

Canning Spam: Developing Regulation of Commercial E-Mail in the U.S. and Around the World

By Andre R. Jaglom*

“Have you got anything without spam?”

“Well, there's spam egg sausage and spam, that's not got much spam in it.”

“I don't want ANY spam!”

MONTY PYTHON'S FLYING CIRCUS, “Spam,” Season 2, Episode 25 (1970)¹

I. Background

Unsolicited commercial e-mail, or spam, is a growing problem for consumers and businesses around the world. Estimates suggest that at present some 45% of all e-mail sent is spam, and that by 2007 this figure may increase to 70%.² Many feel the problem has already reached a critical level. The European Commissioner for Enterprise and the Information Society in July 2003 cited estimates that spam cost European business some €2.5 billion in 2002 and would comprise over 50% of global e-mail by the end of the summer.³ Panelists at a recent Federal Trade Commission Spam Forum overwhelmingly expressed the view that we are at a “tipping point,” where inaction could harm or even destroy e-mail as a productive tool for communication and commerce.⁴

While senders of spam incur almost no significant costs, spam imposes costs on users, who must spend time deleting dozens of unwanted messages daily. Spam imposes costs on businesses whose employees must spend similar time cleaning out inboxes, who expend

* Mr. Jaglom is a member of the New York City firm of Tannenbaum Helpert Syracuse & Hirschtritt LLP. © Andre R. Jaglom 2003. All rights reserved. For reprint permission contact jaglom@tanhelp.com

¹ “SPAM ® (Spiced Pork and Ham) in upper case letters is the registered trademark of Hormel Foods. The term ‘spam’ in lower case letters, and used in connection with [Unsolicited Bulk E-mail], derives from the sketch by the British comedy troupe Monty Python, in which a group of Vikings chant the word spam in a café whose breakfast menu is devoid of all else. See MONTY PYTHON'S FLYING CIRCUS, JUST THE WORDS, Vol. II at 27-29 (Methun, London 1989).” *Verizon Online Services, Inc. v. Ralsky*, 203 F.Supp.2d 601, 606 (E.D.Va. 2002); see also *CompuServe, Inc. v. Cyber Promotions, Inc.*, 962 F. Supp. 1015, 1018 n.1 (S.D. Ohio 1997) (term derived from a Monty Python skit “in which the word ‘spam’ is repeated to the point of absurdity in a restaurant menu”). As in the skit’s café, today’s e-mail cannot be obtained without spam, and like its Viking chorus, spam overwhelms everything else. For a history of spam and the origins of the word’s use in this context, see B. Templeton, “Origin of the Term ‘Spam’ to Mean Net Abuse,” <http://www.templetons.com/brad/spamterm.html>.

² A. Hesseldahl, “Cutting Spam Down to Size,” *Forbes.com* (June 4, 2003), http://forbes.com/2003/06/04/cx_ah_0604tentech.html.

³ Press Release, European Commission, “Spam: European Commission goes on the offensive,” DN: IP/03/1015 (July 15, 2003), http://europa.eu.int/rapid/start/cgi/guesten.ksh?p_action.gettxt=gt&doc=IP/03/1015|0|RAPID&lg=EN&display.

⁴ Prepared statements of the Federal Trade Commission on “Unsolicited Commercial E-mail” before the Committee on Energy and Commerce, Subcommittee on Commerce, Trade and Consumer Protection, Subcommittee on Telecommunications and the Internet, U.S. House of Representatives (July 9, 2003), <http://www.ftc.gov/os/2003/07/spamtest.htm> (hereinafter “FTC Testimony”).

resources to block spam and are forced to expand computer system resources to deal with higher mail volumes, and who may face liability for sexual harassment if they fail to prevent pornographic spam from reaching employees.⁵ And spam imposes costs on internet service providers (ISPs), whose system requirements are increased by the large volumes of spam traffic and who expend resources to protect their customers from unwanted spam. These burdens are exacerbated by spam directed to mobile telephones via text messaging and to other wireless devices, where bandwidth is more limited and the user's cost of receiving messages is higher.⁶

Moreover, spam often involves false claims, deception and fraud. A recent FTC report⁷ found that 33% of spam contained false information regarding the sender, 22% contained false information in the subject line, 40% had "indications of falsity" in the message body, and 66% had at least one of these deceptive features. Indeed the proliferation of spam has raised enough legal issues for at least one U.S. law school, John Marshall Law School in Chicago, to offer a course devoted entirely to spam, with a curriculum including litigation, legislation, application of tort principles to spam, issues of constitutionality, extraterritoriality, jurisdiction and privacy, among others.⁸

Given the burdens, costs and liabilities associated with unsolicited commercial e-mail, it is no surprise that businesses and individuals have tried both technological and legal approaches to the problem, and that legislators and regulators have begun to address the issues associated with spam.

Technical solutions include sophisticated filtering and blocking software (which carry with them the potential costs of false positives, where legitimate e-mails are not delivered because the software erroneously classifies them as spam) and⁹ systems in which e-mails received from an unknown sender is rejected until the sender responds to a challenge e-mail requiring human intervention, which establishes that the sender is an individual (to which spammers generally will not take the time to respond, even if the sender's address is legitimate and the request for confirmation reaches the spammer).¹⁰ Major ISPs have joined forces to try to reduce the amount of spam originating on their systems or received by their users.¹¹

⁵ See "United States: Pornographic Spam Has Potential to Create Hostile Work Environment, WORLD INTERNET L. REP. (BNA) (May 2003) at 23 (failure to block or filter pornographic spam after employee complaints may result in employee liability; issue may be degree of employer control). The author is aware of at least one such claim that is pending.

⁶ See A. Hesseldahl, "Hanging Up On Wireless Spam," Forbes.com (June 4, 2003), http://www.forbes.com/home/2003/06/04/cx_aw_0604spam.html.

⁷ FTC Division of Marketing Practices, Bureau of Consumer Protection "False Claims in Spam" (April 30, 2003), <http://www.ftc.gov/reports/spam/030429spamreport.pdf>.

⁸ P. Festa, "Law School Serves Spam as Main Course," CNet News.com (June 2, 2003), http://news.com.com/2102-1028_3-1012404.html?tag=ni_print. For course syllabus, reading materials and other information, see <http://www.spamseminar.com>.

⁹ E.g. J. Udell "SpamBayes Knows Spam," INFO WORLD (May 16, 2003), http://www.infoworld.com/article/03/05/16/20TCspam_1.html; A. Hesseldahl, "Cutting Spam Down to Size," Forbes.com (June 4, 2003), http://www.forbes.com/2003/06/04/cx_ah_0604tentech.html.

¹⁰ See, e.g., <http://www.digiportal.com/support/choicemail/faq.html>.

¹¹ T. Krazit, "AOL, Microsoft, Yahoo Align to Fight Spam," INFO WORLD (April 28, 2003), http://www.infoworld.com/article/03/04/28/HNfightspam_1.html.

More complicated are potential changes to the Simple Mail Transfer Protocol (SMTP) governing e-mail that would facilitate identifying spam by such means as establishing that the sender's IP address does not match the domain name on the e-mail, thus preventing a typical spammer's trick of "spoofing," or forging, the "From" field in his e-mail.¹² Such changes to SMTP would face serious obstacles, as they would involve agreement on a new standard mail protocol, followed by universal implementation on every server in the world.¹³ Others have proposed using encrypted digital signatures to empower users to determine from whom they will accept e-mails, a solution that would require widespread adoption of digital signatures, incorporated into e-mail software, with methods for approving strangers from whom e-mail may be desired.¹⁴

Legal solutions fall into several categories. Traditional legal principles, such as trespass, fraud, breach of contract and others, have been used in litigation against spammers, with mixed results. A number of states have created anti-spam laws of various kinds. Congress currently is considering several anti-spam bills. And other countries, especially in Europe, are trying to address the problem. We will consider each of these in turn.

II. Applying Traditional Legal Principles to Spam

Victims of spam, both recipients and internet service providers ("ISPs") have taken legal action against spammers, with mixed results, under a variety of traditional legal theories, including trespass to chattels, fraud and deceptive practices, trademark infringement and dilution, false designation of origin and breach of contract. Courts have awarded injunctive relief, compensatory damages and punitive damages against spammers.¹⁵ In all cases, however, it is important to bear in mind two fundamental obstacles to an effective legal remedy against spammers, which explain the continued growth of the problem. First, it is often difficult, if not impossible to identify, locate and obtain jurisdiction over the spammer¹⁶; and second, often the spammer is found to be without substantial assets, so that damages awards amount to an empty victory. These problems may well explain the lack of interest by the class action bar in pursuing

¹² M. Harper, "The Grand United Theory of Spam," *Forbes.com* (June 5, 2003), http://www.forbes.com/2003/06/05/cx_mh_0605spam_print.html.

¹³ See T. Tompkins and D. Handley, "Giving E-mail Back to the Users: Using Digital Signatures to Salute the Spam Problem" *FirstMonday* (Aug. 7, 2003), http://www.firstmonday.dk/issues/current_issue//tompkins/.

¹⁴ *Id.*

¹⁵ *E.g.*, *EarthLink Inc. v. Carmack*, No. 1:02-CV-3041 (N.D.Ga. May 7, 2003) (awarding \$16.4 million judgment against spammer, not dischargeable in bankruptcy) reported in "ISP Wins \$16.4 Million Judgment Against Spammer," *WORLD INTERNET L. REP.* (BNA) (May 2003) at 21; *America Online, Inc. v. Prime Data Systems Inc.*, 1998 WL 34016692 (E.D. Va. 1998) (default judgment enjoining spammer, *inter alia*, from transmitting e-mail to AOL or its members, using return addresses containing "aol.com," and awarding compensatory damages of \$.00078 per message, or \$101,400 for 130 million messages, and punitive damages of \$304,200, or \$.00234 per message).

¹⁶ See for example, the saga of EarthLink's ultimately successful, but time-consuming and expensive, efforts to track down the "Buffalo spammer." Angwin J., "Hunting 'Buffalo' – Elusive Spammer Sends Web Service on a Long Chase – Earthlink Uses Lawyers, Private Eyes to Track Sender of Online Junk," *Wall Street Journal* p. 1 (May 7, 2003); J. Angwin, "How Ruthless Youngblood Cracked An Elusive Spammer," *smh.com.au* (May 13, 2003), <http://www.smh.com.au/articles/2003/05/12/1052591724113.html>.

spam cases. They also explain Professor Lawrence Lessig's proposal to pay a bounty to private citizens who identify spammers.¹⁷

A. *Trespass to Chattels*

Among the most frequent claims asserted against bulk e-mailers is the venerable common law tort of trespass to chattels – essentially the unauthorized use of personal property:

“there may be recovery . . . for interferences with the possession of chattels which are not sufficiently important to be classed as conversion, and so to compel the defendant to pay the full value of the thing with which he has interfered. Trespass to chattels survives today, in other words, largely as a little brother of conversion.”¹⁸

The transmission of electronic signals through a computer network has been held to be sufficiently physical contact to constitute trespass to property.¹⁹ However, this concept was refined by the court in *Ticketmaster Corp. v. Tickets.com, Inc.*, which stated that for a signal from one computer server to another to constitute actionable trespass, there must be physical harm to the chattel or some obstruction of its basic function.²⁰ Some courts have held that harm may be proved by demonstrating that an unauthorized user occupies system capacity on the victim's website, regardless of whether there is physical damage.²¹

Thus, a number of courts have held that the burdens imposed on an ISP's resources by unsolicited bulk e-mail, to the extent that these resources are unavailable or less available to the ISP's customers, is sufficient to establish trespass, even in the absence of physical damage, at least where the plaintiff has tried unsuccessfully to use reasonable technological means to protect its systems.²²

The use of this theory by spam recipients, however, was struck a serious blow in June 2003, when the Supreme Court of California, by 4-3 vote, reversed a lower court decision in favor of Intel Corp. against a former employee, Kourosh Kenneth Hamidi, who had flooded its systems with e-mails critical of Intel sent to thousands of Intel employees.²³ The California Supreme Court held that without damage to, or impaired functionality of, Intel's computer

¹⁷ L. Lessig, “A Bounty on Spammers,” Ziff-Davis CIO Insight (Sept. 16, 2002), <http://www.cioinsight.com/article2/0,3959,533225,00.asp>.

¹⁸ *Prosser & Keeton, Prosser and Keeton on Torts*, §14, 85-86 (1984), quoted in *CompuServe, Inc. v. Cyber Promotions, Inc.*, 962 F. Supp. 1015, 1020 (S.D. Ohio 1997).

¹⁹ *America Online Inc. v. LGCM*, 46 F. Supp. 2d 444, 452 (E.D. Va. 1998); *Thrifty-Tel, Inc. v. Bezenek*, 54 Cal Rptr. 2d 468 (Ct. App. 1996).

²⁰ *Ticketmaster Corp. v. Tickets.com, Inc.*, 2000 WL 1887522, No. 99 CV7654, *4 (C.D. Cal. Aug. 10, 2000).

²¹ *Register.com, Inc. v. Verio, Inc.*, 126 F. Supp. 2d 238, 250 (S.D.N.Y. 2000), citing *eBay, Inc. v. Bidder's Edge, Inc.*, 100 F. Supp. 2d 1058, 1071 (N.D. Cal. 2000).

²² *CompuServe, Inc. v. Cyber Promotions, Inc.*, 962 F. Supp. 1015, 1021-24 (S.D. Ohio 1997). See *America Online, Inc. v. LCGM, Inc.*, 46 F. Supp. 2d 444 (E.D. Va. 1998); *America Online, Inc. v. IMS*, 24 F. Supp. 2d 548, 550-51 (E.D. Va. 1998); see also *Hotmail Corp. v. Van\$ Money Pie Inc.*, 47 U.S.P.Q. 2d 1020 (N.D. Cal. 1998) (finding likelihood of success on trespass claim against spammer); *America Online, Inc. v. Prime Data Systems Inc.*, 1998 WL 34016692 (E.D. Va. 1998).

²³ *Intel Corp. v. Hamidi*, 1 Cal Rptr. 3d 32, 30 Cal. 4th 1342, 71 P.3d 296 (2003).

systems, a trespass claim was not established, because there was no interference with Intel's use or possession of, or other legally protected interest in, the personal property itself.²⁴

The Court took pains to distinguish cases in which ISPs had prevailed against spammers "based upon evidence that the vast quantities of e-mail sent by spammers both overburdened the ISP's own computers and made the entire computer system harder to use for recipients, the ISP's customers." In those cases, the quantity of e-mail impaired the functioning of the ISPs' computer systems, while Intel claimed injury from the distraction caused to recipient employees by the contents of the e-mail, "an injury entirely separate from, and not directly affecting, the possession or value of personal property."²⁵ Hamidi's thousands of copies of six separate messages – some 200,000 e-mails in all – were contrasted with the tens of millions of messages in ISP trespass cases.²⁶

The California Supreme Court's decision has been criticized, not only in two vigorous dissenting opinions,²⁷ but by Congressman Christopher Cox (R-CA), who called it a "most peculiar ruling that needs legislative correction" and promised to introduce such legislation.²⁸

Until then, trespass may be a weapon reserved for ISPs, who are more likely than users to face a sufficient volume of spam to meet the California Supreme Court's test of impaired functionality.

B. *Fraud and Deceptive Practices*

The common use in spam of false header information, false "From" lines, false and misleading subject lines and deceptive content, has led to successful actions against spammers under various fraud theories.

Thus, the New York Attorney General brought a successful consumer fraud action against a spammer who sold magazine subscriptions using falsified sender information, failed to deliver promised magazines or to honor money back guarantees and used fictitious testimonials.²⁹ The SEC has pursued spammers who promoted stocks by bulk e-mail using fictitious names without disclosing relationships with issuers.³⁰ Private fraud actions against spammers have been brought by ISPs, but without reported decisions as yet.

²⁴ *Id.* at 36.

²⁵ *Id.* at 37.

²⁶ *Id.* at 44.

²⁷ *Id.* at 52-67 (Brown, J., dissenting), 67-75 (Mosk, J., dissenting).

²⁸ D. McCullagh, "Lawmaker Slams Bulk E-mail Ruling," CNETnews.com (July 9, 2003), http://news.com.com/2102-1028_3-1024339.html.

²⁹ *People v. Lipsitz*, 174 Misc. 2d 571, 663 N.Y.S. 2d 468 (N.Y.Co. 1997).

³⁰ *SEC v. Tribble*, Civil Action N. 98-8699 (RVX) (C.D. Cal. Oct. 27, 1998) (consent judgment), Litigation Release No. 15959 (Oct. 27, 1998), <http://www.sec.gov/litigation/litreleases/lr15959.txt>; see also "SEC Conducts First Ever Nationwide Internet Securities Fraud Sweep, Charges 44 Stock Promoters in 23 Enforcement Actions; Purveyors of Fraudulent Spam, Online Newsletters, Message Board Postings, and Web Sites Caught in Effort to Clean Up the Internet," <http://www.sec.gov/news/press/pressarchive/1998/98-117.txt>.

C. Trademark Claims

Related to claims of fraud and deception are trademark-related claims, including not only trademark infringement, but false designation of origin under the Lanham Act and trademark dilution.

Thus, for example, the owner of the “CARS.com” registered service mark succeeded in trademark infringement and trademark dilution claims against a spammer that sent pornographic spam with stione@cars.com as a false return address.³¹ Infringement was established by showing the use of “cars.com” for services the Court found were “related” to the plaintiff’s mark by reason of the overlap between the recipients of the spam and the target market of the plaintiff, such that consumers were likely to attribute the spam and the plaintiff’s “CARS.com” service mark to a single source.³² The court also found that the “CARS.com” mark was famous and that its “capacity . . . to identify and distinguish goods or services” was lessened, so that dilution under the federal trademark dilution statute³³ was made out.³⁴

Similar conclusions were reached in an action brought by Hotmail Corp. against a spammer that provided false return addresses using Hotmail’s domain name, where the court found a likelihood of success on false designation of origin under the Lanham Act³⁵ and federal and state dilution claims.³⁶

D. Breach of Contract

Where spammers obtain e-mail accounts from ISPs and use them to send unsolicited bulk commercial e-mail in violation of the ISPs’ terms of service, a breach of contract claim is available. Such a claim was found likely to succeed, and a preliminary injunction was issued, where a spammer used Hotmail accounts to send spam, which Hotmail’s terms of service prohibited.³⁷

E. Other Claims

ISPs have actively pursued spammers under the above theories and others. AOL, for example, has posted on its legal web site numerous complaints asserting a myriad of claims against spammers, which provide a useful compendium of potential claims.³⁸ In addition, claims have been asserted successfully under state and federal statutes, discussed below.

³¹ *Classified Ventures, L.L.C. v. Softcell Marketing, Inc.*, 109 F. Supp. 2d 898 (N.D. Ill. 2000).

³² *Id.* at 900.

³³ 15 U.S.C. §§ 1125(c), 1127.

³⁴ *Classified Ventures, L.L.C. v. Softcell Marketing, Inc.*, 109 F. Supp. 2d 898, 900-01 (N.D. Ill. 2000).

³⁵ *Hotmail Corp. v. Van\$ Money Pie Inc.*, 47 U.S.P.Q. 2d 1020, 1023-24 (N.D. Cal 1998); *see also America Online, Inc. v. LCGM, Inc.*, 46 F. Supp. 2d 444, 449-50 (E.D. Va. 1998); *America Online, Inc. v. IMS*, 24 F. Supp. 2d 548, 551 (E.D. Va. 1998); *America Online, Inc. v. Prime Data Systems Inc*, 1998 WL 34016692 (E.D. Va. 1998).

³⁶ 15 U.S.C. §§ 1125(a).

³⁷ *Hotmail Corp. v. Van\$ Money Pie Inc.*, 47 U.S.P.Q. 2d 1020 (N.D. Cal. 1998).

³⁸ *E.g., America Online, Inc. v. Byte Night, LLC*, No. 03-465-A (E.D.Va.) (complaint filed April 11, 2003) and others available at <http://legal.web.aol.com>

F. *Claims by Spammers*

It is worth noting that litigation has been brought in the other direction by spammers against ISPs, seeking to preserve their right to send spam. The courts have generally been less than sympathetic. Thus a spammer's claim of a First Amendment right to send bulk e-mail and attempt to prevent an ISP from blocking his spam was unsuccessful,³⁹ as were another spammer's counterclaims that an ISP was a common carrier and could not discriminate against bulk commercial e-mail, that the ISP's efforts to block spam constituted an antitrust violation, and that those efforts constituted tortious interference with the spammer's relationship with its customers.⁴⁰

A spammer whose internet access was terminated by its ISP without a contractually required notice period of thirty days did, however succeed in obtaining a preliminary injunction temporarily restoring access.⁴¹

III. **State Anti-Spam Laws**

As of August 2003, at least 35 states had enacted laws regulating spam.⁴² Others are under consideration.⁴³ The statutes vary in nature. Often they require an indication in the subject line that the e-mail contains advertising, usually by requiring that the subject line begin with "ADV" or "ADV:ADULT," require a method for opting out of further messages, and prohibit falsified routing information and false or deceptive subject lines.⁴⁴

Other state laws go much further. Delaware makes it criminal to send unsolicited bulk commercial e-mail to recipients located in Delaware with whom the sender has no pre-existing business relationship if the sender knows the recipient's presence in the state is a reasonable possibility, or to fail promptly to stop sending unsolicited commercial e-mail after being requested to do so.⁴⁵ Virginia makes the sending of unsolicited bulk e-mail with falsified header information in violation of an ISP's policies a felony if more than specified numbers of messages are sent in any given 24-hour, 30-day or one-year period.⁴⁶

Other features of various state laws include:

- A prohibition on deceptive subject lines designed to evade spam-altering software.
- A prohibition on sending e-mail in violation of an ISP's policies.

³⁹ *Cyber Promotions, Inc. v. America Online, Inc.*, 948 F. Supp. 436 (E.D. Pa. 1996).

⁴⁰ *America Online, Inc. v. Greatdeals.net*, 49 F. Supp. 2d 851 (E.D. Va. 1999).

⁴¹ *Cyber Promotions, Inc. v. Apex Global Information Services, Inc.*, 1997 WL 634384 (E.D. Pa. 1997).

⁴² See e.g., Cal. Bus. Profs. Code §17538.4; Colo. Rev. Stat. §6-2.5-101; Idaho Code §48-603E; 815 Ill. Comp. Stat. 511; Iowa Code §§714E.1-2; Nev. Rev. Stat. Ann. §§41.705-.735; R.I. Gen. Laws, §11-52-1; Tenn. Code Ann. §§47-18-1602, -2501; Va. Code §§ 18.2-152.2, -152.3:1, 152.4, -152.12 and -152.16; Wash. Rev. Code, tit. 19, Chap. 19.190.

⁴³ E.g. California SB12, which would outlaw spam and provide consumers a right to sue spammers for \$500 per unwanted e-mail, which has passed the California Senate and awaits action by the Assembly. *Text of bill available at* http://info.sen.ca.gov/pub/bill/sen/sb_0001-0050/sb_12_bill_20030626_amended_asm.html.

⁴⁴ E.g. Tex. Stat., tit. 4, §46,003.

⁴⁵ Del. Code Ann., tit. 11, §§937, 938.

⁴⁶ Va. Code §18.2:152.3:1.

- A requirement that the sender be identified, often with a physical address or telephone number.
- A requirement for a functioning reply feature.
- A requirement for an opt-out method that is honored.

Some state laws provide a private right of action for violations, with statutory penalties per violation, leading to claims ranging from one for \$80 against Elizabeth Dole’s North Carolina Senate campaign for eight violations of that state’s anti-spam law⁴⁷ to one by law firm Morrison & Foerster against Etracks, an e-mail marketing company, for \$50 per e-mail received, up to \$25,000 per day, for 6,500 unsolicited e-mails received by its employees in violation of California anti-spam laws.⁴⁸

Current summaries and the full text of state spam laws can be found at <http://www.spamlaws.com/state/index.html>.

In addition, ISPs have successfully sued spammers under state laws. For example, Virginia’s Computer Crimes Act provides that “[a]ny person who uses a computer or computer network without authority and with the intent to [c]onvert the property of another shall be guilty of the crime of computer fraud” and authorizes a private right of action for violations.⁴⁹ AOL has successfully claimed that sending spam with “aol.com” headers through AOL’s computer network was unauthorized, that the spammers intended to obtain services by false pretenses, obtained the unauthorized service of AOL’s mail system, and obtained free advertising from AOL by shifting the cost of the e-mails to AOL, and that therefore the Virginia statute had been violated.⁵⁰

A few state laws have been struck down as unconstitutional on commerce clause grounds,⁵¹ where courts have found them to regulate conduct occurring entirely outside the state and determined that the burden on interstate commerce outweighed the local benefit.⁵² In other cases, however, where a statute is limited to apply to spam sent from the state, to a resident of the state, or by means of equipment located in the state, they have been upheld.⁵³ Courts have found the statutes to provide benefits that outweigh any burden, noting the costs and burdens imposed on ISPs and users by spam, and the lack of any appreciable burden on spammers from requirements of truthfulness, disclosure and opt-out rights.⁵⁴

⁴⁷ See <http://www.cbsnews.com/stories/2002/10/09/national/main524957.shtml>.

⁴⁸ See <http://www.siliconvalley.com/mld/siliconvalley/news/local/2861505.html>.

⁴⁹ Va. Code § 18.2-152.3(3), -152.12

⁵⁰ *America Online, Inc. v. LCGM, Inc.*, 46 F. Supp. 2d 444, 451 D. (E.D. Va. 1998).

⁵¹ See e.g., *American Libraries Ass’n v. Pataki*, 969 F. Supp. 160, 169 (S.D.N.Y. 1997). See also discussion in Carl Kaplan, *In Spam Case, Another Defeat for State Internet Laws*, reported in *Cyber L.J.*, Mar. 24, 2000 (New York, Michigan and New Mexico anti-spam laws have been struck down either in state or federal court for violating the commerce clause of the U.S. Constitution).

⁵² E.g., *American Library Ass’n v. Pataki*, 969 F.Supp. 160, 169 (S.D.N.Y. 1997).

⁵³ E.g., *State v. Heckel*, 143 Wash.2d 824, 24 P.3d 404 (2001); *Ferguson v. Friendfighters, Inc.*, 94 Cal. App. 4th 1255, 115 Cal. Rptr. 2d 258 (Cal. App. 1st Dist. 2002).

⁵⁴ *Id.*

IV. Federal Anti-Spam Regulation

On the federal front, there is no U.S. legislation yet in effect directly regulating spam. ISPs have however, successfully used the Computer Fraud and Abuse Act⁵⁵ against spammers. The Act has several provisions relevant to the activities of spammers. Under the Act any person who:

(i) “intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from a protected computer if the conduct involved an interstate or foreign communication,”⁵⁶

(ii) “knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than \$5,000 in any 1-year period;”⁵⁷

(iii) “knowingly causes the transmission of a program, information, code or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;”⁵⁸

(iv) “intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage;”⁵⁹ or

(v) “intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage;”⁶⁰

is punishable by fines and imprisonment⁶¹ and subject to a private civil action by anyone “who suffers damage or loss by reason of a violation” of the Act.⁶²

The use by spammers of falsified return addresses using an ISP’s domain has been held to violate the Act. The practice was found to result in customer complaints, replies and “bounced back” messages being sent to the ISP rather than to the spammer, causing risks to the ISP’s computer system and online service, including risks that the ISP “would be forced to withhold or delay the use of computer services to its legitimate subscribers,” causing damage to the ISP.⁶³

Similarly, maintaining an account with an ISP and extracting e-mail addresses from other ISP customers in violation of the ISP’s terms of service amounted to unauthorized access and

⁵⁵ 18 U.S.C. §1030.

⁵⁶ 18 U.S.C. §1030(a)(2) (C).

⁵⁷ 18 U.S.C. §1030(a)(4).

⁵⁸ 18 U.S.C. §1030(a)(5)(A).

⁵⁹ 18 U.S.C. §1030(a)(5)(B).

⁶⁰ 18 U.S.C. §1030(a)(5)(C).

⁶¹ 18 U.S.C. §1030(c).

⁶² 18 U.S.C. §1030(g).

⁶³ *Hotmail Corp. v. Van\$ Money Pie Inc.*, 47 U.S.P.Q. 2d 1021, 1023-24 (N.D. Cal 1998);

obtaining of information from a protected computer, resulting in damages to the ISP, and so violated the Computer Fraud and Abuse Act.⁶⁴

In addition, despite the lack of a specific federal statute directed at spam, the Federal Trade Commission has taken action against deceptive spammers under its authority to regulate deceptive and unfair practices.

As of July 9, 2003 the FTC had brought 54 cases in which spam was an integral element of the alleged deception or unfair practice, including deceptive content, misleading subject lines, spoofing of "From:" lines, and failure to honor a "remove me" request.⁶⁵ It also joined with other federal agencies, U.S. Attorneys and state attorneys general and regulatory agencies in May 2003 to bring 45 criminal and civil actions against Internet scams, including five federal court actions that resulted in preliminary or final injunctions shutting down the operations.⁶⁶

The FTC has urged a combination of technology, education, legislation and enforcement to address the spam problem, and notes that the principal enforcement challenge is to identify and locate the spammer. Doing so requires an extraordinary commitment of resources, without advance knowledge of whether the target's operation is significant enough to justify the commitment, or even whether the spammer is subject to jurisdiction in the U.S. or in a state seeking to take enforcement action.⁶⁷ It observed that the path of an e-mail from spammer to consumer frequently crosses international borders, and legislation could assist the FTC in working with international law enforcement agencies.

In particular, the FTC sought legislation to allow it to obtain court orders to prevent recipients of civil investigative demands from notifying targets that the FTC is investigating, as required in some circumstances by some federal privacy legislation. It also seeks the ability to obtain from internet service providers complaints received about their subscribers, and to have hackers and spammers who hijack a legitimate customer's account be deemed an "unauthorized

⁶⁴ *America Online, Inc. v. LCGM, Inc.*, 46 F. Supp. 2d 444, 450-451 (E.D. Va. 1998).

⁶⁵ *FTC Testimony, supra* (citing *FTC v. Westby*, No. 032-3030 (N.D. Ill. filed April 15, 2003); *FTC v. 30 Minute Mortgage, Inc.*, No. 03-60021 (S.D. Fla. filed Jan. 9, 2003); *FTC v. G.M. Funding*, No. SACV 02-1026 DOC (C.D. Cal. filed Nov. 2002).

⁶⁶ *FTC Testimony, supra* (citing *FTC v. Evans*, No. 4:03 CV178 (E.D. Tex.) (complaint and stipulated final judgment filed May 9, 2003) and *FTC v. Benson*, No. 03CV0951 (N.D. Tex.) (complaint and stipulated final judgment filed May 6, 2003), both available at <http://www.ftc.gov/opa/2003/05/swnetforce.htm>; *FTC v. Cella*, Nos. CV-03-3202 (C.D. Cal.) (complaint filed May 7, 2003), available at <http://www.ftc.gov/os/2003/05/patrickcellacmp.pdf>; *FTC v. K4 Global Publishing, Inc.*, No. 5:03-cv0140-3 (M.D. Ga.) (complaint filed May 7, 2003), available at <http://www.ftc.gov/os/2003/05/k4globalcmp.pdf>; *FTC v. Clickformail.com, Inc.*, No. 03-c-3033 (N.D. Ill.) (complaint filed May 7, 2003), available at <http://www.ftc.gov/os/2003/05/clickformailcmp.pdf>.

⁶⁷ *FTC Testimony, supra*. Issues of jurisdiction and choice of law are beyond the scope of this paper. For a discussion of these issues in an internet context, see A.R. Jaglom, "Liability On-Line: Choice of Law and Jurisdiction on the Internet, or Who's In Charge Here?" (2002), <http://www.tanhelp.com/newsworthy/Articles/LiabilityOn-Line.pdf>.

user” not entitled to protection afforded to “customers” under the Electronic Communications Privacy Act.⁶⁸

In addition, the FTC sought legislative authority to adopt rules addressing deceptive and abusive practices with respect to spam, modeled on the Telemarketing and Consumer Fraud and Abuse Protection Act.⁶⁹ It urged that any legislation include rulemaking authority to address deceptive spam practices, without a need to show intent or knowledge (the same standard of liability now in place under Section 5 of the FTC Act) and with enforcement authority in both the FTC and the states. It also noted the need for consistency between state and federal laws, and suggested consideration of criminalization of false header and routing information.⁷⁰

FTC Chairman Timothy Muris has noted that the ability of spammers easily to hide their identities and to cross international borders, combined with the fact that recipients and ISPs, not spammers, bear virtually all of the costs of spam, mean that normal market forces cannot solve the problem and government intervention is needed. He urged that legislation address how to locate and prosecute spammers and deal with adequate punishment, including criminal authority so there will be a viable deterrent when spammers have no assets or potential civil penalties are inadequate to reduce the financial incentive to spam.⁷¹

While no such legislation has yet been enacted, Congress is considering several bills specifically addressing the spam problem. In general these bills would apply to unsolicited commercial e-mail sent to recipients with whom the sender has no prior business relationship. Summaries and texts of pending federal legislation are available at <http://spamlaws.com/federal/index.html>.

On the Senate side, the leading bills sponsors and key provisions include:

- S.877 –Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM Act of 2003) (Burns, R-MT; Wyden D-OR)
 - Unsolicited commercial e-mail must be labeled
 - Opt-out instructions required
 - Sender’s physical address must be included
 - Deceptive subject lines and false headers prohibited
 - State laws *prohibiting* spam would be preempted
- S.1293 – The Criminal Spam Act of 2003 (Hatch, R-UT)
 - Prohibits unauthorized or deceptive use of third party computers to relay spam

⁶⁸ *Id.*

⁶⁹ 15 U.S.C. §§6101-6108.

⁷⁰ *FTC Testimony, supra.*

⁷¹ Remarks of Timothy J. Muris, “The Federal Trade Commission and the Future Development of U.S. Consumer Protection Policy,” Aspen Summit, Cyberspace and the American Dream (Aug. 19, 2003), <http://www.ftc.gov/speeches/muris/030819aspen.htm> (hereafter, “*Muris Aspen Speech*”).

- Prohibits false headers in bulk commercial messages
- Regulates use of multiple e-mail accounts or domain names to send spam
- Applies to more than 100 messages within 24 hours, 1,000 within 30 days or 10,000 within a year
- S.1231 – Stop Pornography and Abusive Marketing Act (SPAM Act) (Schumer, D-NY)
 - Establishes national do-not-spam list administered by FTC
 - Authorizes FTC to bar explicit commercial messages to minors even if not on list
 - Unsolicited commercial messages must have “ADV:” at start of subject line
 - Prohibits commercial e-mail sent in violation of an internet service provider’s policies
 - Prohibits false or misleading subject lines or headers
 - Prohibits sending to addresses harvested from web pages
 - Requires inclusion of sender’s physical address
- S.1052 – Ban on Deceptive Unsolicited Bulk E-Mail Act of 2003 (Nelson, D-FL)
 - Prohibits false message headers in unsolicited bulk commercial e-mail
 - Requires opt-out instructions and honoring opt-out requests
 - Prohibits harvesting e-mail addresses for web pages and other services
 - Violators can be prosecuted under RICO.
- S.563 – Computer Owners’ Bill of Rights (Dayton, D-MN)
 - Requires FTC to establish a “do-not-e-mail” registry, with authority to impose civil penalties for sending unsolicited commercial e-mails to listed addresses

A variety of similar bills has been introduced on the House side:

- H.R.2515 – Anti-Spam Act of 2003 (Wilson, R-NM; Boucher, D-VA; Markey, D-MA)
 - Commercial e-mail must be identified as such
 - Sender’s physical address must be included
 - An opt-out message must be included
 - Prohibits false or misleading message headers and subject lines
 - Prohibits sending to addresses generated by automated dictionary attack

- H.R.2214 – Reduction in Distribution of Spam Act of 2003 (RID-Spam Act) (Burr, R-NC; Tauzin, R-VA; Sensenbrenner, R-WI)
 - Commercial e-mail must be identified as such
 - Sender’s physical address must be included
 - Opt-out method must be included
 - Prohibits false or misleading headers
 - Preempts state laws restricting sending of commercial e-mail, regulating opt-out procedures, or requiring subject labels; state laws regulating false message headers remain in affect
- H.R.1933 – Restrict and Eliminate the Delivery of Unsolicited Commercial E-mail or Spam Act of 2003 (REDUCE Spam Act) (Lofgren, D-CA)
 - Requires valid reply address
 - Requires opt-out instructions
 - Requires “ADV:” or “ADV:ADULT” subject label
 - Applies to messages sent in quantities of 1,000 or more in a two-day period
 - Prohibits false or misleading message headers in all unsolicited commercial e-mails regardless of quantity
- H.R.122 – Wireless Telephone Spam Protection Act (Holt, D-NJ)
 - Prohibits used wireless messaging systems to send unsolicited advertisements

What, if any, federal legislation will ultimately be enacted is unclear at the moment. The CAN-SPAM Act (S.877) was approved by the Senate Commerce Committee on June 19, 2003.⁷² The Commerce Committee also approved the FTC request for authority to bypass disclosure requirements under the Right to Financial Privacy Act and the Electronic Communications Privacy Act,⁷³ but there has been no further action. Widespread early support for Congressional action⁷⁴ has moderated, with questions being raised as to what approach to take and whether legislative action is needed.⁷⁵

While the dramatic success of the FTC’s “do not call” list, implemented in June 2003, when an average of a million phone numbers a day were registered to avoid telemarketing

⁷² R. Mark, “Senate Panel Overwhelmingly Passes Anti-Spam Bill,” <http://dc.internet.com/news/print.php/2224681>.

⁷³ *Id.*

⁷⁴ J. Lee, “Congress Finds Rare Unity in Spam, to a Point,” N.Y. TIMES (June 23, 2003), <http://www.nytimes.com/2003/06/23/technology/23SPAM.html>.

⁷⁵ *See, e.g.*, S. Hansell, “The Bandwagon to Fight Spam Hits a Bump,” N.Y. TIMES (Aug. 11, 2003), <http://www.nytimes.com/2003/08/11/technology/11SPAM.html>; L. McKinney, “Antispam Legislation Hits Rocky Road,” PCWORLD.COM (July 8, 2003), <http://www.pcworld.com/news/article/0,aid,111487,00.asp>.

phone calls,⁷⁶ led to the Congressional bills calling for a similar “do not spam” registry, the FTC has expressed skepticism for this approach. In testimony before the House Committee on Energy and Commerce in July 2003, Harold Beales, Director of the FTC’s Consumer Protection Bureau, supported legislation to bar false headers and harvesting of e-mail addresses from websites, and to require simple opt-out methods. He expressed the view that a “do not spam” registry was impractical, given the difficulty of identifying scofflaw spammers and the risk that unscrupulous spammers would use the list as a source of valid addresses.⁷⁷ More recently, FTC Chairman Timothy Muris expressed similar views, noting the illegitimacy of spammers and the difficulty of identifying them, and concluding, “There is no basis to conclude that a Do Not Spam list would be enforceable or produce any noticeable reduction in spam.”⁷⁸

Another concern has been expressed by state attorneys general opposed to federal preemption of stronger state laws, including those permitting private rights of action against spammers.⁷⁹ What legislation will actually emerge from the process is thus very much up in the air. It is worth noting that any legislation that is enacted is likely to withstand constitutional challenge. The analogous Telephone Consumer Privacy Act of 1991,⁸⁰ which prohibits unsolicited commercial faxes, withstood a First Amendment challenge when the Court found a substantial governmental interest in preventing unwanted fax advertising from shifting costs to unwilling consumers.⁸¹ This justification applies with even greater force to spam, where unwilling consumers and ISPs bear virtually the entire cost of the advertising.

V. Regulation of Spam Outside the U.S.

With the exception of Europe, most other nations are less far along the road to regulation of spam. In North America, Canada, while it has strong privacy protections,⁸² has moved more slowly in the area of spam, where the government has expressed the view that legislation is unnecessary.⁸³

In Asia, Japan enacted legislation in 2001 requiring labeling of unsolicited advertising and instructions on how to reject future messages and prohibiting the sending of large quantities

⁷⁶ S. Hansell, “The Bandwagon to Fight Spam Hits a Bump,” N.Y. TIMES (Aug. 11, 2003), <http://www.nytimes.com/2003/08/11/technology/11SPAM.html>.

⁷⁷ R. Davidson, “FTC Official Calls Do-Not-Spam List Unrealistic,” USA TODAY, p. B3 (July 9, 2003), http://www.usatoday.com/money/industries/technology/2003-07-09-spam_x.htm

⁷⁸ *Muris Aspen Speech*.

⁷⁹ “States vs. Feds Over Anti-Spam Legislation,” beSpacific (May 1, 2003), <http://bespacific.com/mt/archives/002603.html>.

⁸⁰ 47 U.S.C. § 227(b)(1)(C).

⁸¹ *Missouri v. American Blast Fax, Inc.*, ___F.3d___ (9th Cir. 2003), available at <http://www.ca8.uscourts.gov/opndir/03/03/022705P.pdf>.

⁸² For information on Canadian privacy legislation and regulations and related information, see the website of the Privacy Commissioner of Canada, http://www.privcom.gc.ca/legislation/index_e.asp.

⁸³ M. Geist, “Time to Hit Delete Key on Weak Spam Policy,” THE GLOBE AND MAIL p. B15 (May 30, 2002), <http://www.theglobeandmail.com/servlet/ArticleNews/printarticle/gam/20020530/TWGEIS2> (article by University of Ottawa Law School professor).

of e-mail to non-existent addresses.⁸⁴ South Korea apparently requires labeling of spam in the subject line and a toll-free telephone number for spam recipients to opt out of further e-mails.⁸⁵

In Australia, there is no specific anti-spam legislation. A report of the National Office for the Information Economy (“NOIE”) in April 2003 recommended legislation requiring prior consent of, or a prior relationship with, the recipient before commercial e-mail may be sent; inclusion of accurate details of the sender’s name and physical and e-mail addresses; and a co-regulatory approach with industry that recognizes appropriate codes of practice.⁸⁶ The NOIE Report also urges increased industry self-regulation and development of anti-spam technologies, international cooperation, and an information campaign.⁸⁷

The Australian NOIE Report did identify existing Australian law with applicability to the spam problem, including privacy laws; laws prohibiting false and misleading claims; laws dealing with on-line gambling, therapeutic goods and pornography; and, perhaps more directly, provisions of the Criminal Code 1995 analogous to the U.S. Computer Fraud Abuse Act. These provisions prohibit the knowing unauthorized impairment of electronic communications to or from a computer by means of telecommunications services (which might include spam that overtaxes computer resources), and the modification of data held in a computer, or impairment of the reliability, security or operation of such data, by means of a telecommunications service (which might include spam sent through third party servers).⁸⁸

Finally, Europe has perhaps the most developed set of anti-spam legislation, both on the EC level and in individual nations. The EC Directive on Privacy and Electronic Communications prohibits unsolicited e-mail without the consent of the recipient unless the sender has an existing commercial relationship with the recipient.⁸⁹ It also requires opt-out methods where prior relationships do exist, prohibits disguising or concealing the sender’s identity, and requires a valid address for opt-out requests.

⁸⁴ See “New Japanese Anti-Spam Rules,” WORLD INTERNET L. REP. (BNA) (Mar. 2002); “Law on Unsolicited E-mail Takes Effect,” Japan Today (Sept. 3, 2001), <http://www.japantoday.com/gidx/news221054.html>.

⁸⁵ National Office for the Information Economy (Australia), “Spam: Final Report of the NOIE Review of the Spam Problem and How It Can Be Countered” (April 2003) (hereafter “*Australian NOIE Report*”), Attachment C at p. 41, http://www.noie.gov.au/publications/NOIE/spam/final_report/SPAMreport.pdf (noting source of South Korean information was a media release and questioning re liability of translation).

⁸⁶ *Australian NOIE Report* at 3, 11-12, 17-19.

⁸⁷ *Id.* at 3-4, 17-19, 20-25.

⁸⁸ *Id.* at 12-16.

⁸⁹ Directive 2002/58/EC of the European Parliament and the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Recitals 40-43, Art. 13, available at http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=32002L0058&model=guichett. See also Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce in the internal market (Directive on electronic commerce), Recitals 30, 31, Art. 7 (unsolicited commercial e-mail should be clearly identifiable as such and should not increase recipient’s costs; Member States permitting unsolicited commercial e-mail without prior consent must ensure senders regularly check opt-out registers by which individuals may register not to receive such e-mails), available at www.spamlaws.com/docs/2000-31-ec.pdf.

Legislation requiring recipient opt-in before unsolicited commercial e-mail may be sent has been enacted in Austria, Denmark, Finland, Greece, Hungary, Italy, Norway, Poland, Slovenia, and Spain,⁹⁰ and is being considered in other countries. France's National Assembly passed such a bill and sent it to the Senate in early 2003.⁹¹ The European Coalition Against Unsolicited Commercial E-mail ("EuroCAUCE") has surveyed the current status of spam law on a country-by-country basis, including enacted anti-spam legislation, proposed laws under consideration, and existing laws that may alleviate spam.⁹²

Conclusion

The growing threat of spam to the continued efficacy of e-mail as a method of communication requires both a technological and a legal riposte. Legal tools to respond to spam are still being developed, as ISPs and users use both traditional legal theories and recently enacted statutes to respond to spammers, and legislatures develop new laws to address the problem.

Several aspects of spam hamper the development of effective legal tools to combat the problem. Most spammers appear ready, willing and able to disregard legal and ethical requirements and to use fraudulent means to pursue their activities. It can be extraordinarily difficult to identify spammers who take great pains to cover their tracks. And issues of jurisdiction and enforceability of judgments against spammers arise with spammers who may operate from foreign territories and who may lack substantial assets. Combined, these factors make enforcement efforts and liability claims difficult endeavors at best. Success will require the development of technological tools to address the problem as well, so as better to arm both the private and the public fighters in the battle against spam.

⁹⁰ For listings of the status of anti-spam laws in European nations, with links to the text and translations of enacted and pending legislation, see <http://www.euro.cauce.org/en/countries/index.html>. See also <http://www.spamlaws.com/eu.html>.

⁹¹ Agence France-Presse, "French Legislators Vote to Ban Spam," newsobserver.com (Feb. 26, 2003), <http://newsobserver.com/24hour/technology/story/782597p-5609931c.html>.

⁹² See <http://www.euro.cauce.org/en/countries/index.html>.