

“Opting-Out”: A Technical, Legal and Practical Look at the CAN-Spam Act of 2003

Dominique Chantale Alepin*

INTRODUCTION

“VIAGRA MAILED DIRECT!” “PRE-APPROVED LOAN!” “MAKE 1,000,000 FROM Your Own Home!” “B\$% @es ready for you!”—the dread of opening e-mail and finding these messages in one’s inbox is a reality for the majority of American e-mail users. Spam¹, or Unsolicited Commercial E-mail (UCE), has risen to the level of a major epidemic for e-mail users and ISPs. In reaction, lawmakers, law enforcers and private actors are all scrambling to find a way to stem this growing problem.

E-mail is replacing the telephone, fax and the physical mail system as a cheap, convenient and simple way to communicate. With its speed and immediacy, e-mail can substitute for expensive cross-country telephone conversations. Letters that would have waited weeks to travel to the opposite end of the globe now, as e-mail, traverse the world in a matter of seconds. E-mail has become an important way of communicating for both personal and business purposes. It is also available ubiquitously from PCs to Blackberries to internet cafés. It is woven into the fabric of modern day life. As the number of e-mail users increases, businesses and merchants are looking for ways to capitalize on this growth.²

The low cost of e-mailing has also made it a great medium for commercial advertisers to reach consumers directly. Indeed, as FTC Chairman Timothy J.

* J.D. Candidate 2005, Columbia University School of Law; B.A., Honors, Economics, Bowdoin College, 2003. Special thanks to James Tierney, Esq., Director, The National State Attorneys General Program at Columbia Law School, Ronald and Linda Alepin, David Johnson, Esq., Visiting Professor of Law, Yale Law School, and Kenneth Dreifach, Esq., Chief, New York State Attorney General Internet Bureau. This will be published in the Columbia Journal of Law & Arts, Vol. 28, Issue 1.

1. “Use of the term ‘spam’ as internet jargon for this seemingly ubiquitous junk e-mail arose out of a skit by the British comedy troupe Monty Python, in which a waitress can offer a patron no single menu item that does not include spam: ‘Well there’s spam, egg, sausage and spam. That’s not got *much* spam in it.’” State v. Heckel, 24 P.3d 404, 406 n.1 (Wash. 2001), citing 2 GRAHAM CHAPMAN ET AL., THE COMPLETE MONTY PYTHON’S FLYING CIRCUS: ALL THE WORDS 27 (Pantheon Books 1989). Spam entered the dictionary in 2003 meaning “[u]nsolicited e-mail, often of a commercial nature, sent indiscriminately to multiple mailing lists, individuals, or newsgroups; junk e-mail” *Spam*, Dictionary.com at <http://dictionary.reference.com/search?q=SPAM> (last visited Oct. 29, 2004). There are variations on the word “Spam” including “Spammed”, “Spamming” (“to send unsolicited e-mail to”) and “Spammer” (“one who send unsolicited e-mail”). *Id.*

2. Richard C. Lee, *State Actor: Cyber Promotions Inc. v. America Online, Inc.*, 13 BERKELEY TECH. L.J. 417 (1998).

Muris has remarked, “[t]he magic of e-mail is that you can e-mail almost anyone. The tragedy is that almost anyone can e-mail you.”³ Although early spam was dominated by pill peddlers, sellers of internet pornography and get-rich-quick schemes, legitimate companies are starting to learn of the prospects inherent in e-mail advertising. More and more companies and merchants are starting to use this medium to bombard e-mail users with their products. Indeed, Morgan Stanley’s Discover Card, Altria’s Gevalia Coffee, Schering-Plough’s Claritin and even *The New York Times* are all products from large companies that have been advertised through spam.⁴ In addition, organized crime rings are getting online and using spam as a means of getting sensitive information on bank accounts through “phishing”⁵ and are also using spam as a way of unloading “fake pharmaceuticals and counterfeit software.”⁶

The statistics on spam are astounding. While the internet and e-mail were hailed as a source of learning and opportunity, spam now accounts for forty percent of all e-mail sent daily⁷, which amounts to 12.4 billion spam messages per day.⁸ The Yankee Group has recently released a study that spam is costing American businesses \$4 billion a year in lost productivity. Yankee estimates that an average worker will spend ten seconds a day deleting spam adding up to sixty lost minutes a year. Cost of each minute? Forty-five cents. While that number might not seem large, a firm with 1,000 employees will lose \$27,500 per year.⁹ In addition to other costs such as server overload, fraud and filtering costs, the total costs of spam worldwide have been estimated at \$9.4 billion.¹⁰ Spam might also be affecting commerce in the United States in another indirect yet important way—the more consumers become frustrated with the amount of junk bulk mail they are receiving, the more likely they are to dismiss any commercial e-mail as spam and the less likely they are to use e-mail in general.¹¹ This, in turn, affects the total usefulness of e-mail as a mode of communication.

3. FTC, *Protecting Consumer’s Privacy: Goals and Accomplishments: Remarks of FTC Chairman Timothy J. Muris at the Networked Economy Summit* (June 11, 2002), available at <http://www.ftc.gov/speeches/muris/gmason.htm>.

4. See Saul Hansell, *It Isn’t Just the Peddlers of Pills: Big Companies Add to Spam Flow*, N.Y. TIMES, Oct. 28, 2003, at A1.

5. See Saul Hansell, *Online Swindlers, Called ‘Phishers,’ Lure the Unwary*, N.Y. TIMES, Mar. 24, 2004, at A1.

6. Michelle Pountney, *Criminals turn to spam*, HERALD SUN (Melbourne, Austl.), July 16, 2004, at 38.

7. Doug Bedell, *Study finds law fails to cut spam; Volume of unwanted e-mails has actually increased, firm says*, DALLAS MORNING NEWS, Mar. 18, 2004, at 1D.

8. *Spam Statistics, 2004*, Spam Filter Review, A TopTenREVIEWS™ Website, at <http://www.spamfilterreview.com/spam-statistics.html> (last visited Oct. 29, 2004).

9. Jon Chesto, *Junk e-mail still costing \$4B a year*, THE BOSTON HERALD, Apr. 6, 2004, at 38.

10. S. REP. NO. 108-102, at 6 (2003), reprinted in 2004 U.S.C.C.A.N. 2348, 2325, 2003 WL 21680759 at *6.

11. Try, try again to can ‘spam’, NEWSDAY (N.Y.), July 5, 2004, at A30; See also Robert MacMillan, *Survey Finds Spam Undeterred; People Report Little Impact from New Federal Law*, WASH. POST, Mar. 18, 2004, at E05 (“Thirty percent [of e-mail users] said they had reduced their use of e-mail because of spam. . .”). In addition, seventy percent of e-mail users say that spam is making their online experience “unpleasant and annoying.” Bedell, *supra* note 7.

There have been several responses to the proliferation of spam in the United States and elsewhere. While ISPs and businesses have invested in spam filters¹² which prevent spam from reaching inboxes, frustrated e-mail users, as well as major ISPs, have resorted to litigation against spammers. Recognizing the costs imposed on e-mail users, businesses and ISPs, states and the federal government recently enacted various statutes, hoping to regulate spam.¹³ The responses by e-mail users, ISPs and legislators have yielded uneven results.

Most recently, in December of 2003, federal lawmakers joined the battle by passing one of the most controversial pieces of legislation surrounding spam: the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, more commonly known as the CAN-Spam Act.¹⁴

This federal bill is not without problems. The CAN-Spam Act seems to dictate “rules of conduct” for spam, rather than reducing the amount of unwanted e-mail clogging inboxes. The greatest victory for the Act has been the reduction in the amount of pornographic spam, which dropped from 21.8% in 2003 to 4.8% in early 2004.¹⁵ The reason for the reduction of pornographic spam is unclear—some analysts have suggested it is because the labeling requirement makes the messages easier to filter while others believe that the pornography industry does not want to irritate e-mail users or prosecutors any further.¹⁶

However, regarding fraudulent messages, as well as financial and pharmaceutical spam, the federal bill has yet to prove its worth. Since the federal bill pre-empts state legislation aimed at regulating spam directly¹⁷ and takes away the right of action of e-mail users against spammers,¹⁸ its efficacy will depend on the success of enforcement by ISP’s, state Attorneys General, the FCC and the FTC, as well as on the coordination of technical solutions among private parties.

12. Spam filters are the technical solution for dealing with spam. Some private companies have capitalized on the spam problem by creating and selling spam filters to ISPs and e-mail users. Take, for example, Brightmail.com which has sold its technology to Microsoft for use in hotmail.com. Brightmail, recently sold to Symantec for \$104 million or four times Brightmail’s 2003 sales, also sells spam filters to individual e-mail users. Alex Pham, *These Days, Tech Firms Would Rather Merge Than Go Public; Companies are deciding that stock offerings, once a rip off, are more trouble than they’re worth. And eager buyers abound*, L.A. TIMES, July 26, 2004, at C1.

13. See discussion *infra* Parts II, IV.

14. Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, Pub. L. No. 108-187, 117 Stat. 2699-2719 (2003), *hereinafter* CAN-Spam Act.

15. Pountney, *supra* note 6, at 38.

16. Bedell, *supra* note 7, at 1D.

17. The federal CAN-Spam Act preempts all state laws that specifically regulate commercial e-mail including more restrictive laws such as the California state spam statute that was to take effect in January of 2004. The scope of federal preemption is not absolute as states are still allowed to prohibit false and deceptive e-mail content and message relaying. State computer crime laws also will still remain intact. However, as will be discussed below, although common law and other state laws can address spam, the most effective litigation comes from laws specifically directed at spam. Note that New York State Attorney General, Elliot Spitzer, before the passage of the CAN-Spam Act, brought suits against the most major spammers under a state deceptive practices law since New York did not have a state spam statute. Telephone Interview with Kenneth Dreifach, Chief, New York State Attorney General’s Office Internet Bureau, Jan. 5, 2004.

18. See CAN-Spam Act § 8.

The outlook on further progress against spam is not encouraging. Indeed, since the passage of the CAN-Spam Act, the amount of spam has actually *increased*.¹⁹ Federal lawmakers have passed a bill and disappeared; the word “spam” vanishing from the headlines, and prosecutors turning to other issues. The FTC, charged with finding alternative solutions to litigation, recently released a report that underscored the FTC’s inability to combat spam without technical measures which would be implemented in partnership with the e-mail services industry.²⁰ Given this and the fact that weak construction of the law severely undermines the efficacy of its enforcement, it is unlikely that the CAN-Spam Act will actually CAN anything.

This Note is an examination of the legal, regulatory and technical problems posed by spam. Part I outlines the costs associated with spam and how these costs are externalized onto ISPs, businesses and e-mail users. Part II analyzes the constitutionality of state and federal spam laws in relation to case law from the regulation of other commercial advertising mediums. Part III examines the CAN-Spam Act and contrasts it to state spam statutes. Part IV looks at past regulation of spam and litigation by private parties, state Attorneys General as well as federal actors. Part V explores the effectiveness of the bill and how to decrease the total amount of spam clogging America’s inboxes.

I. Spam Costs

While there are arguments that spam is nothing but junk mail transmitted through an internet connection, there is a strong case that spam is essentially different from the junk mail that is delivered to one’s mailbox by a postman. These fundamentally different costs imposed upon the receiving parties involved make physical mail different from e-mail.

A. E-mail Users

Spam shifts the costs of advertising to the e-mail user by resembling “postage due” in the physical mail system.²¹ E-mail users that pay for their internet connection per minute by contract with their ISP physically incur the cost by sorting their inbox and deleting spam. Spammers have become very good at disguising the spam “nature” of their messages by using subject lines that resemble personal e-mails from friends and colleagues, as well as by falsifying the origin of the message. E-mail users are frequently forced to open the e-mail revealing its content before they can erase the message. Roughly two dollars of an e-mail user’s monthly fee goes to spam filtering.²²

In addition to the money spent on the internet for filtering through spam messages, e-mail users lose time and energy. Spam is not a passive form of marketing like direct mail and infomercials, where the user has the choice of

19. Bedell, *supra* note 7, at 1D.

20. National Do Not Email Registry: A Report to Congress, FTC (June 2004), available at <http://www.ftc.gov/reports/dneregistry/report.pdf>.

21. Jonathan Krim, *Spam’s Costs to Business Escalates; Bulk E-Mail Threatens Communication Arteries*, THE WASHINGTON POST, Mar. 13, 2003, at A01.

22. See Kenneth Amaditz, *Canning “Spam” in Virginia: Model Legislation to Control Junk E-mail*, 4 VA. J.L. & TECH. 4, para. 11 (1999), citing Johanna Bennett, *Should SPAM Be Banned?*, DOW JONES NEWS SERVICE, July 21, 1998.

throwing the junk mail in the garbage without opening it or simply turning off the TV. Spam e-mail entails some degree of involvement of the e-mail user in opening or sorting through the junk mail, which constitutes tangible cost of time and energy.

Having to sort through the mounds of spam might deter internet users from using their e-mail as frequently as they would were it not overflowing with junk mail.²³ Fear of getting even more spam causes internet users to steer away from putting their e-mail address on valuable lists where they might be connected to people with the same interests or fruitful business contacts.²⁴ E-mail users wanting to be rid of junk mail may *try* to unsubscribe from marketers' mailing lists and may even resort to buying their own costly filters.²⁵ Spam has even started deterring people from using e-mail at all—indeed, thirty percent of American internet users surveyed by the Pew Internet & American Life Project in March of 2004 had reduced their use of e-mail because of spam.²⁶

Spam is also a haven for fraudulent scams, computer worms,²⁷ spoofs,²⁸ phishing schemes,²⁹ pyramid schemes, get-rich-quick offers as well as child and adult pornography.³⁰ “Such e-mails are particularly troubling when they are sent to minors: [spammers] rarely know the age of persons to whom the messages are sent.”³¹ These are some of the especially undesirable effects of spam that, for

23. See Paul Hoffman, *Unsolicited Bulk E-Mail: Definitions and Problems*, INTERNET MAIL CONSORTIUM REPORT: UBE-DEF IMCR-004 (Oct. 5, 1997), at www.imc.org/ube-def.html.

24. Interview with Linda T. Alepin, President, Center for New Futures, in Los Altos, Cal. (Nov. 24, 2003).

25. John Magee, *The Law Regulating Unsolicited Commercial E-Mail: An International Perspective*, 19 SANTA CLARA COMPUTER & HIGH TECH. L.J. 333, 338 (2003). The filtering business is booming in Silicon Valley—spending on anti-spam products will increase fifty percent in 2004. Jon Swartz, *Anti-Spam Industry Consolidating*, USA TODAY, July 20, 2004, at 2B.

26. Bedell, *supra* note 7, at 1D.

27. “A computer worm is a self-replicating computer program, similar to a computer virus. A virus attaches itself to, and becomes part of, another executable program; however, a worm is self-contained and does not need to be part of another program to propagate itself. They are often designed to exploit the file transmission capabilities found on many computers.” *Computer Worm*, Wikipedia, at http://en.wikipedia.org/wiki/Computer_worm (last visited Oct. 20, 2004).

28. “The term [spoo]f is used in computer security to refer to a situation in which one person or program is able to masquerade successfully as another. . . Many insufficiently carefully designed protocols are subject to spoof attacks, including many of those used on the internet.” *Spoof*, Wikipedia, at <http://en.wikipedia.org/wiki/Spoof> (last visited Oct. 10, 2004).

29. “In computing, phishing, short for password harvest fishing, is the luring of sensitive information, such as passwords and other personal information, from a victim by masquerading as someone trustworthy with a real need for such information. . . Today, online criminals put phishing to more directly profitable uses. Popular targets are users of online banking services, and auction sites such as eBay. Phishers usually work by sending out spam e-mail to large numbers of potential victims. These direct the recipient to a Web page which *appears* to belong to their online bank, for instance, but in fact captures their account information for the phisher's use. . . .” *Phishing*, Wikipedia, at <http://en.wikipedia.org/wiki/Phishing> (last visited, Oct. 11, 2004).

30. See Robert Ditzion, et al., *Computer Crimes*, 40 AM. CRIM. L. REV. 285, 290 (2003). See also Scott Shane, *Bill would make spammers' spam e-mail tactics a crime; Passage would give Md. one of the most powerful measures in the U.S.*; *General Assembly*, THE BALT. SUN, Apr. 15, 2004, at 1B.

31. David E. Sorkin, *Technical and Legal Approaches to Unsolicited Electronic Mail*, 35 U.S.F. L. REV. 325, 336 (2001), *citing* *Reno v. ACLU*, 521 US 844, 855-856 & n.20 (1997).

reasons mentioned below, can only be solved through regulation.³²

B. Businesses

Businesses are also victims of external spam costs. Businesses lose productivity of employees forced to sort through their inboxes, open messages and filter spam from the important business-related messages.³³ Businesses that provide their employees with a corporate e-mail account (which is a growing percentage of companies in the United States) also incur significant costs in seeking to prevent spam from overloading their servers. Since there is a substantial risk of the business' servers becoming congested (which would stall important e-mails from getting to their recipients and increase server costs), companies actively install and update technical filters to eliminate spam before it even gets through to the inbox. These technical filters are expensive and take time to install onto all of the business' computers.³⁴

In addition, a downside to installing these highly effective technical barriers is that at least some important e-mails from business contacts are liable to get caught in the filter.³⁵ This problem of "false positives" requires increasing efforts on the part of the business sector to fight the spammers.³⁶ Businesses can lose out on opportunities communicated to them through e-mail because of an overactive filter. These additional costs reduce the total effectiveness of e-mail as a tool of communication for businesses.

C. ISPs

ISPs may be the hardest hit by spam.³⁷ Spam increases storage costs on ISP servers, forcing them to increase bandwidth and hard drive storage.³⁸ ISPs have started passing these costs on to consumers in the form of higher prices for internet service or e-mail accounts.³⁹

ISPs, as the companies who service internet connections for their consumers, must also hire personnel, technical support and other consultants to field angry complaints from customers. ISPs have seen the costs devoted to dealing with the

32. See discussion *infra* Part III.

33. As mentioned above, the total cost of a business with 1,000 employees would be \$27,500 per year. Chesto, *supra* note 9, at 38.

34. Interview with Ronald Alepin, President, Los Altos Systems Research, in Los Altos, Cal. (Nov. 27, 2003). The rise in spending on anti-spam products also demonstrates that businesses are spending more and more on filtering devices. Swartz, *supra* note 25, at 2B.

35. Alepin, *supra* note 24.

36. Steven Miller, *Washington's "Spam Killing" Statute: Does It Slaughter Privacy in the Process?*, 74 WASH. L. REV. 453, 454 (1999).

37. See Brad Stone, *Soaking in Spam*, NEWSWEEK, Nov. 24, 2003, at 66; see also Michael B. Edwards, *Recent Development: A Call to Arms: Marching Orders for the North Carolina Anti-Spam Statute*, 4 N.C. J.L. & TECH. 93, 118 (2002).

38. Messages addressed to false e-mail addresses the spammer has collected or fabricated are "bounced" off the ISP meaning they are sent back to the sender. Because most of the addresses the spammer sends use are fictitious, messages get bounced back and forth increasing the storage space used on the ISPs' bandwidth and server. Miller, *supra* note 36, at 456.

39. Neil Swidey, *Spambusters Cyberwarriors of Many Stripes Have Joined the Battle Against Junk E-Mail. But the Enemy is Wily, Elusive and Multiplying*, THE BOSTON GLOBE MAGAZINE, Oct. 5, 2003, at 12.

spam problem increase in recent years—a conservative estimate is that ISPs devote ten percent of resources to dealing with spam.⁴⁰

Spammers also compromise internet security of ISPs by “relaying” their messages through open proxies.⁴¹ Mail relays hijack third-party servers, overloading it in the process, in order to relay bulk spam. This can result in performance degradation of the open proxy and might even cause the system to crash, all at no cost to the spammer.⁴²

The “closed” ISP servers—i.e., those which prohibit use by non-users—have become frustrated by ISPs that operate open proxies. The former have put pressure on the latter to prevent server hijacking by spammers.⁴³ Although closed proxy server ISPs may be successful at preventing spammers from using their own servers as the starting point of spam, they have engaged in fruitless attempts at punishing open proxy ISPs and have not been successful at implementing filtering software to block spam, as spammers frequently use “spoofed” subject lines and false message origins.⁴⁴

Because ISPs have been the most directly and tangibly harmed by spam, they have been the fastest to react against spammers through litigation and implementation of anti-spam technical solutions.

D. Costs for spammers

Even though spam has proved to be a highly ineffective way of marketing goods in terms of sales per messages sent, the relatively low cost of spamming has meant that more and more merchants and businesses are using spam as a marketing tool.⁴⁵ “The cost of sending a million e-mails is about \$3,000, compared to \$1.5 million to send a million pieces of mail.”⁴⁶

Costs to spammers include “finding a cooperative or naïve internet service provider, figuring out how to send spam, composing the message text, and setting up a system for receiving payment and processing orders.”⁴⁷ Once these costs have been incurred, the marginal cost of sending one more message closes in on zero.⁴⁸ While some companies send their own spam, several independent spam companies have set themselves up as “agents” and independently contract with major firms to

40. See Amaditz, *supra* note 22.

41. A “mail relay” is when a “spammer connects to a Simple Mail Transfer Protocol (SMTP) server operated by a third party, where neither the spammer nor the recipient are local users and directs the server to send copies of the message to a long list of recipients. Many sites permit the use of their servers only for messages sent to or from their own users, but there are still many so-called open servers that lack such restrictions.” Sorkin, *supra* note 31, at 339.

42. Sorkin, *supra* note 31, at 340.

43. Dreifach, *supra* note 17.

44. Amaditz, *supra* note 22, at para. 12.

45. Stone, *supra* note 37, at 68.

46. Samay Gheewala, *Spam wars: Mountain View a battleground over unwanted e-mail*, MOUNTAIN VIEW VOICE, Feb. 28, 2003, (quoting Gideon Mantel), available at http://www.commtough.com/coverage/030222_SpamWars.pdf.

47. Sorkin, *supra* note 31, at 338 n.53.

48. Contrast this to physical mail where although the marginal cost of printing will decrease over time, the cost of sending that message stays constant at whatever the postal system fixes as the price of postage.

send their spam and collect information for them.⁴⁹ For example, Ryan Pitylak, a college student who has been spamming since he was 14 years old, has created a spam scheme which claims to give the spam message recipient “5 Free Health Insurance Quotes” or “Incredible 3.51% Mortgage Rates” in exchange for personal information about the recipient. Pitylak then sells the information collected on the recipient (including the e-mail address) to legitimate companies such as IndyMac Bank, ADT Security and MEGA Life and Health Insurance.⁵⁰ A recent *New York Times* article confirms that major corporations are themselves starting to get into the spam act.⁵¹

Spammers enjoy both the low cost of sending the actual bulk e-mail and the low cost of finding the e-mail addresses to which to send them. Spammers can send about 100,000 e-mails for under \$200 and they can buy one million e-mail addresses for under \$100.⁵² E-mail addresses are harvested off websites and also ‘guessed’ by increasing numbers and changing letters for known e-mail addresses.⁵³

In the quest for gaining anonymity to escape all liability, a couple hundred dollars can buy any spammer 250,000 messages with forged headers and fake e-mail addresses.⁵⁴ The low cost of spamming creates the problem that even if the businesses receive only a couple orders for the product or service, they can recover the costs of their spam marketing venture.

For these reasons, the goal of litigation and regulation in this area should be to increase costs of spamming so that the costs currently imposed on ISPs and e-mail users are internalized by the spammer.

II. Regulation of Commercial Advertisements

There are three major problems caused by spam: (1) the sheer volume of spam overwhelms e-mail users, businesses and ISPs; (2) spam has become inherently deceitful in subject headers and routing information which defrauds consumers; and (3) spam is a haven for fraudulent schemes and adult material. State and federal legislation has varied as to which problem it has sought to ameliorate.

Given the current costs associated with spam, regulation at both the state and federal level should be focused on internalizing the costs and shifting them to spammers, preventing the negative social effects of adult material and deceptive spam as well as protecting the privacy interests of ISPs and e-mail users. The best and most legal method of achieving these goals is subject to debate, and the

49. Another example includes the case of Scott Richter who has made a lucrative living off sending spam for all types of products including diet pills, sexual aids and porn sites. His company, OptInRealBig makes over \$2 million in monthly revenue. See Stone, *supra* note 37, at 68.

50. Howard Witt, *22-year-old thrives in world of spam; Law fails to stop flood of e-mails*, CHICAGO TRIBUNE, July 18, 2004, at 1.

51. See Hansell, *supra* note 5.

52. Frances E. Zollers et al., *Fighting Internet Fraud: Old Scams, Old Laws, New Context*, 20 TEMP. ENVTL. L. & TECH. J. 169, 171 (2002).

53. Carol Jones, *E-Mail Solicitation: Will Opening a “Spam-Free” Mailbox Ever Be a Reality?*, 15 LOY. CONSUMER L. REV. 69, 71-72 (2002).

54. Lorrie Faith Cranor & Brian A. LaMacchia, *Spam!*, 41 COMM. ACM 8, 74 (1998), available at <http://portal.acm.org/citation.cfm?id=280336>.

variation in legislation (federal and state) reflects this uncertainty. A comparison of the regulation of other modes of communication and advertising sheds light on what types of regulation by federal or state lawmakers should be legally permissible. However, what is practical when it comes to regulation is a different question.

A. Legal Background

The Supreme Court has always recognized the government's interest in protecting the privacy of the home. As the Supreme Court held in *Rowan v. United States Postal Office Department*, the government can legislate to protect citizens from unwanted intrusions into private domiciles.⁵⁵

Legislation crafted to fight spam will be subject to the past quarter century of litigation surrounding other commercial advertising mediums. It is useful, therefore, to explore how courts have approached the other media such as fax and telephone solicitation.

Commercial advertisers, when confronted with government regulation of advertising, commonly invoke a First Amendment challenge to the legislation. Courts have utilized a test (frequently called the *Central Hudson* test) in order to balance the rights of commercial speech with the duty of the government to protect its citizens. The Supreme Court has always held that commercial speech, as long as it is not fraudulent or deceitful, is protected by the First Amendment—but the protection afforded is less than that of freedom of religion or non-commercial speech.⁵⁶ “When a law regulates non-misleading commercial speech that concerns a lawful activity, the government may regulate that speech as long as [1] the regulation serves a substantial government interest, [2] the regulation directly advances that government interest and [3] the regulation is not more extensive than is necessary to serve that interest.”⁵⁷ In sum, the test consists of three prongs: (1) whether the speech concerns a lawful activity (2) whether the regulation serves an important government interest and (3) whether the government regulation is narrowly tailored to that goal.⁵⁸ In respect to narrowly tailored legislation, the Supreme Court has held that while the regulation be reasonably related to the goals, it need not be the least restrictive means of regulation.⁵⁹

In general, communication that does not pose a significant cost to the consumer cannot be banned on principle by the state or the federal government because of the First Amendment protections afforded to commercial advertisements.⁶⁰ Such communication can be stopped from reaching a consumer through an “opt-out”⁶¹

55. *Rowan v. United States Post Office Dep't*, 397 U.S. 728 (1970).

56. *Posadas de Puerto Rico Assoc. v. Tourism Co.*, 478 U.S. 328, 349 (1986).

57. *Fraternal Order of Police v. Stenehjem*, 287 F. Supp. 2d 1023, 1027 (N.D. Dakota 2003), citing *Central Hudson Gas & Elec. Co. v. New York*, 447 U.S. 557, 577 (1980).

58. *Central Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of New York*, 447 U.S. 557 (1980).

59. *City of Cincinnati v. Discovery Networks, Inc.*, 507 U.S. 410 (1993).

60. *Rowan*, 397 U.S. at 737.

61. An “opt-out” procedure is commonly used in spam and other commercial communication. The consumer notifies either the company or a third party (such as a government agency) that he or she does not want to receive further communication from that particular company or from companies in general.

system where the consumer voluntarily chooses whether or not to receive advertisements from merchants.⁶² It is important to note that this rule has been qualified, as new media which impose costs of communication on consumers or third parties have been created and used more frequently.⁶³ Media that pass costs onto third parties may be banned outright by federal or state legislation.⁶⁴

B. Post—Physical Mail and Direct-Mail Marketing

The Court has held that direct-mail marketing does not externalize a significant cost on the consumer, does not infringe privacy in the home and therefore cannot be constitutionally banned outright.⁶⁵

In *Bolger v. Youngs Drug Products Corp.*, the Court invalidated a total ban on direct mail commercial advertisements for contraceptives. The ban interfered too much with the right of the advertiser to communicate with consumers. The Court held that the unreceptive recipients could simply “avert their eyes” if they wished to avoid the advertiser’s message.⁶⁶

This ruling has not stopped government agencies from attempting to curb the amount of junk mail that floods consumers’ mailboxes. Indeed, the federal government has enacted the Federal Salary Act, which allows individuals to “opt out” of commercial mailings by putting their name on a “do-not-contact” list that prohibits the advertisers from sending unsolicited mail to them.⁶⁷

The constitutionality of this law was tested in *Rowan*. There, the Court ruled that the Federal Salary Act did not violate the First Amendment. The Court balanced the right of commercial advertisers to communicate through the postal system and the right of every person to be “left alone” and held that the right to communicate “stop[ped] at the mailbox of an unreceptive addressee.”⁶⁸ Indeed, the Court went on to specify that “[t]o hold less would tend to license a form of trespass and would make hardly more sense than to say that a radio or television viewer may not twist the dial to cut off an offensive or boring communication.”⁶⁹ The Court placed a significant amount of weight on the construction of the statute which allowed for adequate communication in the form of an opt-out system.

The primary difference between *Bolger* and *Rowan* in a direct-mail system is the availability of the unreceptive addressee to remove voluntarily his name from the mailing list in *Rowan* versus an outright ban in *Bolger*.

C. Telephone Solicitations

The Court has also held that telephone solicitations, although annoying and an imposition on one’s time, do not pose enough of a cost or constitute enough of an

62. *Rowan*, 397 U.S. at 738.

63. *Destination Ventures v. FCC*, 844 F. Supp. 632 (D. Or. 1994), *aff’d*, 46 F.3d 54 (9th Cir. 1995).

64. *See Missouri ex rel. Nixon v. American Blast Fax, Inc.*, 323 F.3d 649 (8th Cir. 2003).

65. *Bolger v. Youngs Drug Prod. Corp.*, 463 U.S. 60 (1983).

66. *Id.*

67. Title III of the Postal Revenue and Federal Salary Act of 1967, 39 U.S.C. §4009(a) (1964 ed. Supp. IV) (current version at 39 U.S.C. 3010 (2001)).

68. *Rowan v. United States Post Office Dep’t*, 397 U.S. 728, 737 (1970).

69. *Id.*

invasion of the home privacy to justify a *total* ban on this medium of commercial advertising.

However, telephone calls have been differentiated from direct-mail advertising on the grounds that the telephone is more of an invasion into the home than the sending of a letter. The Minnesota Supreme Court distinguished the two mediums in *Humphrey v. Casino Marketing Group*:

...the residential telephone is uniquely intrusive. The caller...is able to enter the home for expressive purposes without contending with such barriers as time, distance, doors or fences...Unlike the unsolicited bulk mail advertisement found in the mail collected at the resident's leisure, the right of the telephone mandates prompt response, interrupting a meal, a restful soak in the bathtub, even intruding on the intimacy of the bedroom...⁷⁰

Although live telephone unsolicited communications have been held constitutionally protected as commercial speech,⁷¹ pre-recorded unsolicited telephone calls can be constitutionally banned by the government.⁷²

In *Moser v. FCC*, the Court of Appeals for the Ninth Circuit upheld a section of the Telephone Consumer Protection Act (TCPA),⁷³ which banned pre-recorded telephone calls.⁷⁴ In this case, the court found that pre-recorded telephone calls created a substantial invasion of privacy and were a nuisance because consumers could not interact with the solicitors, could not vent their frustration to the solicitors and had to wait until the end of the message to express to the solicitor that they would not like to be contacted in the future for such calls. In addition, the court found that pre-recorded unsolicited messages can clog up answering machines and prevent important messages from being recorded. In determining whether the regulation was overbroad, the court examined whether the government interest was narrowly tailored to the residential privacy interest and whether there were ample alternatives for communication besides pre-recorded messages. The court found that Congress had made sufficient findings to justify such regulation on the grounds of invasion of privacy and the unjust externalization of costs onto the consumer. In addition, the court found that the law still allowed several alternatives for commercial advertisers, including taped messages introduced by a live caller, taped messages to which consumers had previously consented, as well as other avenues, like direct-mail and infomercials.⁷⁵ Other courts have similarly found against advertisers in upholding total bans on pre-recorded unsolicited telephone calls.⁷⁶

In response to various courts' interpretation of First Amendment constraints on telephone solicitations, in 2003, Congress gave authority to the FTC through the

70. *Humphrey v. Casino Mktg. Group*, 491 N.W.2d 882, 888 (Minn. 1992), *cert. denied*, 507 U.S. 1006 (1993).

71. *See Silverman v. Walkup*, 21 F. Supp. 2d 775 (E.D. Tenn. 1998).

72. *See Moser v. FCC*, 46 F. 3d 970 (9th Cir. 1995).

73. Telephone Consumer Protection Act of 1991, Pub. L. No. 102-243, §3, 105 Stat. 2394, 2395 (1991).

74. *Id.*

75. *Id.*

76. *Margulis v. P & M Consulting, Inc.*, 121 S.W.3d 246 (Mo. App. E.D. 2003).

TCPA to establish a national “Do-Not-Call” list for live telephone solicitations. The law was constitutionally challenged in *FTC v. Mainstream Marketing Services, Inc.*, where the plaintiff telemarketers requested a stay on the implementation of the FTC’s “Do-Not-Call” list in early 2003.⁷⁷ The Tenth Circuit Court of Appeals dismissed the claims, holding the “Do-Not-Call” registry was a valid exercise of the FTC’s power and rejecting First Amendment violation arguments. Citing *Rowan*, the court focused its holding on the opt-in nature of the law, which gave individuals the choice of privacy.⁷⁸

D. Fax Machines

Unlike live telephone calls and direct mail advertising, use of a fax machine to communicate an advertisement causes the fax machine owner to incur actual and physical costs in receiving messages. Fax advertising shifts costs to the recipients who then must use paper, ink and fax time (time when the fax machine cannot receive business or personal faxes) when receiving the advertisements.

In *Missouri ex rel. Nixon v. American Blast Fax*, the Eighth Circuit Court of Appeals held that the TCPA’s outright ban of unsolicited commercial faxes was not a violation of the First Amendment.⁷⁹ The court held that although technological changes had decreased the costs of receiving the advertisements through fax machines, these costs had not been eliminated and the government had a significant interest in preventing cost-shifting.⁸⁰ The court held that the outright ban on unsolicited advertisements through this medium was not overly broad, but was narrowly tailored to achieve the goal of preventing cost-shifting. The court also held that although Congress might have instituted an “opt-out” system that would have allowed more communication by the advertisers, the TCPA did not act as a total ban on fax advertising. The court went on to explain that “. . .advertisers may obtain consent for their faxes through such means as telephone solicitations, direct mailing, and interaction with customers in their shops.”⁸¹

Recently, a Louisiana district court agreed with the Eighth Circuit that an outright ban on unsolicited faxes was not in violation of First Amendment rights of advertisers. In *Accounting Outsourcing v. Verizon Wireless Personal Communications*, the court held that the government’s interest in protecting the consumer from the time and monetary costs associated with receiving unsolicited faxes was substantial, and although the commercial speech sent by Verizon was protected, the TCPA advanced a substantial and valid government interest.⁸²

Courts in most jurisdictions agree with the Eighth Circuit’s interpretation in *Missouri ex rel. Nixon v. American Blast Fax*.⁸³ However, the New York Civil

77. *FTC v. Mainstream Mktg. Servs., Inc.*, 358 U.S. 1228 (10th Cir. 2004).

78. *Id.*

79. *Missouri ex rel. Nixon v. American Blast Fax, Inc.*, 323 F.3d 649 (8th Cir. 2003).

80. There was evidence at the time that cost shifting from fax advertisements had imposed onto the recipient costs of “more than one hundred dollars a year in direct costs.” *Nixon*, 323 F.3d at 655.

81. *Id.* at 659.

82. *Accounting Outsourcing v. Verizon Wireless Personal Communications*, 329 F. Supp. 2d 789 (M.D. L.A. 2004).

83. *See, e.g., Harjoe v. Herz Fin.*, 108 S.W.3d 653 (Mo. 2003); *The Chair King, Inc. v. GTE*

Court in *Rudgayzer & Gratt v. Enine* held the TCPA's fax ban was an unconstitutional infringement of First Amendment communication, since there was a less intrusive means of restricting unsolicited faxes, such as the restriction in the New York state version of the TCPA that allowed an opt-out system.⁸⁴ New York joins a minority of states on this issue.⁸⁵ The Supreme Court has not yet ruled on the constitutionality of this aspect of the TCPA.

E. Application to E-mail

Because arguments in favor of regulating unsolicited e-mails are substantially similar to those on the regulation of junk facsimiles and unsolicited pre-recorded telephone solicitations, a federal ban on the medium *may* be constitutionally viable. However, there are those who believe that e-mail is more similar to live telephone calls and should be legally protected as a medium in order to protect the future viability of the internet.⁸⁶

Spam is a particularly sensitive issue because American courts have been reluctant to enact hard-line positions regarding the internet for fear of stifling the medium, which has generated so much discussion and prosperity.⁸⁷ The internet is a growing marketplace—nearly forty percent of internet users purchase goods and services online.⁸⁸

The most effective legislation concerning a curb on spam, as argued below, would be a federal ban on the medium as was enacted in the TCPA in regard to unsolicited faxes. The constitutionality of such a ban is questionable given the sensitivity of courts in regard to the internet as well as the First Amendment.⁸⁹

Should courts find that there were significant First Amendment protections afforded to spam, a federal program supporting “authentication” by e-mail servers before the e-mail is sent, as enacted in Nigeria, would be the next best solution to the spam problem.⁹⁰ However, the feasibility of forcing all e-mail services to implement this technical measure would be low, as it would be costly to e-mail service providers.

III. Legislation on Spam

A. State Legislation

Mobilenet of Houston, Inc., 135 S.W.3d 365 (Tex. App. 2004).

84. *Rudgayzer & Gratt v. Enine, Inc.*, 749 N.Y.S.2d 855 (N.Y. Civ. Ct. 2002).

85. *See, e.g., Van Bergen v. State of Minn.*, 59 F.3d 1541 (8th Cir. 1995); *Kenro, Inc. v. Fax Daily, Inc.*, 962 F. Supp. 1162 (S.D. Ind. 1997); *Minnesota v. Sunbelt Communs. & Mktg.*, 282 F. Supp. 2d 976 (D. Minn. 2002); *Texas v. American Blast Fax, Inc.*, 121 F. Supp. 2d 1085 (W.D. Tex. 2000); *Kaufman v. ACS Systems, Inc.*, 110 Cal. App. 4th 886 (2003); *Hooters of Augusta, Inc. v. Nicholson, et al.*, 537 S.E.2d 468 (Ga. Ct. App. 2000); *Harjoe*, 108 S.W.3d 653 (all holding that the TCPA's ban on unsolicited facsimiles is not a violation of the First Amendment).

86. *See Jonas Geissler, Whether 'Anti-Spam' Laws Violate the First Amendment*, 2001 J. ONLINE L. art. 8.

87. *Reno v. ACLU*, 521 U.S. 844 (1997). *See also United States v. Am. Library Ass'n*, 537 U.S. 1170 (2003).

88. U.S. DEP'T OF COMMERCE, A NATION ONLINE: HOW AMERICANS ARE EXPANDING THEIR USE OF THE INTERNET 1, 10 (2002) (39% of US population bought goods online).

89. Telephone Interview with David Johnson, Esq., Visiting Professor of Law, Yale Law School, Jan. 5, 2004.

90. *See discussion infra Part V.*

Before the passage of the CAN-Spam Act, thirty-eight states had enacted regulations concerning spam.⁹¹ However, that legislation varied from state to state in form and degree of restriction on spam.

While Washington's law regulating spam served as the model for most state legislation,⁹² states had been selective in the amount of the Washington law they borrowed for their individual statutes.

The most common form of regulation required the sender to include "ADV" (for advertisement) or "ADV: ADLT" (for an advertisement that involves adult subject matter like pornography) in the subject line and to include a valid sender name and e-mail address for opt-out instructions⁹³ so that the e-mail user could choose not to receive future e-mails.⁹⁴ One common problem with this type of legislation was that different states had imposed different variations on the way that "ADLT"⁹⁵ was spelled (sometimes "ADULT"⁹⁶ or sometimes "ADULT ADVERTISEMENT"⁹⁷) and had also varied in the legally required sender information (sometimes the physical address needed to be included, sometimes just the e-mail address).⁹⁸ The conflicts in the legislation across jurisdictions promoted confusion among spammers. These conflicts also prevented multi-party action on the part of various consumers or ISPs in class actions or by state Attorneys General in multi-state litigation.

Other states had gone farther than simply regulating the label on spam messages. Some states had outlawed the use of falsified routing information and the placement of false or misleading statements in the subject line.⁹⁹ In addition, some states had prohibited the use of a third party's internet address or domain name without express consent—preventing the problem of having innocent third parties

91. See David E. Sorkin, *State Spam Laws*, at <http://www.spamlaws.com/state/summary.html> (last visited Oct. 13, 2004).

92. Douglas J. Wood, *The Impact of State Anti-Spam Laws*, GigaLaw.com, at www.gigalaw.com/articles/2002-all/wood-2002-03-all.html (last visited Oct. 13, 2004).

93. The e-mail user is usually given a website link to connect to where he or she can inform the company that he or she no longer wishes to receive spam messages from that particular company.

94. ALASKA STAT. § 45.50.479 (Lexis Supp. 2003); ARIZ. REV. STAT. ANN. § 44-1372.02 (West Supp. 2003); ARK. CODE ANN. § 4-88-603 (Lexis 2003); CAL. BUS. & PROF. CODE § 17538.4 (West Supp. 2000); COLO. REV. STAT. § 6-2.5-103 (West 2002 & West Supp. 2003); 815 ILL. COMP. STAT. ANN. 511/1-15 (West Supp. 2004); IND. CODE ANN. § 24-5-22-8 (Lexis Supp. 2003); KAN. STAT. ANN. § 50-6,107 (Lexis 2002); LA. REV. STAT. ANN. § 14:106 (West Supp. 2004); 2003 ME. Legis. Serv. 327 (Lexis 2003); MICH. COMP. LAWS ANN. § 445.2503 (Lexis 2003); MINN. STAT. ANN. § 325F.694 (Lexis 2003); MO. ANN. STAT. § 407.1138; NEV. REV. STAT. ANN. § 41-730 (Lexis 2002); N.M. STAT. ANN. § 57-12-23 (Michie Supp. 2003); N.D. CENT. CODE, § 51-27-04 (Lexis Supp. 2003); OKLA. STAT. ANN. tit. 15, § 766.6 (Lexis 2004); 18 PA. CONS. STAT. § 5903(a.1) (West Supp. 2004); S.D. CODIFIED LAWS § 37-24-39 (Michie 2003); TENN. CODE ANN. §47-18-2501 (Lexis Supp. 2003); TEX. BUS. & COM. CODE § 46.003 (West Supp. 2004-2005); WIS. STAT. § 947.25 (West Supp. 2003).

95. ALASKA STAT. § 45.50.479 (Lexis Supp. 2003).

96. ARK. CODE ANN. § 4-88-604 (Lexis Supp. 2003).

97. TEX. BUS. & COM. CODE § 46.003 (West Supp. 2004-2005).

98. Sorkin, *supra* note 31, at 381.

99. Probably the most common problem arises from the use of apparently personal subject lines, such as "Hi" or "Re: this weekend," which seem to be from a personal contact but, in fact, contain advertisements.

(in mail relaying) seem responsible for the transmission of spam.¹⁰⁰

Virginia passed the first felony anti-spam law in May of 2003. The law makes it a state Class 1 misdemeanor to send spam “with the intent to falsify or forge electronic mail transmission information or other routing information in any manner.”¹⁰¹

In order to improve the efficacy of spam regulation, some states had expanded the parties who could sue spammers under spam laws. California, for example, had extended the list to include ISPs, e-mail users and the state Attorney General. Under the California law, each of these parties could sue for fifty dollars per e-mail sent in violation of the law, but they were limited to a maximum of \$25,000 per day. Courts were also permitted to award reasonable attorney fees to the prevailing party.¹⁰²

Several scholars questioned the constitutionality of state anti-spam laws, because of the risk of regulating interstate traffic or commerce not entirely within the state.¹⁰³ The internet is a non-jurisdictional medium as it has no physical location and permits media to be transmitted to and from anywhere in the world. Accordingly, internet communication, in any form, would seem to resemble interstate commerce. The dormant Commerce Clause prohibits states from regulating Congress’ supreme territory of interstate commerce, and this constitutional principle would seem to have prohibited states from regulating internet communication in general.¹⁰⁴ However, each state spam statute had a qualifying clause that “grounded” the regulation of spam to a message that is (1) sent from a computer within the state or, (2) transmitted to an ISP located in the state or (3) if the recipient of the message is located in the state.¹⁰⁵

The constitutionality (in regards to the dormant commerce clause issue) of state spam laws had been tested in two state court cases: *Ferguson v. Friendfinders* (California)¹⁰⁶ and *State v. Heckel* (Washington).¹⁰⁷ Both these cases upheld laws

100. ARIZ. REV. STAT. ANN. § 44-1372.02 (West Supp. 2003); ARK. CODE ANN. § 4-88-603 (Lexis Supp. 2003); CAL. BUS. & PROF. CODE § 17538.4 (West Supp. 2004); COLO. REV. STAT. § 6-2.5-103 (West 2002 & West Supp. 2003); DEL. CODE tit. 11 § 937(d) (Lexis 2003); 815 ILL. COMP. STAT. ANN. 511/10 (West Supp. 2004); LA. REV. STAT. ANN. § 14:73.6 (Lexis 2002); NEV. REV. STAT. ANN. § 41.735 (Lexis 2002); N.D. CENT. CODE, § 51-27-03 (Lexis Supp. 2003); OKLA. STAT. tit. 15, § 766.2 (Lexis 2004); 18 PA. CONS. STAT. § 5903(a.1), (l), (m) (West Supp. 2004); S.D. CODIFIED LAWS § 37-24-37 (Michie 2003); TENN. CODE ANN. § 47-18-2501 (Lexis Supp. 2003).

101. Terry Ross, *Virginia Passes the First Felony “Anti-Spam” Law*, MONDAQ BUSINESS BRIEFING, May 27, 2003.

102. CAL. BUS. & PROF. CODE § 17538.4.45 (West Supp. 2004).

103. See Zollers et al., *supra* note 52, at 184; see also Amy Keane, *Validity of State Statutes and Administrative Regulation Regulating Communications under Commerce Clause and First Amendment of the Federal Constitution*, 98 A.L.R.5th 167; see also Amaditz, *supra* note 22.

104. *Gibbons v. Ogden*, 22 U.S. 1 (1824).

105. Note that even with the qualifying clause, internet websites cannot be regulated by the state. As was held in *American Library Ass’n v. Pataki*, since internet sites are not “aimed” at a particular state citizen, the website creator has not availed himself towards any particular state. *American Library Ass’n v. Pataki*, 969 F. Supp. 160 (S.D.N.Y. 1997). However, e-mail seems to be different, since the actual message is purposefully sent to a particular state citizen—indeed, the e-mail user does not fall upon spam by accident as it is purposefully sent to his or her inbox.

106. *Ferguson v. Friendfinders, Inc.*, 94 Cal. App. 4th 1255 (2002).

regulating spam and struck down Commerce Clause challenges. Although *Ferguson* was a private action for damages and *Heckel* was brought by the state Attorney General, both cases resulted in holdings against spammers. Responding to challenges of unconstitutionality under the dormant Commerce Clause, the court held that the local benefits of the Act outweighed the burdens it placed on interstate commerce in the sending of spam.¹⁰⁸

Heckel was a particularly favorable case for spam litigators since the spammer in question resided in a state other than Washington. Accordingly, the question of the location from which the spammer initiated the messages was adjudged as totally irrelevant with respect to the constitutionality of Washington's anti-spam law. The qualification clause was sufficient to avoiding a problem of states' intruding on dormant Commerce Clause jurisdiction.

The courts in these actions also concluded that the defendants' First Amendment rights had not been violated as the laws were narrowly tailored to the goals of the regulation of commercial speech. Note, however, that both the Washington state law and the California state law (which had since been changed for implementation in January 2004) were not outright prohibitions, but, rather, "rules of conduct" on labeling and sending requirements.¹⁰⁹

B. Problems with the State Laws

As these state laws stood, they were an ineffective means of combating the growing spam problem.

1. Labeling and Opt-Out Procedures

The labeling requirement that most states had enacted combated the problem of fraud and sought to protect minors and e-mail users from fraudulent subject lines and adult material. The labeling requirement was also considered useful for private filtering solutions in identifying spam and deleting it before it hit the inbox. Supporters of the labeling requirement claimed that it "enables recipients to filter unwanted e-mails without banning spam outright."¹¹⁰ This approach also imposed the least restrictions on free speech and internet communication.

However, most spammers are already using false headers in order to evade technical filters erected to stop spam from reaching the inbox. Requiring valid subject headers and routing information is simply a legal codification of technical barriers that have been erected to filter spam.¹¹¹

The mandatory opt-out clause in the e-mail is, theoretically, a good idea for avoiding First Amendment conflicts, but in terms of utility in dealing with spam, it is not effective.

As the European Commission on spam, EuroCAUCE, recently concluded, "opt-out" procedures are ineffective because of the sheer scale and administration that spammers are required to take on. "If only 1% of the EU's 18.4 million businesses

107. State v. Heckel, 24 P.3d 404 (Wash. 2001).

108. *Id.*

109. CAL. BUS. & PROF. CODE § 17538.4 (WEST SUPP. 2000); WASH. REV. CODE § 19.190.020 (West 1999 & Supp. 2000).

110. See Amaditz, *supra* note 22, at para. 80.

111. Sorkin, *supra* note 31, at 346.

decided to [take part in opt-out] procedures, it would be possible to have someone employed full-time for a *whole year* doing *nothing else* but issuing ‘remove’ requests at nearly two per minute. . . And that’s just for *one* email address”¹¹² [emphasis included].

In addition, some spammers use false opt-out sites, and frustrated, angry e-mail users frequently ‘bomb’ their webpages, i.e. render them unable to collect e-mail addresses.¹¹³ Spammers are then unable to collect the information and names that they would need to comply with the law and to decrease the amount of spam sent to unwilling recipients. In addition, unrelenting spammers sometimes use the opt-out procedure to validate e-mail addresses. For example, if the e-mail user responds to the message by sending a request to stop receiving messages, the spammer knows that the e-mail address is an active e-mail address.

2. Prohibitions

The most promising state laws for curbing the total amount of spam sent and received were those that totally banned the transmission of spam. Such statutes had been enacted for implementation in 2004 in Delaware and California.¹¹⁴ Although these laws still had enforcement issues (such as exercising jurisdiction over foreign spammers with no economic ties to the United States), they still created a tough policy for domestic spammers. In addition, both the Delaware and the California laws gave the ability to enforce the state laws to the State Attorneys General, ISPs and individual users.¹¹⁵ A distribution of the power of enforcement provided the largest possibility for effective litigation that would, in turn, increase the effectiveness of the legislation.¹¹⁶

C. Federal Legislation: The CAN-Spam Act

Since spam is a national problem with large cost barriers of litigation and eradication, effective legislation will need to be uniform in character and requirements in order to promote efficiency and compliance. Cognizant of the differences between state requirements and aware of the fact that the state laws were seldom enforced, spammers had a huge disincentive to comply with the various state laws. Indeed, the legislative history of the CAN-Spam Act itself points to the fact that state laws had not been successful because e-mail (without geographic location) “can be extremely difficult for law-abiding businesses [and by this the legislation means law-abiding spammers] to know with which of the disparate statutes they are required to comply.”¹¹⁷ In addition, the large variety in state laws prohibited multi-state or multi-private party action on the part of Attorneys General, ISPs or individual consumers across states. Given the large

112. *Opt-in vs. Opt Out*, EuroCAUCE, at <http://www.euro.cauce.org/en/optinvsout.html> (Oct. 29, 2004).

113. *Id.* at 340.

114. Christine E. Lyon, *Client Alert: New California Law Prohibits Unsolicited “Commercial” E-mail*, Mofo Update (Oct. 2003), at <http://www.mofo.com/news/general.cfm?MCatID=&concentrationID=&ID=1082&Type=5>.

115. *Id.*

116. Amaditz, *supra* note 22, at 74.

117. CAN-Spam Act, § 2.

costs of tracking spammers and enforcing the laws against them, a uniform law would provide cost savings if parties across state boundaries might be joined in legal action.

As of January 1, 2004, federal legislation regulating the use of spam went into effect. This law was highly controversial. Advocates of broader consumer and ISP protection claim that Congress had catered to the pro-spam lobby,¹¹⁸ while others were concerned that any federal regulation would stifle internet commerce.¹¹⁹

The law makes it illegal (with punishment of a fine) to send an unsolicited commercial e-mail¹²⁰ which (1) gives false or misleading transmission information¹²¹, (2) provides deceptive headings (subject lines)¹²², (3) does not include a valid return address in physical mail form¹²³, (4) does not provide a valid opt-out procedure in the e-mail message¹²⁴ and (5) does not label adult content messages with the requisite "ADLT" subject header¹²⁵ or (6) is sent to the e-mail user after the user has already requested to stop being sent messages.¹²⁶ The law also gives future power to the FTC to establish a do-not-spam list if the FTC finds it economically feasible and beneficial.¹²⁷

The law gives enforcement power to (1) the FTC, (2) national and member banks, (3) the Securities and Exchange Commission, (4) state insurance authorities, (5) the FCC, (6) state Attorneys General and (7) ISPs.¹²⁸ The law does not provide individual e-mail users, businesses or other private parties a cause of action for harm resulting from spam.

Plaintiffs can seek \$100 per e-mail in statutory damages.¹²⁹ In addition, reasonable attorney's fees will be awarded to plaintiffs.¹³⁰

Federal enforcers can also seek felony charges against a spammer who knowingly (1) intentionally transmits messages through a protected computer, (2) uses a computer to send bulk messages with intent to deceive the recipient as to the origin of the message, (3) materially falsifies header information in bulk e-mail and (4) falsifies information in registering for five or more e-mail accounts and initiates bulk e-mail from those accounts.¹³¹ Violators of this section are subject to a fine or

118. "Critics say the law, a result of compromise after years of Congressional stalemate, places the interests of businesses above those of consumers. . ." Cynthia L. Webb, *Un-Canning Spam*, THE WASHINGTON POST, Dec. 17, 2003, at www.washingtonpost.com.

119. See Clyde Wayne Crews, Jr., *Why Canning 'Spam' Is a Bad Idea*, POLICY ANALYSIS, Jul. 26, 2001, No. 408, at 4.

120. Unsolicited as defined by the federal bill means a lack of previous relationship between the sender and the receiver. CAN-Spam Act, § 1(a).

121. *Id.* § 4(a)(2).

122. *Id.* § 4(a)(3).

123. *Id.* § 5(a)(5).

124. *Id.* § 5(a)(4).

125. *Id.* § 5(d).

126. *Id.* § 5(a)(3).

127. *Id.* § 9.

128. *Id.* § 7(a), 7(b).

129. *Id.* § 6(f)(3).

130. *Id.* § 6(f)(4).

131. *Id.* § 4(a)(1)-(5).

imprisonment of no more than five years.¹³²

In addition to excluding consumers from the enforcement framework, the bill also pre-empts all state spam bills, including those with stronger civil regulatory schemes, such as the laws enacted in California and Delaware.¹³³ The federal law does pressure states to enact their own criminal statutes on spam.¹³⁴

The CAN-Spam Act resembles state bills enacted in Arkansas and Illinois. As previously discussed, these types of statutes serve as “rules of conduct” and should not be considered a prohibition against all spam. The CAN-Spam Act is aimed more at fighting fraudulent headers and routing information. It may by itself indeed prove to be ineffective at combating the growing amount of spam transmitted. As Ray Everett-Church of the E-Privacy Group argues:

The law is a little more than an instructional guide for how to keep pumping out millions of e-mails per hour while avoiding legal liability. CAN-Spam sets forth various dos and don'ts for the spammer who seeks to be legitimate. . . This law is a result of the direct-marketing lobby's success in convincing Congress to redefine the spam problem as being about dishonesty rather than the negative effects of massive volumes of unwanted e-mail.¹³⁵

Indeed, when looking at Congress' findings as its foundation for enactment of the law, one finds that Congress has focused most essentially on stopping fraud in e-mail information rather than protecting inboxes from overflowing with unwanted e-mail. Quoting from the bill's “Sense of Congress,” “spam has become the method of choice for those who distribute pornography, perpetuate fraudulent schemes, and introduce viruses, worms, and Trojan horses into personal and business computer systems. . .”¹³⁶ There is no mention of the costs associated with overflowing inboxes and overloaded servers.

With the enactment of the CAN-Spam Act, the focus has shifted from the state arena to the federal arena and from technical filters to enforcement of the bill for regulation of spam. The hope is that if spam is less well disguised, then technical filters will be able to combat spam more effectively by identifying and deleting messages before they ever hit the inbox.¹³⁷

IV. Enforcement

A. Private Parties

1. ISPs

Private parties have not relied on the presence of state or federal legislation in protecting themselves from spam. E-mail users as well as ISPs have instead used common law remedies to deal with their spam-related grievances. The efficacy of their efforts is questionable; common law remedies cannot serve as the primary means of regulation to curb the growing epidemic.

132. *Id.* § 4(b)(1)

133. *Id.* § 8(b).

134. Dreifach, *supra* note 17.

135. Ray Everett-Church, C.Net.com, *quoted in* Webb, *supra* note 118.

136. CAN-Spam Act.

137. *See infra* Part V.

Because ISPs are the hardest hit by spam and are the most directly affected in cost by the medium, they have been the most active litigators.¹³⁸

The internet's structure makes it particularly tricky to attach liability to wired wrongdoers. Tracking down and prosecuting spammers can be cost- and labor-intensive,¹³⁹ time consuming and particularly ineffective since most spammers are acting on the part of a company and lack sufficient resources to pay large damages.¹⁴⁰ However, ISPs continue to go after spammers—fearing that in the absence of state or federal action, the problem will continue to worsen and the costs of spam will continue to mount.¹⁴¹

The relatively early case, *CompuServe v. CyberPromotions*, established important precedent for ISPs looking to litigate against spammers.¹⁴² CompuServe, which was one of America's largest ISPs, sued Cyberpromotions, a company that created spam for a host of companies, for an injunction against using CompuServe's network for the purpose of mass electronic mailings because it had received a large number of complaints from its subscribers. Despite numerous requests by CompuServe to Cyberpromotions to stop the dissemination of such e-mails (and notifications that such actions were against its use policy), the volume of spam increased. CompuServe reacted by creating spam-filtering software which Cyberpromotions managed to subvert by falsifying information in subject lines and routing information. Such deceptive behavior, CompuServe determined, meant its only solution was litigation.¹⁴³

CompuServe's primary cause of action was common law trespass to chattels.¹⁴⁴ Although trespass to chattels has been primarily relegated to physical items (such as property), the court held that e-mails were sufficiently tangible and physical to constitute trespass and that the defendant's actions were clearly intentional.¹⁴⁵ Although Cyberpromotions had claimed that there was no physical damage, the court rejected this argument, citing the diminished value of CompuServe's server and services to subscribers as well as harm inflicted upon CompuServe's reputation for quality internet service.¹⁴⁶

The *CompuServe* case has served as a weapon for private actors against spammers. ISPs have expanded causes of action against spammers, adding to trespass trademark infringement¹⁴⁷ and false designation of origin.¹⁴⁸

138. Sorkin, *supra* note 31, at 358.

139. Dreifach, *supra* note 17.

140. "Network admins [sic] like Lucas say it's impossible to trace the original spammer back through hijacked computers to other internet locations that have probably long been abandoned." Stone, *supra* note 37, at 68.

141. *See id.*

142. *CompuServe Inc. v. Cyber Promotions, Inc.*, 962 F.Supp. 1015 (S.D. Ohio, 1997).

143. *See Magee, supra* note 25, at 359.

144. *CompuServe*, 962 F. Supp. at 1017.

145. *But see Intel v. Hamidi*, 30 Cal. 4th 1342 (2003).

146. *CompuServe*, 962 F.Supp. at 1028.

147. *See Classified Ventures, L.L.C. v. Softcell Mktg., Inc.*, 109 F. Supp. 2d 899 (E.D. Ill. 2000).

148. *See Verizon Online Servs. v. Ralsky*, 203 F. Supp. 2d 601 (E.D. Va. 2002).

The Lanham Act prohibits the false designation of origin.¹⁴⁹ This cause of action was successfully used by AOL in *America Online v. IMS*, where the court held that IMS (a notorious spammer) had used the AOL name in falsely identifying that the mail came from AOL and had caused sufficient damages to AOL in creating the confusion.¹⁵⁰

The Lanham Act also prohibits trademark dilution, meaning the “reduction of the distinctive quality of a famous or well-known service mark.”¹⁵¹ In *America Online v. LCGM*, AOL brought a claim for trademark dilution, arguing that its famous mark had been tarnished through the defendant’s negative use. The court held that spamming indeed had a negative effect on AOL’s name.¹⁵²

ISPs have also started including anti-spam clauses in their contracts with e-mail users to prevent the use of their e-mail account services for dissemination of spam. They have included a stiff liquidated damages clause that should sufficiently deter breach of contract. *Hotmail Corp. v. Van\$ Money Pie, Inc.* is a case of a successful breach of contract action. Although this case was a straightforward breach of contract case (Hotmail had specified that use of its service for sending unsolicited bulk commercial e-mail was grounds for termination of service),¹⁵³ the court specified that contract provisions must clearly prohibit bulk spamming to be used against the spammer—a mere “breach of netiquette” will not be grounds for breach of contract or for a grant of punitive damages.¹⁵⁴

Even upon winning in court, ISPs have had a hard time collecting damages from defunct spammers. Although Earthlink in July of 2001 won a \$25 million settlement against a Tennessee-based spammer, it has been unable to collect a penny from the now-bankrupt violator.¹⁵⁵

Despite numerous difficulties in litigating against and recovering from spammers, ISPs have continued to sue spammers—whether under new state spam laws or under common law causes of action. As recently as June 2003, Microsoft sued fifteen spammers—fourteen under the Washington spam statute and one under the California spam statute—for sending over two billion messages to its Hotmail and MSN e-mail users.¹⁵⁶ In March of 2004, four large ISPs filed six lawsuits under the CAN-Spam Act against several spammers in various states.¹⁵⁷

ISPs have not been active in litigating against other ISPs who use open proxies and allow their servers to be hijacked to disseminate millions of spam messages. The possibility of forming a trade association and blocking messages from ISPs

149. 15 U.S.C. § 1125(a)(1) (2000).

150. *America Online v. IMS*, 24 F. Supp. 2d 548 (E.D. Va. 1998); see also Magee, *supra* note 25, at 351.

151. *Id.*

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

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

154. Sorkin, *supra* note 31, at 365; Magee, *supra* note 25, at 338.

155. Sam Smith, *N.Y. Moves to Can the Spam: State in Court vs. Snake Oil Mouse Jockeys*, N. Y. POST, Sept. 29, 2002, at 9.

156. Chris Gaither, *Microsoft Sues 15 Firms Over Spam*, BOSTON GLOBE, June 18, 2003, at A1.

157. Chris Gaither, *Rival internet Providers Fight Spam; Yahoo Microsoft AOL and Earthlink use a new law to sue hundreds of bulk e-mailers*, L.A. TIMES, Mar. 11, 2004, at C1.

that do not employ closed proxies is a possibility for combating spam which will be explored in Part IV.¹⁵⁸

2. E-Mail Users

An increasing number of individual e-mail users and individual businesses have used state anti-spam legislation to bring causes of actions against spammers.

For example, a private law firm, Morrison & Foerster, sued spammer Etracks.com for sending spam to its employees through its internet domain mofo.com. Morrison & Foerster had two causes of action: one relating to the use of their server, which was explicitly against Morrison & Foerster's policy, and the other relating to the fact that Etracks.com failed to use the connotations of "ADV"¹⁵⁹ and "ADV: ADLT"¹⁶⁰ in the subject line to identify unsolicited commercial advertisements, which was in violation of California law.¹⁶¹ Morrison & Foerster asked for not only the statutorily allowed fifty dollars per e-mail, an injunction against further e-mails and reasonable attorney's fees, but also that a fund be established from which people affected by Etracks.com's spam might seek restitution.¹⁶²

Although action on the part of individual e-mail users may seem uneconomical,¹⁶³ there has also been much action on the part of private attorneys seeking attorney's fees granted in affirmative judgments. For example, private solo practice attorney Dietrich Biemiller, one year out of law school, has been making a living off the Washington State spam statute by vigorously prosecuting spammers under the Washington state spam statute and collecting reasonable attorney fees.¹⁶⁴

3. Efficacy of Private Party Litigation

Spam is a "unique and novel"¹⁶⁵ problem that can only be effectively addressed through specific and tailored legislation that will seek to regulate spam and curb its costs. Common law actions which attempt to handle the spam problem will be of limited effectiveness. Even in light of legislation directed specifically at spam, litigation by ISPs and individual e-mail users will be less than optimal given disincentives against litigation, including the time- and labor-intensive nature of the suits, the ease of relocating spam operations, as well as the fact that the low resources of many spammers would effectively preclude monetary recovery. As Brady Stone of *Newsweek* notes,

158. Michael A. Fisher, *The Right to Spam? Regulating Electronic Junk Mail*, 23 COLUM.-VLA J.L. & ARTS 363, 396 (2000).

159. CAL. BUS. & PROF. CODE §17538.4 (West Supp. 2000).

160. *Id.*

161. *Morrison & Foerster v. Etracks.com, Inc.*, First Am. Verified Compl., June 28, 2002, (Cal. Super. Ct.), 4-5.

162. *Id.* at 5-6.

163. See Edwards, *supra* note 37, at 117.

164. Gary Young, *FTC Struggles to Gain Ground in War on Spam*, INTERNET NEWSLETTER, Vol. I, No. 6, June 19, 2003, at 3. Biemiller lost his first case in August of 2002. Despite this setback, he has brought more civil cases against spammers, causing opponents to argue that he is using Washington law for his own benefit, and not for his clients'. See Peter Lewis, *Anti-Spam Activist Loses Court Battle, Judge: Man Must Pay Junk E-mailers Legal Fees*, SEATTLE TIMES, Aug. 11, 2001, at B1.

165. Magee, *supra* note 25, at 355.

Private action against spammers, both in and out of the courtroom, has not been effective either. . . civil suits have led to large fines but spammers often don't pay the penalties and survive with operations in tact. ISPs are still committed to the courtroom, though, and continue to file suits in pursuit of big judgments that will scare bulk e-mailers out of business.¹⁶⁶

Civil penalties seem to be nothing more than a slap on the wrist—most spammers, when hit with damages, move to a different internet domain and start the same operations under a different name.¹⁶⁷ It is questionable whether suits by ISPs and private actors gaining civil damages will diminish the level of spam, given the lucrative profits and low risks of penalties for spamming.

B. State Attorneys General and Federal Enforcement

Action on the part of the state Attorneys General, so far, has been limited.¹⁶⁸

State Attorneys General, in their role as consumer protectors, have focused most intensely on protecting e-mail users from fraudulent schemes,¹⁶⁹ communication of sexually explicit materials to minors,¹⁷⁰ as well as prosecuting spammers who open fraudulent e-mail accounts.¹⁷¹ Since fraud has historically been regulated at the state level, state Attorneys General have focused on regulating spam involving fraudulent rooting information, pyramid and phishing schemes and other deceptive activities.¹⁷²

State Attorneys General are most often tipped off by private parties who receive multiple complaints from customers about a particular spammer.¹⁷³ Complaints are

166. Stone, *supra* note 37, at 68.

167. Take, for example, *Verizon Online Servs. v. Ralsky*, 203 F. Supp. 2d 601 (E.D. Va. 2002). Ralsky was sued by Verizon for \$37 million for sending bulk e-mail to Verizon customers, but settled two years into the suit. Ralsky paid an undisclosed sum to Verizon, in addition to agreeing not to e-mail Verizon customers. However, Ralsky didn't stop spamming. He simply moved his operations off-shore to a different network in China. See Stone, *supra* note 37 at 68.

168. California won its first spam case in 2003 against PW Marketing of Southern California. Reuters, *Anti-Spam Law Victory*, BOSTON GLOBE, Oct. 25, 2003, at D1. Christine Gregoire, Attorney General of the state of Washington, brought suit in August, 2002 against a Minnesota-based debt consolidation group which used deceptive subject headers to advertise its services. *United States: Washington Attorney General Sues Minnesota Debt Consolidators for Spam Law Violations*, MONDAQ BUSINESS BRIEFINGS, Aug. 2, 2002. New York State Attorney General Eliot Spitzer brought a lawsuit in 2002 against Niagra Falls-based spammer MonsterHut, Inc. president Todd Pelow; the action was based on MonsterHut's false representations that it operated on an 'opt-in' basis. This was the state's first spam case. *Spitzer Sues MonsterHunt.com; State's First Spamming Case*, BUFFALO NEWS, May 29, 2002, at B4.

169. *State v. Heckel*, 24 P.3d 404 (Wash. 2001).

170. See *Hatch v. Superior Court*, 94 Cal. Rptr. 2d 453 (4th Dist. 2000); see also *People v. Foley*, 94 N.Y.2d 668 (N.Y. 2000).

171. For example, Eliot Spitzer's arrest of Buffalo based spammer Howard Carmack in 2003 for opening EarthLink accounts with stolen credit cards. Carmack was charged with credit card fraud. Spitzer did not charge him with sending over 825 million spam e-mails. Stone, *supra* note 38, at 68; see also Fred O'Williams, *Heading Set for City Man in Spam Case*, BUFFALO NEWS, Oct. 9, 2003, at C6.

172. Zollers et. al, *supra* note 52, at 180.

173. On December 19, 2003, Microsoft and Eliot Spitzer, the Attorney General for the state of New York, jointly filed civil charges against Scott Richter, president of a Colorado based spamming operation, Justin Champion, president of a Manhattan based spamming company and Paul Boes of a Texas based ring. To "trap" the spammers and collect evidence for their cases, Microsoft set up a test

also fielded to the Consumer Protection Division or Internet Bureau of the State Attorney General's Office.¹⁷⁴

State Attorneys General had been most willing in previous years to prosecute aggravated spamming where location of the spammer could be easily identified.¹⁷⁵

Towards the end of 2003, with increasing attention being paid to the mounting costs of spam and prospective federal legislation, state Attorneys General began attacking some notorious large spammers.¹⁷⁶ This included an action by Eliot Spitzer, who did not use a spam-specific statute (New York state did not have one), but instead sued the world's third largest spammer for deceptive business practices.¹⁷⁷

Although state Attorneys General have banded together through the National Association of Attorneys General (NAAG) to establish a commission on computer crimes,¹⁷⁸ perhaps because of the variation in state legislation or the "back-burner" status of the spam issue in comparison to other hot topics, NAAG has been weary of waging a multi-state action against the large spammers.

The FTC was inactive in regards to spam until the middle of 2002. After February 2002, the FTC filed fifty-seven charges against spammers, but under unfair and deceptive business practices, as there was no specific spam-related legislation until December 2003.¹⁷⁹ In one case, settled in 2002, the FTC brought an action against CyberData for deceptive business practices in selling 20,000 e-mail addresses.¹⁸⁰ Because the federal government had no specific federal cause of action and no authority to bring criminal sanctions, its overall activity level had been quite low in combating the spam problem.¹⁸¹ Indeed, even FTC spokesperson Claudia Bourne Farrell admits that "the agency [didn't] have the wherewithal to

account on which 8,799 e-mails had been caught in two weeks which made a total of 40,000 fraudulent claims. Mark Harrington, *Spitzer, Microsoft Jointly File Anti-Spam Lawsuit*, NEWSDAY, Dec. 19, 2003, at A70.

174. Take, for example, *Heckel*, where the Consumer Protection Division of the Washington State Attorney General's Office had received complaints from Washington's recipients of Heckel's spam both because the scheme was a fraud and because, even after informing Heckel that they no longer wanted to receive messages from him, he continued to bombard them with spam. *Heckel*, 24 P.3d. 405.

175. Washington State's consumer protection head, David Hill, wrote Heckel a letter which Heckel contested in a phone call to Hill and flouted Hill's demand to follow the state anti-spam law. Heckel's case was an easy one—his location could be easily identified, as he a physical post address to which payment for the product was to be sent. In addition, Heckel was also engaged in fraudulent conduct. Heckel was selling a product under the name "Natural Instincts" and when payment was sent to the address in Salem Oregon, no product was received. *See id.* *See also* Dreifach, *supra* note 17.

176. In December 2003, Virginia made its first criminal indictment by charging Jeremy James, the eighth most prolific spammer in world, and Richard Rutowski under the Virginia anti-spam law. *See* Jon Chesto, *Virginia spam law nets first felony charges vs. e-mailers*, BOSTON HERALD, Dec. 12, 2003, at 2.

177. Saul Hansell, *Spitzer Files Suit Against 3 Over Spam*, N.Y. TIMES, Dec.19, 2003, at C4.

178. *See NAAG Initiatives: Computer Crime Point-of-Contact List*, National Association of Attorneys General, at www.naag.org/issues/20010724-cc_list_bg.php (last visited Oct. 13, 2004).

179. There was no federal cause of action for spamming until the CAN-Spam Act. *See Spam Wars: Federal Agencies Focus on Criminals*, ATLANTA JOURNAL-CONSTITUTION, Dec. 15, 2003, at 48.

180. Young, *supra* note 164, at 3.

181. *Id.*

tackle the whole problem.”¹⁸²

The US Department of Justice had been active only in fighting crimes perpetrated through spam, such as child pornography and fraudulent schemes.¹⁸³

V. The New Role of the FTC, ISPs and State Attorneys General

The CAN-Spam Act re-focuses the attention being paid to spam from the state level to the federal level where, some might argue, the focus belongs. Indeed, spam, as an internet problem, is an issue that transcends boundaries and affects states and countries simultaneously.

In addition, the CAN-Spam Act has put pressure on federal and state government agencies, as well as on private actors, not only to enforce the law but also to seek technical solutions in coordination with the Act. As John Mozena of the Coalition Against Unsolicited Commercial E-mail comments,

The law’s success. . .depends on several factors including how much state and federal law enforcers can prosecute illegal junk e-mail operations; whether or not the Federal Trade Commission can design an effective do-not-spam list; and whether setting rules for legitimate marketing e-mail prompts bulk e-mailers to play by rules that give recipients an easy way to opt out of future mailings.¹⁸⁴

This coordination becomes even more important when one examines the inability of the CAN-Spam law to curb all spam¹⁸⁵ and the expenses and incentives associated with litigation.

Before the passage of the CAN-Spam Act, although state laws varied in their protection of consumers against spam, some states had very strong laws that went as far as banning all spam. The CAN-Spam Act has pre-empted all state civil laws, including those that offered more protection to e-mail users and ISPs. By pre-empting state civil spam laws, all actions brought by ISPs, State Attorneys General, the Federal Government and the other named parties (SEC, etc.), will have to be under (1) common law (which, as discussed above, does not provide an effective cause of action), (2) state consumer protection laws (which are aimed at protecting consumers from fraud—not reducing the total amount of spam clogging networks), (3) felony state spam laws, or (4) the CAN-Spam Act.

Considering that individuals cannot sue under the CAN-Spam Act (and are now preempted from suing under state anti-spam laws), e-mail users have become an unprotected class. Class action suits that would have proved fruitful by the banding together of legal resources and plaintiff’s bar are no longer a form of enforcement. As private attorney-at-law Biemiller reports, private individuals must now rely on overburdened government agencies to protect their inboxes from overflowing with spam.¹⁸⁶

Given that e-mail users have no remedy under either state or federal law, state Attorneys General and the FTC, in their role as consumer protectors, must now step

182. *Id.*

183. *Spam Wars: Federal Agencies Focus on Criminals*, *supra* note 179, at 48.

184. *See Webb*, *supra* note 118.

185. Spam is legal if properly labeled.

186. Young, *supra* note 164.

in and vigorously enforce the CAN-Spam Act. The FTC and state Attorneys General have a duty to enforce the law not only because of the substantial costs imposed on e-mail users and ISPs by spam, but also because the purpose of the CAN-Spam Act is to prevent fraud over e-mail and to protect the privacy of individual e-mail users and ISPs (a duty that a majority of the State Attorney Generals are given).¹⁸⁷ This requires concerted effort at establishing an effective internet division to field complaints, as well as coordinating efforts with ISPs and domain users who have first-hand knowledge of violations.

Even though the CAN-Spam Act pre-empts more protective legislation (like the laws of California and Delaware), the federal bill may prove to be more beneficial for state and federal actors for several reasons. First, since spam is an inherently national problem, the law refocuses energies and attention on spam as a federal problem and involves the federal government more specifically. Second, a federal bill allows uniformity of requirements and therefore provides a foundation for multi-state action. This also allows for coordination between state Attorneys General of information and cost/labor sharing for investigations and prosecutions. Third, state Attorneys General and ISP's in states that had not enacted spam-specific statutes (such as New York) have been granted a cause of action as well as the possibility of gaining reasonable attorney's fees from prosecution. This may increase litigation in states that had previously not gone after spammers. In addition, plaintiffs can now choose to bring their case in either state or federal court.¹⁸⁸

ISPs, as the most heavily impacted parties in the spam battle, can recover their own damages by suing under the CAN-Spam Act for \$100 per violation with a maximum recovery of \$1,000,000 per day.

ISPs face disincentives to bring anti-spam suits since litigation costs are high, monetary recovery post-judgment is uncertain and ISPs can simply pass the higher costs onto their subscribers in the form of higher prices.¹⁸⁹ However, ISPs are not totally deterred from bringing suits as they compete among themselves on quality of service and price.¹⁹⁰

ISPs have other means of combating the spam problem, in addition to litigation against spammers. Legitimate ISPs have proposed banding together in a trade union and automatically rejecting messages from servers that have remained "open proxies" (thus havens for transmission of spam). The banding together of large ISPs has potential anti-trust implications, as the coordination of some large ISPs would seem to be suppressing competition from smaller, less technically savvy companies.¹⁹¹

Other technical solutions besides filters have been proposed by ISPs, including the recent announcement by Yahoo! that it would implement an authentication

187. Amaditz, *supra* note 22, at 63.

188. Dreifach, *supra* note 17.

189. Joshua Marcus, *Commercial Speech on the Internet: Spam and the First Amendment*, 16 CARDOZO ARTS & ENT. L.J. 245, 250 (1998); Magee, *supra* note 25, at 338.

190. Dreifach, *supra* note 17.

191. See Fisher, *supra* note 158, at 396.

2004]

OPTING-OUT

127

system starting in 2004:

Under Yahoo's new architecture, a system sending an e-mail message would embed a secure, private key in a message header. The receiving system would check the internet's domain name system for the public key registered to the sending domain If the public key is able to decrypt the private key embedded in the message, then the e-mail is considered authentic and can be delivered. If not, then the message is assumed not to be an authentic one from the sender and is blocked.¹⁹²

With such a system in place, locating the actual situs of messages would prove easier (thus facilitating less costly litigation if the message turns out to be fraudulent) and e-mail users might be able to reduce the amount of spam by filtering out all e-mail that came from "unauthenticated" sources.¹⁹³

However, the technical solutions implemented by ISP's alone will not suffice to stem the spam problem. The benefits of the federal bill may be wasted if the bill is not enforced against spammers. Relying solely on technical barriers to eradicate the growing amount of spam is likely to fail, as it has in the past. "Spammers are an elusive lot. They have been able to defeat filtering software, evade professional spam hunters and use a host of tricks to shroud the origination point of their spam messages."¹⁹⁴ Indeed, filters are useless unless the source of the message or the subject can be accurately identified—a requirement that only effective enforcement of the CAN-Spam act can bring.

On the other hand, enforcement alone will also prove ineffective. Unless enforcement is accompanied by technical solutions that would filter subject headers or authenticate addresses, implementing the CAN-Spam Act by ISPs, state Attorneys General and the federal agencies will not decrease the amount of spam. Enforcement may weed out fraudulent information in spam. But reducing the total amount of spam depends on the coordination of the two efforts—enforcement of the CAN-Spam Act (to label messages correctly) and the creation of effective technical barriers (to "catch" spam before it overloads inboxes and servers).

The FTC recently released a report on the establishment of the national "Do-Not-E-mail" registry, stating that a "Do-Not-E-mail" list would do more harm than good.¹⁹⁵ The FTC concluded that such a list would be a way for spammers to get their hands on a list of valid e-mail addresses. The FTC emphasized a need for the implementation of an authentication system—however the timetable for the creation of such a standard and the funding for such mechanisms were omitted from the FTC's report. The FTC did recommend that, once such measures are created, they should be mandated.

In this respect, state Attorneys General and the FTC have two important roles in not only bringing cases against spammers, but also encouraging private parties to

192. *New authentication systems tries to block Spam*, CNN.COM, Dec. 5, 2003, at <http://edition.cnn.com/2003/TECH/internet/12/05/spam.yahoo.reut/>.

193. Johnson, *supra* note 89.

194. Amaditz, *supra* note 22, at 70.

195. National Do Not Email Registry: A Report to Congress, *supra* note 20.

invent and implement technical barriers.¹⁹⁶ In the face of the CAN-Spam Act, emphasis must be placed on both of these actions in order not only to ameliorate the problem of fraudulent information in spam, but also to stop spam from being a growing percentage of e-mail sent and received.

Efficacy of enforcement by any party also depends on the extent to which spammers move abroad and the degree to which foreign governments comply with U.S. law enforcement officials in prosecuting off-shore spammers. Domestic enforcement of the CAN-Spam Act may simply force spammers to locate outside of the United States. An increasing amount of off-shore spammers might create more problems of jurisdiction, costs and enforcement. As Kelley D. Talcott, a partner at Pennie & Edmonds, points out,

[b]ecause the act requires the recipient to “opt out” of receiving spam, it will be a simple matter for foreign spammers to make their messages appear as if they are complying with the requirements of the act. Recipients, conditioned by domestic spammers that have complied with the act, may very well respond to the foreign spam with opt-out requests. By doing so, the recipient will have confirmed the viability of their e-mail addresses so that the foreign spammers can target those addresses for more spam.¹⁹⁷

Foreign prosecution is a viable option for enforcers of the CAN-Spam Act, but it requires cooperation of foreign governments. Microsoft has recently joined forces with foreign government agencies to sue spammers in Taiwan, South Korea and Japan.¹⁹⁸ Should foreign government assistance be required, federal government agencies might be better positioned to prosecute off-shore spammers than state Attorneys General due to the international nature of the claims.

The CAN-Spam Act has refocused spam as a worldwide problem. A federal bill as a uniform national standard can allow the United States to cooperate more with foreign nations and to put more pressure on foreign nations to implement similar spam laws. Indeed, it is not enough for one nation or a handful of nations to attempt to eradicate spam, just like it was not enough for one state or a handful of states to enact spam laws. Some countries will inevitably become safe havens for spammers and scam artists.¹⁹⁹

CONCLUSION

Preliminary results from the CAN-Spam Act are not good—estimates indicate that the amount of spam has actually *increased* since the enactment of the CAN-Spam Act.²⁰⁰ It is clear that as the law stands, and with the relative inaction of the FTC, state Attorneys General and ISPs, it is an ineffective means of combating the

196. *Id.*

197. Kelley D. Talcott, *Canning Spam*, N.Y.L.J., Dec. 18, 2003, at 5.

198. Raju Chellam, *Microsoft slams spam ring; It joins govt organizations to file lawsuits against individuals in the US, Taiwan, S Korea, and Japan*, BUS. TIMES SINGAPORE, Dec. 22, 2003, at B1.

199. *Spam world: Global effort needed to end scourge*, SAN DIEGO UNION-TRIBUNE, July 28, 2004, at B-8.

200. Bedell, *supra* note 7, at 1D.

volume of spam. Given the general ineffectiveness of the law and the FTC's emphasis on technical solutions, it is clear that the federal government must return to the drawing board in order to create a better spam statute. That legislative solution should come in the form of a constitutionally permissible ban or a coordinated legal and technical solution.

If the United States needs help divining an effective spam-reducing scheme, it might look to Nigeria. Nigeria, which implemented both technological and legislative solutions to halt the proliferation of spam, had the reputation in 2002 for being a gateway for spam.²⁰¹ The country then began working with Barracuda a country based company which develops anti-spam solutions, to stop *outbound* spam e-mails. Nigeria then made it mandatory for all ISPs to install outbound e-mail filtering.²⁰² Preliminary results from these efforts are encouraging—Nigeria has seemingly successfully combated the spam problem and Nigeria is no longer considered a “safe haven” for spam.²⁰³

As it stands, the CAN-Spam Act has proven, so far, to be an ineffective tool at tackling spam, and it is unlikely that the law will yield further positive results. Federal legislators should take a more stringent stance on spam and either ban the medium in totality (or to the extent permissible by the constitution) or force private parties and government agencies to start inventing and implementing effective technological measures.

201. Chandra Devi, *Using laws and tools to fight spam*, NEW STRAITS TIMES (Malaysia), May 20, 2004, at 18.

202. *Id.*

203. *Id.*