DePaul University
University Libraries

DePaul Journal of Art, Technology & Intellectual Property Law

Volume 10
Issue 1 *Fall 1999: Symposium - Theft of Art During World War II: Its Legal and Ethical Consequences*

Article 9

Regulating Your Internet Diet: The Can Spam Act of 1999

Vasilios Toliopoulos

REGULATING YOUR INTERNET DIET: THE CAN SPAM ACT OF 1999

I. INTRODUCTION

The proliferation of unsolicited commercial e-mail ("UCE"), commonly known as "spam,"[1] has gorged Internet Service Providers ("ISPs")[2] worldwide, creating a need for legislative intervention. As a result of increased e-mail transmission, Internet access has become more lethargic and web-users have become increasingly frustrated.[3] Although the Internet has quickly become an indispensable medium of communication, it has also fallen prey to advertisers selling everything from pornographic web-site memberships to get-rich quick schemes.[4] Solicitors on the Internet have found that spam is one of the easiest, least expensive, and least regulated means of reaching a captive audience.[5]

---

1 The true origin of the term "spam" is disputed. Some claim the term is derived from a Monty Python skit where a couple go into a restaurant and attempt to order a meal. In the background, a group of Vikings chant and sing the praises of spam, which drowns out all other conversation. By the end, all conversation except the word "spam" is unintelligible. *See Spam FAQ: Figuring Out the Site the Spam Came From*, (visited Oct. 2, 1999), <http://www.bluemarble.net/scotty/forgery.html>. Others claim the term is derived from the canned meat "Spam" by Hormel Foods, which is believed to have little if any nutritional value. *See* Donna Lampert, et al., *Overview of Internet and Regulatory Issues*, 544 PLI/Pat 179, n. 114 (1998).

2 Matisse Enzer, *Glossary of Internet Terms* (visited Oct. 20, 1999) <http://www.matisse.net/files/glossary.html>.

3 Daniel P. Dern, *Postage Due on Junk E-Mail—Spam Costs Internet Millions Every Month* (visited October 8, 1999) <http://www.techweb.com/se/directlink.cgi?>.

4 Stanley A. Miller, *Taking Aim at Spam E-Mail Abuse Affects Providers*, Milwaukee Journal & Sentinel, May 11, 1999, at 1.

5 *See* Roberta Furger, *Opinion: Is AOL Losing the Fight Against Spam?*, (July 5, 1999) <http:cnn.com/TECH/computing/9907/05/aolspam.idg/>. (stating that harvesting e-mail addresses is as simple as calling an ISP's member directory or writing a program that stores all screen names as they appear in chat rooms).

According to conservative estimates of e-mail use, thirty percent of approximately fourteen million e-mail messages sent daily consist of spam.[6] Rampant abuse of the Internet by bulk commercial solicitors has led to a public outcry for action.[7] This action has taken the form of numerous propositions in the United States Congress, none of which have succeeded in passing both houses. The most recent and widely supported is the Can Spam Act of 1999,[8] sponsored by Representative Gary Miller.

II. BACKGROUND

A. Self-Regulatory Measures

The problem of unsolicited commercial e-mail is economically unique.[9] As opposed to traditional junk mail, the cost of sending spam is borne by the recipient rather than the sender.[10] The solicitor, who is required to pay for printing materials as well as the postage necessary to send it, funds traditional mass mailing.[11] In contrast, junk e-mail can be sent to millions of e-mail addresses at virtually no cost to the spammer because the recipient, the service provider and ultimately Internet subscribers as a whole,

---

6 Dern, *supra* note 3. (approximation by America Online Inc.,) Netcom Communications Inc., estimates that approximately 10 percent of customers' Internet service bill or $1 million per month goes toward fighting spam.

7 *Forum for Responsible & Ethical E-Mail: Spam Primer* (visited Oct. 8, 1999), <http://www.spamfree.org/spamprimer>. *See also* Elizabeth Weise, "Feeling Spammed? Internet Users Get Deluged by More Junk E-mail" (Aug 5, 1999) <http://www/detnews/1999/technology> (stating that 90% of all Internet users receive junk-email at least weekly and 96% who have e-mail addresses for more than four years).

8 HR. 2168, 106th Cong. (1999).

9 *Id.*

10 Lorrie Faith Cranor and Brian A. LaMacchia, *Spam!*, COMMUNICATIONS OF THE ACM, Aug. 1998, Vol. 41, No. 8, at 77-78.

11 Ray Everett-Church, Testimony on Behalf of the Coalition Against Unsolicited Commercial E-Mail before the United States Senate Communications Subcommittee (June 17, 1998) (available at http://www.cauce.org/testimony/senate_testimony>).

absorb the cost.[12] The recipient of spam is required to pay for additional time of Internet access in order to download, delete and register complaints for the unwanted solicitation.[13] Second, an ISP used for transmitting spam also bears the cost of its transmission.[14] An ISP must deal with the problem of increased bandwidth, requiring the expense of large amounts of money on hardware to handle the increased volume of e-mail sent and stored on a daily basis.[15] Service providers must also hire additional administrative staff to register and handle customer complaints.[16] Ultimately, the added expenses incurred by the ISPs are transferred onto the consumers in the form of increased hourly or monthly charges.[17]

In order to reduce the transmission of spam, most suggested measures fail to work adequately, if at all.[18] The first and most obvious measure is to attempt to remove the junk e-mail, and request that the sender cease further transmission.[19] While only some unsolicited e-mail contains removal instructions to stop future spam, it is one of the most ill advised ways to deal with the problem.[20] By following such instructions a junk e-mail recipient will accomplish one of two things: 1) verify his/her e-mail address to the spammer, allowing for the address to be used repeatedly and have the address added to other bulk mailing lists; or 2) the removal will be returned as "undeliverable" because the domain

12 *Id.*

13 *Id.*

14 *Id.*

15 E-mail messages that are undeliverable to the intended address effectively "bounce back" to the sender in order to be stored. If the sender's address is forged, the undelivered mail is bounced back to and stored by the service provider itself. The use of more space to store thousands of undelivered e-mail messages daily is a major factor in increased bandwidth consumption. Hotmail Corp.v. Van$ Money Pie, No. C-98 JW PVT ENE, C 98-20064 JW, 1998 WL 388389, at *2 (N.D. Cal. Apr. 16, 1998).

16 Cranor, *supra* note 10, at 77.

17 *See,* Stanley A. Miller, *supra* note 4, (stating that for Netcom Online Communications Service, a global service provider, $3 per customer per month is applied to hardware and labor costs).

18 James A. Martin, *Three Ways to Spamproof Your Inbox,* (June 30, 1998), <wysiwg:126/http://cnn.com/TECH?...ng/9806/30/diy.spam.idg/index.html>.

19 *Id.*

20 *Id.*

name had been fraudulently obtained, making the spammer unreachable and the removal request ineffective.[21]

Another proposed way to deal with UCE is through the use of spam-blocking filters.[22] Programs such as Netscape Communicator 4.0 and Microsoft Explorer,[23] attempt to stop spam before it even reaches an intended e-mail address by allowing the e-mail user to create and maintain a "whitelist" of names and addresses from whom e-mail is acceptable and a "blacklist" of suspected spammers to be blocked out.[24] Yet the most common problems with filtering are that some well-meaning and acceptable e-mail messages go undelivered simply because they contain words that are automatically blocked, or that well disguised spam slips through the filter undetected.[25] Since filtering systems are not foolproof, they simply create an incentive for spammers to create new ways of bypassing such systems.[26]

Similar to filtering systems, the creation of "opt-in" and "opt-out" lists offers similar protection, yet have nearly identical failures.[27] Essentially, such lists are compiled by ISPs and allow their subscribers to request to be taken off marketing lists and

---

21 *Id.*

22 Jeff Partyka, *AT&T Worldnet to Use Brightmail to Block Spam*, CNN.com (August 27, 1999) <http//cnn.com/TECH/...9908/27/bright.mail.icg.index.html>

23 Martin, *supra* note 18 at 2.

24 *SpamCop: File A Spam Report,* (visited Oct.8, 1999), <http://spamcop.net> (discussing service that filters spam before reaching the recipient's e-mail inbox and creates "white" and "black" lists to determine what e-mail the subscriber deems acceptable).

25 Martin, *supra note* 8; *See also* 544 PLI/Pat 179, 212 (spam detection software that identifies the mail through content rather than domain name has been used increasingly by service providers including Bright Light, Concentric, AT&T, EarthLink and USA.net).

26 *See,* CAUCE Testimony, *supra note* 11, at 11 (noting that once ISPs implement a block on a particular location the spammer simply changes his location by either obtaining throw-away internet accounts, which are usable only once).

27 David E. Sorkin, *Unsolicited Commercial E-Mail and the Telephone Consumer Protection Act of 1991*, 45 Buff. L. Rev. 1001 (1997).

require advertisers' strict compliance.[28] Many programs are created in order to head off legislation that would arguably hinder reputable marketers' efforts to use e-mail legally and ethically.[29] To date, very few junk-e-mailers comply with customer requests by cross-referencing their opt-out lists with mailing lists and actually delete those who have requested it.[30] As can be speculated, the creation of either type of list would need strong enforcement mechanisms. However, the first problem is that of incentive.[31] While most agree that such lists should exist, the cost to an ISP to promote and maintain a master list could outweigh the benefits. Arguably, it could be more economically efficient to employ more full-time customer service personnel to handle complaints rather than employ the same if not more personnel to constantly update "opt-in" and "opt-out" lists.[32]

In order to equalize the cost of transmission, many have suggested the creation of payment plans for all those who receive spam.[33] The payment systems work in one of two ways: 1) allow internet users free e-mail, as long as they agree to have their e-mail addresses on advertising mailing lists;[34] or 2) pay a nominal fee to

---

28 Sharon Machlis, *Marketing Group to Offer "Opt-Out" for E-Mail*, (March 1, 1999) <http://www.computerworld.com/home/news.nsf/all/990301thisone> (marketing group, Direct Marketing Association, attempt to create system and have all members pledge compliance with the associations guidelines regarding Internet privacy).

29 *Id.*

30 *See,* Cranor *supra* note 10, at 79.

31 James W. Butler III & Andrew Flake, *AOP: The Effective Control of Direct Electronic Marketing* (visited October 12, 1999) <http:aop.org/pubs/dem.html> (stating that the success of the opting solutions depends on whether there is sufficient motivation to keep such lists well-maintained, well-promoted and easily accessible to consumers).

32 Martin Stone, *ISP Seeks Relief From Spammer* (March 19, 1999) <http://www.computercurrents.com/newstoday/99/03/19/news11.html> (Internet Direct, Ltd., was forced to over-build its additional staff strictly to deal with customer complaints since technical solutions such as filtering, warnings, and account terminations were having very little deterrent effect).

33 Cranor & LaMacchia *supra* note 10, at 81.

34 Kathleen Murphy, *ISPs Offered Money To Accept Spam E-Mail*, (April 6, 1998) <http://www.internetworld.com/print/1998/04/06/news/19980406-money.html>.

recipients for each piece of commercial e-mail they read.[35] The first system is similar to the opt-in method discussed above, except subscribers receive any and all e-mail advertisers send. This system both fails to create incentives for spammers to stop mass mailings, and invites others to begin their own spam campaigns.

In contrast, a system of incremental payments creates a disincentive for "small-time" spammers to transmit blind junk mail, the system would not affect larger solicitors as much. Although the payment system arguably distributes the cost of spam more evenly among all parties, many large companies would not change simply because the system is only an increased cost of doing business. Another problem is that payments to spam recipients are made by use of digital systems, which must be compatible to all servers.[36] To date, a majority of service providers have not created such systems, and those who have succeeded find their programs are often incompatible with others.[37]

B. Federal Legislation

Since the effectiveness of self-regulatory options has been questionable at best, many frustrated Internet service providers have looked to statutory law for assistance. Although the Internet is a relatively novel phenomenon, several federal statutes have recently been passed to regulate this unique medium. However, no legislation has been passed to deal exclusively with commercial e-mail. Thus a need has been created for new federal laws to be broadly interpreted to encompass situations and problems not originally contemplated. Specifically, ISPs have asked the judiciary to loosely interpret federal statutes in order to successfully sustain numerous civil suits against the most shameless and incorrigible junk e-mailers. Presently, there is no

35 Cranor, *supra* note 10, at 81.
36 *Id.*
37 *Id.*

federal statute that adequately tackles all aspects of the multi-faceted problem created by unsolicited commercial e-mail.

1. Computer Fraud and Abuse Act

Established in 1984, the Computer Fraud and Abuse Act[38] has been one of the most popular statutes cited in suits against unsolicited e-mail advertisers. The Act prohibits any person from intentionally accessing a computer without authorization, knowingly transmitting information, and as a result causing damage to the computer.[39] While punishment for a first offense under the Act is "a fine or imprisonment for not more than ten years, or both," a second conviction for the same conduct mandates no more than twenty years imprisonment and/or another fine.[40] Furthermore, the Act gives the Secret Service authority to initiate investigations involving computers used by the United States government or associated with financial institutions and authorizes the Attorney General to prosecute such conduct.[41] Although the Computer Fraud and Abuse Act has been effective in dealing with fraudulent misrepresentations and false information transmitted by spammers,[42] the statute fails to address ISPs rights to monitor and or filter the massive flow of non-fraudulent unsolicited commercial e-mail and the abuses that occur.

2. Telecommunications Act of 1996

One of the most recent federal statutes is the Telecommunications Act of 1996.[43] The Act ensures that no user of an interactive computer service shall be liable for any action taken in good faith to restrict access or availability of material the provider considers "lewd, lascivious, filthy, excessively violent,

38 18 U.S.C. § 1030 (1984).
39 *Id.* at (a)(4).
40 *Id.* at (c)(1)(A).
41 *Id.* at (h).
42 *Hotmail Corporation v. Van$ Money Pie Inc.*, 1998 WL 388389, at *2.
43 47 U.S.C. § 230 (1996).

harassing, or otherwise objectionable" regardless if it is constitutionally protected.[44] Further, the Act requires that service providers notify subscribers of control options available to them, such as filters, and other software.[45] Although it is directed at controlling minors' access to adult websites, the statute allows service providers great discretion to deal with other electronically transmitted material.[46] Arguably, the Act does not only deal with material that is harmful because it is indecent, obscene or pornographic, but also grants ISPs enough latitude to filter or control any material that it finds "harassing or otherwise objectionable," including junk e-mail. Since the Telecommunications Act does not specifically deal with certain major problems such as forged domain names and one-time unsolicited advertisements, its applicability is severely limited to repeat aggressive spammers who qualify as "harassing." Based on its limited applicability, the Telecommunications Act does not adequately serve the wide-ranging and constantly changing problem posed by the largest and most brazen spammers.

3. Telephone Consumer Protection Act of 1991

Another statute, the Telephone Consumer Protection Act of 1991[47] ("TCPA"), commonly known as the "Junk Fax Law," protects telephone and facsimile recipients from unsolicited advertisements.[48] The law protects telephone solicitation recipients by placing stringent time, place and manner restrictions on the phone calls by telemarketers.[49] First, the TCPA makes it unlawful for telephone solicitors to use an artificial or pre-recorded voice to deliver a message or make a solicitation without the prior written

44 *Id.* at (b)(2)(A).
45 *Id.* at (d).
46 *Id.* at (f)(4).
47 47 U.S.C. § 227 (1991).
48 *Id.*
49 *See,* Moser v. Federal Communications Commission, 46 F3d. 970 (9th Cir. 1995) (holding that the application of the Telephone Consumer Protection Act to telemarketers was a content-neutral restriction subject only to intermediate scrutiny).

consent of the called party.[50] Based on this prohibition the Act allows any person or entity a private right of action for a violation.[51] The action allows recovery for each violation in the amount of the actual monetary loss or $500, whichever is greater. Furthermore, a plaintiff can receive up to $1500 for each message if the defendant is deemed to have acted willfully or knowingly in violation of the law.[52] Second, the TCPA allows for telephone users to be placed on "do not call lists" upon request.[53] These lists are compiled by a national database of residential telephone numbers at no additional cost to subscribers. Similarly, the Act provides that if a solicitor calls a telephone number on a "do not call" list, the recovery of $500 to $1500 per call is also allowed.[54] Finally, the Act sets out technical and procedural standards, stating that all facsimiles must identify the sender prominently on the first page of transmission.[55]

Although the TCPA has been extremely efficient in dealing with junk faxes and telemarketers, its application to unsolicited e-mail would be tenuous at best.[56] The first difference between the two media is the fundamental differences in their basic hardware. Fax machines use a modem to establish a one-to-one connection between the sender and recipient, making it impossible for any other communication to either party while a fax is being transmitted.[57] In contrast, e-mail is transmitted nearly instantaneously, and can be stored by the recipient until she decides to open it. Ultimately, junk faxes make the recipient a captive audience, raising issues of privacy infringement, which are not as easily applicable for junk e-mail claims.[58] The second distinction is varied costs. While maintaining an operational fax machine with paper and toner is not extremely expensive, it is far

50 47 USCA § 227 (b)(1)(a) and (b).
51 *Id.* at (b)(3).
52 *Id.* at (b)(3)(C).
53 *Id.* at (c)(3).
54 *Id.* at (c)(5)
55 *Id.*
56 David E. Sorkin, *supra* note 27, at 1006.
57 *Id.*
58 *Id.*

more costly than maintaining an e-mail account. E-mail is transmitted, stored and read electronically, at less cost to both sender and recipient.[59] Fundamental differences such as these evidence the inapplicability of the TCPA to junk e-mail without extensive alteration.

4. Electronic Communications Privacy Act

In 1986, the Electronic Communications Privacy ("ECPA") was passed as an Amendment to Federal Wiretap Act.[60] Generally the ECPA prohibits the interception of electronic information while it is transmitted,[61] and the unauthorized interference with or access to such information while in storage.[62] Furthermore, the Act prohibits electronic service providers from knowingly divulging to any person or entity the contents of stored communications.[63] Under all provisions of the ECPA, an award of civil damages is available for violating any of these provisions.[64] However, the problem with the ECPA lies in the limited discretion and rights allowed to service providers in monitoring the types of e-mail transmitted. Although the ECPA provisions allow for disclosure of information unrelated to the substance of an electronic transmission, ISPs are prohibited from examining both the content of e-mail messages and their subject lines.[65] Consequently, many of the monitoring and filtering activities employed by service providers in order to stem the tide of junk e-mail would qualify as

---

59 *Id.*

60 18 U.S.C. § 2510 (1986).

61 18 U.S.C. § 2511 (1994) "Interception" is defined as the "acquisition" of any electronic communication "through the use of any electronic, mechanical, or other device".

62 18 U.S.C. § 2710 (1994) "Access" is defined as when a person "obtains, alters, or prevents authorized access to" and electronic communication while it is in electronic storage.

63 18 U.S.C. § 2702 (1994).

64 18 U.S.C. § § 2520, 2707 (1994).

65 Steven Miller, *Washington's Spam Killing Statute: Does It Slaughter Privacy in the Process?*, 47 WASH. L. REV. 453, 462 (1999).

"interception" violations of the ECPA.[66] Although ISPs have unrestricted access to the contents of electronic communications after they are stored, this does not solve the constant problem of increased bandwidth. If a junk e-mail message is both transmitted and stored by an ISP, the spammer's goal has effectively been accomplished unhindered. Therefore, any access to or monitoring of junk e-mail by ISPs after transmission does not create an incentive for junk e-mailers to stop forging e-mails' points of origin or transmitting e-mail with false or misleading information on subject lines.

C. State Legislation

To date fourteen states have enacted legislation to deal specifically with the problem of unsolicited commercial e-mail.[67] One of the first to formally enact such a law was Nevada, which banned unsolicited commercial e-mail unless the message is "clearly and conspicuously identified" as an advertisement, and required all such messages to include "opt-out" instructions.[68] Other states such as Virginia impose stricter penalties and larger fines for similar conduct.[69] The Virginia statute provides for criminal penalties against spammers, in addition to insulating service providers by their subscribers for the junk e-mail they

---

66 *Id.* at 472 Although a "protection of interests" exception to the interception exists, ISPs would most likely fail in qualifying for the exception. The use of hybrid and/or proactive approaches to monitoring electronic communications would not meet the requirements of the exceptions allowed by the interception provision because less intrusive approaches to protecting ISPs property interests exist.

67 *Unsolicited E-Mail Statutes*, (visited Sept. 23, 1999) <http.jmls.edu/cyber/statutes/email/state>.

68 41 N.R.S. § 7 (1997) (as amended by Senate Bill No.13) (the original bill prohibited UCE absent a preexisting business or personal relationship, and civil damages in the amount of $10 or actual damages for each violation).

69 *See* Zeleny Jeff, *Legislators Target Unsolicited E-mail*, THE DES MOINES REGISTER, Feb. 19, 1999, at 6 (Proposed Iowa statute allows for a fine of $250 to $5000 per violation); Illinois House Bill No. 2616, 91st Gen. Ass. (1999) (allowing for private right of action and recovery of $500 per violation).

receive from mass commercial e-mail.[70] Based on its provisions, forged sender addresses are classified as a misdemeanor, punishable by a fine of up to $500 per message.[71] However, if the spammer's transmission is considered "malicious" and/or causes more than $2500 in damage, the conduct is chargeable as a felony.[72]

In the Washington statute, not all unsolicited commercial e-mail is prohibited, only communications that either misrepresent a sender's e-mail address or contain false information on the subject line.[73] The statute also allows ISPs and spam recipients to bring a civil suit to recover their damages,[74] and gives the Attorney General the power to sue based on provisions of the Electronic Consumer Protection Act.[75]

In California, the state legislature has passed several statutes to deal with the spam problem, including an amendment to the California Business and Professional Code. This amendment is the predecessor of the Federal Can Spam Act, both sponsored by Representative Gary Miller.[76] First, the California statute defers to service providers by prohibiting the use of equipment owned by ISPs that is in violation of their respective policies regarding the initiation of unsolicited commercial e-mail.[77] Second, the statute provides for "a civil action to recover actual monetary loss suffered by a service provider, or fifty dollars ($50) for each violation, . . .

---

70 VA CODE ANN. § 18.2-152.4 (1998).

71 VA CODE ANN. § 18.2-152.4 (C)

72 *Id.*

73 WASH. REV. CODE §19.190.005 - 050 (1998).

74 WASH. REV. CODE §19.190.040. For each violation service providers are allowed damages of $1000, and junk e-mail recipients receive actual damages or $500, whichever is greater,.

75 WASH. REV. CODE §19.86.080.

76 CAL. BUS. & PROF. CODE §17538.4. Among other provisions, the California statute mandates any business conducting advertising using e-mail to include a valid return e-mail address that the recipient can use to notify the sender not to transmit any further solicitations. Also, unsolicited advertising material transmitted via e-mail is required to include "ADV:" in the first four characters in the subject line, and "ADV:ADLT" if the solicitation is directed at adult recipients.

77 CAL. BUS. & PROF. CODE §17538.45 (b).

up to a maximum of twenty-five thousand dollars ($25,000) per day."[78] However, by bringing such an action, a service provider is required to prove that the defendant spammer had notice of the ISP's spam policy and defendant's transmission used plaintiff's equipment located in the state.[79]

D. Litigation

Since less intrusive means of curbing spam have proven unsuccessful, many Internet Service Providers have resorted to common law litigation in order to enjoin the practice. In *Cyber Promotions Inc. v. America Online Inc.,*[80] the district court for the Eastern District of Pennsylvania consolidated cross-complaints between a private online company and an Internet Service Provider regarding the right to freely disseminate spam to ISP subscribers.[81] In this case, Cyber Promotions sought injunctive relief and damages based on America Online's (AOL's) "e-mail bombs,"[82] AOL's prevention of its members from receiving Cyber Promotions e-mail messages, and declaratory relief stating that Cyber Promotions had a First Amendment right to send advertisements to AOL's subscribers.[83] The court held the actions taken by a private online company to eliminate unsolicited e-mail sent to its subscribers did not constitute state action for the purposes of the First Amendment.[84] Furthermore, the court found that a right to freely distribute unsolicited commercial e-mail is not

78 CAL. BUS. & PROF. CODE §17538.45 (f).

79 CAL. BUS. & PROF. CODE §17538.45 (f)(3)(A)(i-ii).

80 Cyber Promotions Inc. v. America Online Inc., 948 F. Supp. 436 (E.D. Pa. 1996).

81 *Id.* at 456.

82 An "e-mail bomb" occurs when many e-mails are collected and sent all at once to an address. In this case, AOL gathered all the undelivered unsolicited e-mail sent by Cyber Promotions, altered the return path, and sent a bulk e-mail back to Cyber Promotions. This bulk mailing disabled Cyber Promotions' ISPs, many of whom terminated their contracts with Cyber Promotions. *Id.* at 437.

83 *CyberPromotions,* 948 F. Supp. at 438.

84 *Id.*

guaranteed by the First Amendment, especially when other forms of solicitation are available.[85]

Similarly in *CompuServe v. Cyber Promotions*,[86] an Ohio district court determined that Cyber Promotions' unsolicited bulk advertising was sufficiently reprehensible to be enjoined.[87] In this case, CompuServe relied on the property concept of trespass to chattels in order to protect its computer systems from being used to send spam by the infamous Sanford "Spamford" Wallace.[88] CompuServe, an ISP, had been inundated by unsolicited e-mail sent by the defendants, as well as by customer complaints about this spam.[89] CompuServe claimed the defendants, without consent, used its proprietary computer systems and that such use led to "diminution of its quality, condition and value."[90] The district court agreed and held that Cyber Promotions actions were an actionable trespass.[91] Ultimately, the court granted CompuServe an injunction against Cyber Promotions, restraining defendant from "sending any unsolicited advertisements to any electronic mail address maintained by the plaintiff."[92] Although emphasizing a preference for the use of self-help measures such as those suggested above, the court found that an injunction was the only adequate remedy sufficient to protect CompuServe's nationwide computer network.[93]

---

85 *Id.*

86 962 F. Supp. 1015 (S.D. Ohio 1997).

87 *Id.* at 1016.

88 *Id.* at 1017.

89 *Id.* at 1019.

90 *Id.* at 1021, citing RESTATEMENT (SECOND) OF TORTS §218 (1965) Trespass to a chattel subjects the possessor of the chattel to liability if, but only if: (a) he dispossesses the other of the chattel, or (b) the chattel is impaired as to its condition, quality, or value, or (c) the possessor is deprived of the use of the chattel for a substantial time, or (d) bodily harm is caused to the possessor or harm is caused to some person or thing in which the possessor has a legally protected interest.

91 *Id.* at 1024.

92 *Id.* at 1028.

93 *Id.* at 1017.

Similar to *CompuServe,* the plaintiff in *Hotmail Corp. v. Van$ Money Pie, Inc.*[94] sought relief to enjoin Van$ Money Pie from sending bulk commercial e-mail messages under falsified e-mail addresses owned by the plaintiff.[95] Hotmail based its cause of action not only on common law trespass to chattels, but also violation of the Computer Fraud Abuse Act,[96] unfair competition, breach of contract, fraud, misrepresentation, and trademark dilution.[97] In this case, Van$ Money Pie obtained consent to create Hotmail accounts limited to Terms of Service which included a prohibition against spamming.[98] The defendant, however used the Hotmail domain name to solicit plaintiff's subscribers, and falsely designated the spam's point of origin.[99] The forged sender addresses caused all customer complaints regarding the spam to "bounce back"[100] to Hotmail.[101]

The district court took a similar position to the court in *CompuServe*, and found defendant's actions violative of the common law trespass to chattels.[102] This trespass was caused by transmitting misdirected spam without authorization, filling up plaintiff's computer storage space, and threatening to damage Hotmail's ability to service its legitimate customers.[103] The court also found that the defendant violated the Lanham Act[104] by causing "consumer confusion or mistake as to the origin, sponsorship, or approval" of the defendant's junk e-mail, through the falsified use of Hotmail's mark.[105]

Contrary to the plaintiffs' attempts at equitable relief in *CompuServe* and *Hotmail*, the plaintiff in *America Online Inc. v.*

---

94 1998 WL 388389, at *1.
95 *Id.* at *3.
96 *Id.*
97 *Id.*
98 *Id.* at *2.
99 *Id.*
100 *See supra* note 14.
101 *Hotmail*, 1998 WL 388389, at *2.
102 *Id.* at *7.
103 *Id.*
104 15 U.S.C. § 1125 (a)(1).
105 *Hotmail*, 1998 WL 388389, at *4.

IMS[106] instead sought damages against a marketing company for unauthorized e-mail advertising.[107] Yet, analogous to *CompuServe* and *Hotmail*, the claim was primarily based on IMS's tortious trespass to personal property, and its violation of the Lanham Trademark Act.[108] The court found IMS liable for trespass to chattels and explained that defendant's contact was actionable not only because its bulk solicitations diminished the value of plaintiff's possessory interest in its computer network, but also that it "injured AOL's business good will."[109] Although the loss of good will damages were not easily quantifiable, the court cited the more than 50,000 subscriber complaints in only ten months, defendant's spamming, and the increased subscriber cancellation rate since IMS began its mailings.[110] The court deferred ruling on damages, however, until the issuance AOL's offer of proof and IMS's opportunity to object.[111] The court also found that IMS violated the Lanham Act by sending over sixty million e-mail advertisements and falsely designating their origin as being sent from "aol.com" addresses.

III. PROPOSED FEDERAL LEGISLATION

Similar to the legislation proposed and passed by Representative Miller in California,[112] the Can Spam Act of 1999 attempts to deal with unsolicited commercial e-mail in three distinct ways: 1) It

106 24 F. Supp.2d 548 (E.D. Va. 1998).

107 *Id.* at 549.

108 *Id.* citing 15 U.S.C. § 1125 which states that "any person who, on or in connection with any goods or services, or any container for goods, uses in commerce any word, term name, symbol, or device or any combination thereof, or any false designation of origin, false or misleading description of fact . . . which: (a) is likely to cause confusion or mistake, or deceive as to the affiliation, connection, . . . origin, sponsorship, or approval of his goods, services or commercial activities . . . shall be liable in a civil action by any person who believes that he or she is likely to be damaged by such an act.

109 *Id.* at 550.

110 *Id.*

111 *Id.* at 552.

112 CAL. BUS. & PROF. CODE § 17538.45 (enacted by Chapter 863).

gives internet service providers (ISPs) a right of action against any spammer who violates the ISP's unsolicited commercial e-mail policy; 2) it allows service providers to post their policy against UCE on the web or on the server itself; and 3) it creates criminal penalties for the unauthorized use of domain names in sending spam.[113]

First, the statutory creation of a cause of action against spammers gives ISPs the ability to self-regulate their medium. A statutory cause of action allows for the award of actual monetary loss suffered by the provider as a result of spamming, a fifty dollar fine for each message that violates the ISP's policy against spam.[114] This award is limited to $25,000 per day.[115] In the event of particularly egregious behavior by junk e-mailers, the bill warrants the granting of injunctive relief as well as attorney's fees for the prevailing party.[116]

Second, the bill proposes that service providers be allowed to post their UCE policy not only on their World Wide Website, but also on the initial banner message that accompanies their mail server.[117] This banner message is transmitted automatically upon connection to the addressee's service provider for all e-mail messages.[118] As proposed, this banner would also notify the purported spammer of the ISP's policy against spam, and offer an option to terminate the connection or to continue delivery.[119] The banner notification would simply state a textual message of "NO UCE" or give a specific definition by stating "UCE POLICY AT [service provider's name]."[120]

Third, the bill proposes criminal penalties for the unauthorized use of domain names. If the spam sender uses a return address other than his/her own and that message causes damage to a computer, computer system, or computer network, the penalty

113 H.R. 2162, 106th Cong. (1999).
114 H.R. 2162 at § 2(c)(2)(B).
115 *Id.*
116 *Id.*
117 *Id.* at § 2(d)(4)(C)(iii).
118 *Id.*
119 H.R. 2162 at § 2(d)(4)(C).
120 *Id.*

would be up to one year in prison.[121] The damage caused could range from transmittal of a computer virus to the "crashing" of a network due to bandwidth overload.[122]

A contemporary bill to Miller's Can Spam Act presently in Congress is the Inbox Privacy Act of 1999.[123] This bill is sponsored by Senators Toricelli and Murkowski and is a combination and modification of two former bills suggested by them in the 105th Congress that failed to pass.[124] Among other requirements, the present bill: 1) demands that valid return addresses be included in all unsolicited e-mail messages; 2) prohibits forgery of headers; 3) requires senders to comply with opt-out requests; 4) allows domain name owners to publish opt-out lists that apply to all addresses under the domain name; 5) requires domain owners and ISPs to register their preferences with the Federal Trade Commission; and 6) requires ISPs to maintain opt-out lists to block spam, but prohibits ISPs from charging additional fees for said service.[125]

---

121 H.R. 2162 at § 3(b)(4)(B).

122 *Pacific Bell Suffers Slowdown*, C-Net News (March 13, 1998) <http://www.news.com/News/Item/0,4,20046,00.html>.

123 759, 106th Cong. (1999); *See also* H.R. 3113, 106th Cong. (1999) As recently proposed by Rep. Wilson, with the short title "Unsolicited Electronic E-Mail Act of 1999. Along with making extensive findings based on public policy, the Wilson Bill suggests the creation of opt-out lists maintained by the Federal Communications Commission and requirements for valid return addresses. Violation of any provision would allow for orders from the FCC or the local district court to cease and desist transmission. The Wilson Bill also creates private rights of action by ISPs or Internet subscribers punishable by injunctions and or monetary awards of $500 per violation, limited to $25,000 per day.

124 Senator Toricelli originally sponsored the "Electronic Mailbox Protection Act of 1997," S 875, 105th Cong. (1997), which would have required any and all senders of unsolicited e-mail to use valid return addresses and comply both with recipient requests to opt-out and Internet standards. Senator Murkowski's "Unsolicited Commercial Electronic Mail Choice Act of 1997," H.R. 771, 105th Cong. (1997), would have required an "advertisement" label on every UCE, required the sender's real name, street address, e-mail address and phone number, and mandated ISP's to block out any and all incoming advertisements upon request.

125 759 106th Cong. (1999).

IV. ANALYSIS

Although private and self-regulatory initiatives are preferred over legislative or judicial intrusion on the Internet, it has become increasingly obvious that service providers and Internet subscribers alone cannot stem the rising tide of junk e-mail. Contrary to past and present proposed federal legislation, the Can Spam Act survives both constitutional and legislative scrutiny by placing full discretion in the hands of Internet Service Providers, establishing strict civil and criminal penalties for violating posted policies and using SMTP banner messaging.[126]

A. Central Hudson Test

In order to pass constitutional muster, a restriction on commercial speech such as unsolicited e-mail must satisfy the *Central Hudson* test.[127] As stated by the Supreme Court, the test requires that where commercial speech is neither misleading nor promoting illegal activity, regulation is allowed if: (a) there is a substantial government interest at stake, (b) the restriction directly advances that interest, and (c) the restriction is narrowly tailored.[128] Moreover, the restriction need not employ the "least restrictive means" to accomplish its ends; the regulation must be narrow enough to have a "reasonable fit" between ends and means.[129] First, the primary interest at stake for the government is to curtail the cost-shifting from spammers to ISPs and ultimately to Internet subscribers as a whole, as well as to protect service providers'

126 Simple Mail Transfer Protocol. *Matisse's Glossary of Internet Terms* (visited Oct. 20, 1999) <http://www.matisse.net/files/glossary.html>.

127 Central Hudson Gas & Electric Corp. v. Public Service Commission, 447 U.S. 557 (1980).

128 *Id.* at 100 (finding that although a ban on all promotional advertising by electric utility directly served the substantial state interest in energy conservation, the Supreme Court invalidated the restriction because it was not sufficiently narrow).

129 Board of Trustees v. Fox, 492 U.S. 469 (1989).

rights to permit or restrict access to their proprietary equipment.[130] Second, the proposed restriction directly advances these interests by allowing ISPs, who are most affected by and most able to curtail spammers free-riding, to exercise full discretion in employing preventive measures. Finally, the Miller Bill is narrowly tailored enough to satisfy the third prong of the *Central Hudson* test. Unlike other congressional propositions which attempt to blindly filter all e-mail, the Can Spam Act focuses on solicitors who operated under forged domain names, and those who intentionally disregard service providers' policies against unsolicited commercial e-mail. Ultimately, the Miller Bill does not serve as a blanket restriction on the transmission of all e-mail, or even commercial e-mail, but instead focuses directly on fraudulent and unauthorized spam.

B. SMTP Banner Notification

The Can Spam Act as initially proposed by the Coalition Against Unsolicited Commercial E-mail (CAUCE), the Can Spam Act's proposed use of SMTP banner messaging is the first found in federal legislation.[131] As discussed above, the notification system would employ the SMTP banners already used between sender and recipient servers upon connection for e-mail transmission.[132] The Miller Bill suggests that when a connection is established and the recipient server transmits its initial greeting to the sender, providing notification that it is ready to receive mail, the recipient

---

130 HR 2162 §2 (b); *See generally,* Destination Ventures, Ltd. v. FCC, 46 F.3d 54 (1995) (finding that a ban on unsolicited commercial faxes served a substantial government interest in preventing the shift of advertising costs from solicitor to consumer because the regulation applied to commercial solicitations by any organization).

131 *CAUCE's 'SMTP Banner Notification Proposal'* (visited Oct.16, 1999) <http://www.cauce.org/proposal/index.html>.

132 Almost all e-mail servers employ SMTP as their main protocol. The protocol simply consists of a set of rules for how programs that send and receive mail should interact. *Matisse's Glossary of Internet Terms* at ¶ 14.

server would also transmit its policy on unsolicited commercial e-mail.[133]

The simplicity of the proposed SMTP notification has several advantages over other regulatory measures.[134] First, SMTP messaging already exists on all servers for both outgoing and incoming e-mail, and it is very easy for an ISP's mail system administrator to configure and monitor.[135] Second, unlike other bills, the system would take very little additional administrative cost to implement.[136] For example, both the Electronic Mailbox Protection Act and the Unsolicited Commercial Electronic Mail Choice Act of the 105th Congress proposed the compilation and maintenance of opt-out lists that could easily include millions of subscribers.[137] In contrast, the Can Spam Act only requires ISPs to modify a simple system that is already in place. Furthermore, organizations such as CAUCE provide free software to describe the process of checking banner messages and the ease of surveying and sorting mailing lists.[138] Third, a possible sender of UCE is instantly notified of the specific policy of each server through SMTP messaging.[139] This instantaneous notification is also beneficial to legitimate advertisers since no extensive research is necessary to uncover the specific policies of each ISP.[140] Fourth, there is no need for the legislature to create more rules for spam regulation than absolutely necessary in order to foreclose any loopholes that spammers could exploit. Because SMTP banners operate on their own well-defined and efficient protocol, the legislature need only defer to the service providers' identification procedures.[141] Finally, SMTP messaging suggested in the Miller

---

133 H.R. 2162 §2(d)(4)(C)(ii).

134 *CAUCE* ¶ 2.

135 *Id.*

136 *Id.*

137 Johnathan Byrne, *Squeezing the Spam Off the Net: Federal Regulation of Unsolicited Commercial E-Mail*, 2 W. VA J.L. & TECH. 4 (1998).

138 *CAUCE's Banner Notification Proposal* at 3.

139 *Id.* at 2.

140 *Id,*

141 *Id.*

Bill has the distinct advantage of having passed and operated extremely effectively in California as a state statute.[142]

Although banner notification has numerous advantages to other suggested programs, some minor hindrances do exist. The greatest inconvenience is that banner messaging requires all prospective advertisers to check the policy of every server it uses before contemplating transmission.[143] Another drawback is that delayed transmission could result in unintentional violations by senders of ISPs' spam policies, subjecting a well-meaning e-mail advertiser to fines of $500 per message.[144]

C. Improvements on Prior Legislation

The Can Spam Act also improves on former legislation that has failed in Congress, specifically the Netizen's Protection Act of 1997.[145] First, the Can Spam Act seeks to be a regulatory, not a prohibitive, measure. Unlike the Netizen's Protection Act, which sought to completely ban the transmission of all unsolicited commercial e-mail, the Miller Bill focuses on fraudulent and intentional abusers of e-mail systems. Second, the Miller Bill retains the valid return address and identification requirements, but unlike the Netizen's Act, makes their disregard criminally actionable, limited to one year of imprisonment.[146] Third, the Can Spam Act establishes stricter civil sanctions than prior proposed

---

142 *Id.*

143 *Id.* at 3.

144 *Id.*

145 H.R. 1748, 105th Con. (1997). The Act sought to extend the Telephone Consumer Protection Act of 1991 to include e-mail. The Bill would have made it unlawful for anyone to send an unsolicited advertisement to an e-mail address of a person with whom the sender: 1) lacked a preexisting and ongoing business or personal relationship, unless the individual provided express invitation or permission; or 2) unless the sender clearly provided, at the beginning of the advertisement the date and time of the message, the identity of the business, entity or individual sending the message, and the sender's return e-mail address. *Bill Summary and Status for the 105th Congress* (visited Oct.2, 1999) <http://thomas.loc.gov/cgi-bin/bdquery/z?d105:HR01748:@@@L>.

146 H.R. 2162 § 3.

legislation. Pursuant to the junk fax law discussed above, the Netizen's Protection Act allowed for a recovery of $500 per violation, with treble damages for intentional misconduct.[147] Comparatively, the Can Spam Act also allows for damage awards based on each item of junk e-mail, at a lower "per message" fine of fifty dollars, yet places a large daily limit of $25,000 per sender.[148] By merely imposing a fine of fifty dollars per use of an ISP's equipment, the Miller Bill takes into account that the cost per transmission to the recipient is lower than that of a facsimile or telephone call, and therefore the fine should not be as great. Yet, the Bill attempts not to merely be viewed by spammers as a cost of doing business thereby setting a significant ceiling of $25,000 per day.

D. Problems with the Inbox Privacy Act

A contemporaneous proposition in Congress to the Can Spam Act is the Inbox Privacy Act of 1999, co-sponsored by Senators Murkowski and Toricelli. Although this Bill is an improvement on prior legislation, several shortcomings still exist. First, the Bill takes discretionary power away from service providers and legislatively dictates how spam is treated.[149] As with any regulation, extensive congressional intervention raises constitutional issues and creates problems with compliance. Second, the Bill creates a loophole for "one-time" and "first-time" unsolicited advertisements.[150] Under this Bill, there would still be a myriad of spammers with access to all Internet subscribers addresses, irrespective of ISP policies. These small-time spammers would be immune from liability as long as they only send the exact same e-mail solicitation once. Third, as previously discussed, even though the implementation and maintenance of

147 *See supra* text and accompanying note 54.

148 H.R. 2162 § 2(c)(2)(B)(i).

149 S. 759 § 2(b), (c), (d).

150 *See, Id.*at (d)(2) Although the Toricelli Bill allows for "remove" options on all unsolicited commercial e-mail, recipients can request to be removed from future advertising only after the spammer has reached his intended target.

opt-out lists has improved, the incentive to seasonably maintain such a list presently does not exist.[151]

Although the use of the Federal Trade Commission to maintain and match such lists of each service provider's UCE policy and e-mail address domain names is admirable, in reality it would be exceedingly confusing. Arguably, merely compiling and maintaining a list of people who simply use electronic messaging, and with which service provider would be a Herculean task. Supplementing such a changing list on an Internet web page with individual ISP policies and their domain names as well as a list of all persons who have elected to be kept off junk e-mailing lists could easily include tens of millions.[152] Such a master list, even if maintained by the Federal Trade Commission, would be too confusing for prospective spammers to adequately comply.

Finally, the Toricelli Bill creates insurmountable problems for ISPs, and how they operate. By prohibiting service providers from collecting a fee for receiving unsolicited e-mail, no incentive exists to change from their original policy to that proposed by the Bill.[153] Essentially, by complying with the Inbox Privacy Act, ISPs would relinquish too many rights in order to advantage their subscribers. Although it intends to strictly control the transmission of spam by establishing numerous procedural guidelines for subscribers, ISP's, government agencies, and junk solicitors, the Inbox Privacy Act would create more problems than it would solve. Service providers who already have an efficient system for dealing with spam would be forced to fully comply with a federally mandated system that is less effective and much more confusing.

V. CONCLUSION

Although nearly all Internet Service Providers and e-mail users agree there is a need for legislative action to deal with spam, the correct form of such action is greatly disputed. It has become

151 *See supra* text accompanying notes 27-32.

152 S. 759 § 4 (c)(1).

153 S. 759 § 2 (c)(3)(B).

increasingly clear that self-help strategies such as anti-spam software and hardware, filtering, listing, and simply deleting have had little to no effect on the torrential proliferation of unsolicited commercial e-mail. Furthermore, based on numerous state initiatives to regulate spam, the need for universal federal legislation has shown itself to be overwhelming. Although individual state statutes have been mildly successful, they fail to completely deal with unsolicited commercial e-mail because of the inherent ubiquity of the Internet. Since the approaches, prohibitions and penalties vary greatly from state to state, service providers and suspected spammers can be regularly confused as to which law applies to whom and where. A simple solution to this problem is passage of one federal law that clearly outlines prohibited conduct and possible penalties therefor.

Passage of the Can Spam Act would be advantageous to all parties involved because it would place full control in the hands of service providers, who are the best equipped to combat spammers. The Act also cleverly allows for all parties affected by unsolicited commercial e-mail a cause of action as well as numerous choices of remedies. Also, by incorporating an SMTP banner messaging system, the Miller Bill employs an existing system of notification, while creating a novel and effective way to notify prospective junk e-mailers of UCE policies and penalties for violating them. The genius of banner messaging and the Can Spam Act can be found in its simplicity. The system does not incorporate large federal agencies or voluminous lists, but simply adheres to the theory of "caveat vendor."

Vasilios Toliopoulos