivity of all the current bills, an extension of the court-tested TCPA along the lines of the failed Smith bill remains the only viable proposed solution to the ever-increasing spam problem. If Congress does not revive the Smith bill, any new legislative solution

\[\begin{align*}
\text{169. See } & \text{HR 3113, 106th Cong., 2nd Sess., } \S 2(a)(2000). \text{ See also HR 3113's companion bill, S2542, 106th Cong., 2nd Sess., at } \S 2(9) \text{ (the "Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2000")) (making additional findings on the evils of "pan-}
\text{dering" email).} \\
\text{170. See } & \text{HR 3113 at } \S 3(2). \\
\text{171. See id. at } & \S 4. \\
\text{172. See id. at } & \S 5(a)(1). \\
\text{173. See id. at } & \S 5(a)(2). \\
\text{174. See id. at } & \S 5(b). \\
\text{175. See id. at } & \S 5(b)(3). \\
\text{176. See id. at } & \S 5(c). \\
\text{177. See id. at } & \S 6. \\
\text{178. See id. at } & \S 8.
\end{align*}\]
must address three critical issues: forgery of router and other identifying information, misappropriation of servers, and cost shifting. To that end, the Miller and the Green bills offer the most promise.

A better solution would be to introduce an entirely new bill combining the best of the past and current proposals. Such a bill would aim to ameliorate a wide variety of the problems that spam creates for consumers, businesses, ISPs, and the government. This contrasts with the piecemeal approach many existing state laws, and all current federal bills, have taken.

The bill would start by amending the TCPA, as the Smith bill would have, to require the recipient's consent before a marketer may send UCE and to require truthful identifying information about the sender in every piece of UCE. It would provide penalties for ignoring removal requests and for reselling or reusing the address information of a user who requests removal. It would not provide implied consent to UCE based on a single prior contact, as would the Murkowski and Green bills. This opt-in approach would be substantially more effective than an opt-out regime, as it would stop spam before it overloads servers and causes system damage.

Second, the bill, like the Wyden, Weygand, Murkowski, and Green bills, would authorize the FTC to regulate spam in order to prevent consumer fraud. In other words, it would empower the FTC to ban common spamming practices such as placing false or misleading information in subject lines. However, it would not require the FTC to promulgate an unwieldy, bureaucratic, and expensive-to-maintain global opt-in list, as would the Murkowski bill.

Third, the bill would provide stiff civil and criminal penalties for the most destructive spamming practices: misappropriating servers and forging router, header, and other identifying information. This section would provide for enforcement by the Attorney General and the FTC, as does the Wilson/Green Bill.

The bill would authorize ISPs to block spam and provide a private right of action for ISPs whose equipment is damaged by spammers. This would include a provision for costs and attorney fees and a meaningful statutory damage award in addition to declaratory and injunctive relief. Such a provision would not replace any common law or intellectual property actions that ISPs could pursue against spammers; it would add to the legal arrows in their quiver and provide more certainty to all parties with respect to possible damage awards. Finally, it would provide a private right of action for users (mainly businesses, who are hardest hit by spamming's detrimental effect on server connect times) who suffer actual pecuniary damage from spam.
There are a few provisions found in state laws (which the model bill, like the Wilson/Green bill, would not preempt) that would not be included. The first is a private right of action in the federal courts for individual users who have not suffered individualized economic damage. Quite simply, although the aggregate costs of spam are huge, to individual users this statutory cause of action would rarely, if ever, involve pecuniary damage in an amount sufficient to justify requiring the already overburdened federal courts to intervene. Otherwise, enforcement through the Attorney General, ISPs, the FTC, and business users who suffer pecuniary damage directly attributable to spam should provide that the law is prosecuted with sufficient vigor.

In addition, the bill would not outlaw the possession, sale, or distribution of software programs that enable mass emails. Clearly, a marketer's use of such a program would be relevant evidence in a trial in which it is charged with violating the anti-spam statute. However, a flat ban on such software sweeps too broadly, snaring noncommercial speakers in its net. Although that the damage and expense caused by bulk email may justify regulation of such software even in a noncommercial context, analysis of such a ban is beyond the scope of this article.

V. CONCLUSION

Until comprehensive anti-spam legislation becomes law, spam recipients and ISPs will continue to play a futile game of legal whack-a-mole with direct e-marketers. Intellectual property and common law actions against spammers have proven a costly, ineffective, and piecemeal non-solution. Similarly, the few state laws that have gone into effect protect few users and may, as Congress concluded with respect to state anti-junk fax laws, have constitutional problems under the dormant commerce clause. While federal regulation will not stop all spam, it seems unlikely that U.S. marketers will continue to spam if they are forced to dial into an overseas connection to do so. Non-U.S. marketers selling Web-based services may still spam, but if they do so by misappropriating U.S. equipment, any of the laws under consideration would confer jurisdiction over the offender.

As discussed above in the context of already existing bills, the provisions of the model bill, as they must, fulfill the constitutional requirements of Central Hudson. The government's substantial interest in ameliorating spam's most pernicious effects is directly advanced by requiring the marketer both to secure the recipient's consent and to include truthful identifying information in the email; these important steps will reduce system overloads by allowing recipients to remove themselves from unwanted mailing lists, while allowing businesses to continue direct e-marketing. The provisions relating to the FTC deal
with misleading advertisements, which under *Central Hudson* can be banned outright; they are, therefore, not unconstitutional, even if they did not directly advance a governmental interest, or were more restrictive than necessary to satisfy that interest. The civil and criminal penalties directly advance a substantial governmental interest by providing an explicit penalty aimed at the effects of identity theft (i.e., the practice of forging identifying information) and property damage (caused by misappropriation of servers). The ISP provisions directly advance a governmental interest in keeping the Internet open for business by empowering ISPs to adopt individual technical solutions to prevent spammer damage and by providing recourse if damage occurs. These provisions are a good example of a truly less restrictive alternative to, for example, a government-run filtering system. Similarly, the private right of action for businesses encourages self-help, as opposed to overregulation.

The steps outlined above would go a long way toward stopping the spam problem, in a manner that does not unconstitutionally target the content of direct marketers' speech but rather the most intrusive and destructive methods some employ. Congress should pass such a bill in order to protect the telecommunications infrastructure, prevent further consumer fraud, system damage, and intellectual property violations, and preserve the viability of the Internet as a medium where both communications and commerce flourish.