THE CAN-SPAM ACT: AN INSUFFICIENT RESPONSE TO THE GROWING SPAM PROBLEM

By Lily Zhang

Although "Spam"[1] is tasty in a can, it is never tasty when it lands in our e-mail inboxes. Spam is an especially pernicious form of advertising because of its low cost, high-volume nature. Traditional advertisers, such as telemarketers and junk mailers, incur significant costs by employing workers, paying long-distance telephone bills, and buying envelopes and paper. In contrast, spammers expend significantly less and even shift costs to recipients, who must sort through the voluminous spam they receive. Thus, spam's attractive nature has led to many abusive uses, which all contribute to the growing spam problem.

As spam becomes a daily nuisance, various responses are being utilized to combat it. Earlier methods employed vigilantism in the forms of self-regulation and self-help, but more sophisticated methods quickly emerged. Those methods included suits against spammers under both common and state law doctrines and technological responses such as filtering. Then in December 2003, the federal government enacted the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act or "the Act") to provide a uniform federal body of law against spamming.[2]

While the Act attempts to curb the spam problem, it still has some shortcomings. Some of the criticism heaped upon the Act centers around its preemptive effects on stricter state spam laws, the severity of the penalties, and its alleged attempt to curb spammers' constitutional rights. Much of the criticism also accuses the Act of potentially increasing the amount of spam because the Act merely provides a set of guidelines for spammers on how to spam legally—in effect legitimizing spam. Many critics believe that the Act will lead more advertisers to rely on spam as their preferred method of advertising.

---

1. See White Buffalo Ventures, LLC v. Univ. of Tex., No. A-03-CA-296-SS, 2004 U.S. Dist. LEXIS 19152, at *3 n.1 (W.D. Tex. Mar. 22, 2004) (noting that the term "spam" started in Internet chat rooms and interactive fantasy games "where someone repeating the same sentence or comment was said to be making a spam" and that "[t]he term referred to a Monty Python's Flying Circus scene in which actors keep saying 'Spam, Spam, Spam, and Spam' when reading options from a menu") (citation and internal quotation marks omitted).

2. 15 U.S.C.A. §§ 7701-7713 (Supp. 2004).

Although some of the prior and current methods of combating spam have been mildly successful, their success has been tempered by one factor: the Internet. As the medium used to propagate spam, the Internet allows spammers to disguise their e-mail addresses, utilize stolen e-mail accounts, and operate across borders. Consequently, the Internet complicates the ability to bring suit or apply legislation against spammers. Moreover, technological responses are costly and not always foolproof. As a result, an effective response to spam must include both technological and legislative components.

This Note provides a brief overview of spam, its characteristics, the problems associated with it, and responses to combat this problem. Part I discusses the fundamentals of spam: its economic structure; the profile of spammers and how they are funded; and spam's attractiveness compared to traditional methods of advertising. Part II focuses on the various techniques used to combat spam, ranging from vigilantism to state legislation to common law causes of action. Part III discusses the CAN-SPAM Act, its weaknesses, and its strengths. Part IV discusses the more progressive and technology-based solutions proposed by various sectors within society. Ultimately, the best response to combating the spam problem is not found in any one of these solutions alone. Rather, spam's unique nature mandates a combination of these solutions, both technological and legislative.

I. OVERVIEW OF SPAM

A. The Rise of Spam

Electronic mail, commonly known as e-mail, began in 1965 and quickly became a method of communication for users to pass messages between different computers.[3] As the Internet increased in popularity and usage in the mid-1990s, e-mail usage became widespread.[4] Concomitant with the rise in e-mail usage, "spam" messages increasingly appeared in e-mail inboxes, becoming a major nuisance.

Generally, e-mail recipients associate "spam" with e-mail that market various products. However, spam refers to other categories of messages as well. Spam is frequently defined as either unsolicited commercial e-mail

3. *See, e.g.*, *Email*, MICROSOFT® ENCARTA® ONLINE ENCYCLOPEDIA, *at* http://encarta.msn.com/encyclopedia_761566348/E-Mail.html (last visited Mar. 2, 2005).

4. *Id.*

(UCE) or unsolicited bulk e-mail (UBE).[5] UBEs encompass not only UCEs but also various forms of non-commercial spams, including opinion surveys, fundraising solicitations, religious and political messages, and chain letters.[6] Thus, spam can take various forms outside of mere commercial marketing.

However, the greatest quantity of spam is still commercial in nature.[7] Most state laws define "commercial e-mail" as e-mail that "advertises or promotes the sale or lease of goods, services, or real property."[8] Under the CAN-SPAM Act, commercial e-mail is similarly defined as "any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service."[9] Furthermore, commercial e-mail does not include transactional or relationship messages, those which serve the primary purpose of facilitating, completing, or confirming a commercial transaction that the recipient has previously agreed to enter with the sender.[10] Essentially, the Act's definition of spam focuses on messages that are *unsolicited* commercial e-mail—the UCEs, which are the messages that clog our inboxes daily.

B. The Problems Associated With Spam

1. General Overview

Spam has established itself as a preferred method of advertising among some because of its quick, cheap, and efficient nature. Spam is quick because it is received within minutes and need not be manually processed and delivered. Because spam messages can be sent to millions of e-mail addresses very quickly, it is more effective in reaching large numbers of consumers than traditional junk mail or telemarketing.[11] Additionally, unlike traditional junk mail or telemarketing, the cost of sending spam

5. Adam Zitter, Note, *Good Laws For Junk Fax? Government Regulation of Unsolicited Solicitations*, 72 FORDHAM L. REV. 2767, 2775 (2004).

6. *Id.*

7. *Id.*

8. Jordan M. Blanke, *Canned Spam: New State and Federal Legislation Attempts to Put a Lid On It*, 7 COMPUTER L. REV. & TECH. J. 305, 307-08 (2004).

9. 15 U.S.C.A. § 7702(2)(A) (Supp. 2004).

10. *Id.* § 7702(2)(B); *see also*, John E. Brockhoeft, *Evaluating the CAN-SPAM Act of 2003*, 4 LOY. L. & TECH. ANN. 1, 5 (2004) (discussing the various categories of spam e-mail).

11. *See, e.g.*, Jacquelyn Trussell, *Is the CAN-SPAM Act the Answer to the Growing Problem of Spam?*, 16 LOY. CONSUMER L. REV. 175, 176 (2004).

does not rise proportionally to the number of e-mails sent.[12] Such advantages help to explain the estimated 2 *trillion* spam messages sent in 2004, one hundred times the volume of "snail" mail advertisements delivered by the United States Postal Service last year.[13] Spam's inherent advantages undoubtedly make spam a desirable form of advertising.

Furthermore, spam advertising is cost effective because spammers need generate only a small percentage of sales in order to garner a profit.[14] A 2002 Wall Street Journal study noted a case in which, among 3.5 million spam messages sent, only eighty-one resulted in a purchase.[15] The success rate in this case was 0.0023% with each sale generating $19 in profit, netting a total profit of $1500 in the first week alone.[16] The cost of sending the 3.5 million spam messages was $350, a small price to pay for generating a profit that was more than four times as much.[17] Spammers are able to generate such a large amount of profit because there is no per-message charge for every piece of spam sent.[18] Instead, a spammer's overhead costs are negligible and confined to equipment, monthly rental fees for an e-mail account, if any, and sometimes the price of a mailing list.[19] Such costs are much less than those associated with telemarketing or paper mailers, activities which can cost hundreds of thousands of dollars because of the various costs imposed, such as telephone bills, postage, paper, staffing, and facilities.[20] One study estimates that the minimum cost for mailing ten thousand letters would be $3,925.[21] Thus, a spammer can potentially send millions of messages for a few hundred dollars, far less than what traditional advertisers have to pay.[22]

---

12. *See, e.g.*, John Magee, *The Law Regulating Unsolicited Commercial E-Mail: An International Perspective*, 19 SANTA CLARA COMPUTER & HIGH TECH. L.J. 333, 338 (2003).

13. *See, e.g.*, Trussell, *supra* note 11, at 177.

14. *See* Sameh I. Mobarek, Note, *The CAN-SPAM Act of 2003: Was Congress Actually Trying to Solve the Problem or Add to it?*, 16 LOY. CONSUMER L. REV. 247, 248-49 (2004).

15. *Id.*

16. *Id.*

17. *Id.*

18. *See* Zitter, *supra* note 5, at 2776.

19. Scot M. Graydon, *Much Ado About Spam: Unsolicited Advertising, the Internet, and You*, 32 ST. MARY'S L.J. 77, 82-83 (2000).

20. Larry Riggs, *Special Report: Costs: Telemarketing*, DIRECT, Mar. 15, 2001, *at* http://www.directmag.com/mag/marketing_special_report_costs_3; Alex Stevenson, *The Dollars and Sense of Direct Mail Advertising for Publishers*, PMA, June 1999, *at* http://www.pma-online/org/scripts/shownews.cfm?id=180.

21. Riggs, *supra* note 20; Stevenson, *supra* note 20.

22. Riggs, *supra* note 20; Stevenson, *supra* note 20.

2. *Not Your Regular Old Advertising Scheme: Spam's Unique Cost-Shifting Structure*

Unlike traditional methods of advertising, spam imposes the bulk of advertising fees on recipients rather than spammers. Spam is junk mail that arrives "postage-due."[23] On a daily basis e-mail users' inboxes are clogged with spam, requiring the expenditure of considerable amounts of time separating spam e-mail from legitimate e-mail. The problem is significant because of the volume of spam sent, as well as the fact that much spam disguises its commercial nature until opened. Spam recipients may have to pay for additional disk space for their e-mail accounts in order to accommodate the influx of messages due to spamming.[24] Some remotely-located Internet users may even incur higher long-distance Internet connection fees as they spend time deleting spam.[25] Thus, individual recipients can potentially incur substantial monetary and non-monetary costs.

Spam also translates into real costs at the workplace. Productivity decreases as employees are forced during working hours to weed out spam e-mail in their inboxes.[26] Such decreases in productivity are reflected in a recent study estimating that spam costs U.S. companies around $9 billion annually.[27] The increased cost faced by companies in the fight against spam is ultimately passed on to consumers in the form of increased prices for the companies' goods and services.[28]

Much of the cost is also shifted to Internet Service Providers (ISPs). Many spammers engage in "Dictionary Attacks," where they send millions of spam messages to e-mail addresses generated by going through the entire alphabet in each letter placeholder of an e-mail address.[29] As a result of this and other spamming techniques, much of the e-mail sent gets bounced because many of the automatically generated addresses are non-functioning.[30] ISPs must then expand their networks and systems not only to accommodate the large quantity of spam but also to process bounced messages.[31] Additionally, ISPs must devote significant monetary resources

---

23. *See, e.g.*, Frequently Asked Questions About Spam, http://spam-mirror.idefix.net/faq (last visited Mar. 2, 2005).
24. *Id.*
25. *Id.*
26. *Id.*
27. Mobarek, *supra* note 14, at 250-51.
28. *Id.*
29. *Id.*
30. *Id.* at 251.
31. *Id.*

to hire personnel to field subscribers' spam-related complaints.[32] One recent study found that spam costs both United States and European ISPs $500 million annually in the form of providing additional server and network capabilities.[33] Like costs imposed at the workplace, the costs incurred by ISPs are also passed onto consumers in the form of higher Internet usage fees.[34]

Spam also creates other secondary costs by forcing the private market to combat spam by using e-mail filters. ISPs spend significant resources implementing filtering mechanisms in their e-mail programs as a way to block spam and maintain customer satisfaction.[35] In addition, private companies offer filtering programs to combat spam. Recently, more sophisticated filters known as Bayesian filters are being used to block out spam in users' inboxes.[36] These filters search for patterns of words that are close to those patterns found in recognized spam messages.[37] Bayesian filters take filtering a step further in that they can "learn" to differentiate between certain terms and patterns that are characteristic of spam versus those that are characteristic of legitimate e-mail.[38] Although some filters are provided free as a part of Internet service, the more effective filters, as rated by Consumer Reports, cost around thirty to forty dollars, a cost that might be prohibitive for some e-mail users.[39] In addition, by the time filtering is being utilized, many of the costs associated with spam have already been incurred. Although the recipient may automatically remove filtered messages to their computer trash can, the spam at this point has already used ISPs' bandwidth, passed through ISPs' staff and filters, and used the recipients' connection time and computer space.[40] Consequently, filters will not alleviate many of the problems associated with spam be-

---

32. Christopher D. Fasano, *Getting Rid of Spam: Addressing Spam in Courts and in Congress*, 2000 SYRACUSE L. & TECH. J. 1, 4.

33. *Id.*

34. *See* Magee, *supra* note 12, at 339.

35. Cindy M. Rice, Comment, *The TCPA: A Justification for the Prohibition of Spam in 2002? Unsolicited Commercial E-Mail: Why is it Such a Problem?*, 3 N.C. J.L. & TECH. 375, 382 (2002).

36. Jeffrey D. Sullivan & Michael B. de Leeuw, *Spam After CAN-Spam: How Inconsistent Thinking Has Made a Hash Out of Unsolicited Commercial E-Mail Policy*, 20 SANTA CLARA COMPUTER & HIGH TECH. L.J. 887, 920 (2004).

37. *Id.*

38. *Id.* at 920-21.

39. *See, e.g.*, *CR Investigates. Protect Yourself Online*, CONSUMER REPS., Sept. 2004, at 12 (2004) (discussing problems with the CAN-SPAM Act and suggesting anti-spam software to lessen the amount of spam received).

40. Gary Miller, *How to Can Spam: Legislating Unsolicited Commercial E-Mail*, 2 VAND. J. ENT. L. & PRAC. 127, 130 (2000).

cause filters perform their function after much of the damage has already been done.

Furthermore, filters could impose additional costs on consumers through over-protection. There is a risk that filters will incorrectly identify legitimate e-mail as spam messages, resulting in the rejection of legitimate messages from a user's e-mail inbox.[41] One report tested numerous filtering programs, all of which failed to filter out 100% of spam messages.[42] The study found that while the most effective program claimed to filter out 95% of spam, actual users reported a rate of only 70%.[43] Furthermore, there is a risk that spammers will eventually tailor their e-mail text to include words and phrases that are uncharacteristic of spam, and that such messages will bypass the filters.[44] These risks suggest that filters should not be overly relied upon as a technological response.

The problem with spam is further aggravated because, unlike traditional junk mail or telemarketing, recipients of spam incur costs regardless of whether the message is opened. With traditional advertising campaigns, recipients can simply discard the mailing if there is no interest by tossing it into the garbage or opting for removal from telemarketing lists by joining the Federal Trade Commission's (FTC) Do-Not-Call list. Although spam recipients can also discard the messages, the process of discarding spam imposes many more costs. Such costs include the usage of valuable disk space, decreased productivity as recipients sift through legitimate and spam e-mail, loss of customer satisfaction, and costs associated with filtering programs. Thus, even if recipients can eventually discard spam, the costs incurred prior to and during removal are generally much greater than those associated with traditional advertising.

3. *The Offensive and Deceptive Nature of SPAM Also Distinguishes It from Traditional Methods of Advertising*

Not only is spam a problem because it shifts the costs from senders to recipients, but spam messages are also often offensive and deceptive. An FTC study reported that 100% of e-mail addresses posted in chat rooms and 86% of addresses posted in newsgroups and webpages received spam

41. *Id.*

42. *See* Sharon D. Nelson & John W. Simek, *Canning the Spam: Unclogging Law Firm Mailboxes*, 64 OR. ST. B. BULL. 9, 12-14 (2004) (discussing filter programs used to sift out spam and testing various filtering software, a combination of which failed to sort out 100% of spam messages received).

43. *Id.* at 12.

44. Sullivan & de Leeuw, *supra* note 36, at 920-21.

messages.[45] Among the most common types of spam are those that advertise "get-rich-quick" schemes,[46] pornographic websites, and pirated software.[47] Another FTC study revealed that among a random sampling of one thousand spam e-mails, 20% of the messages offered a variety of business investment opportunities, 18% offered adult-oriented products/services, and 17% involved financial products such as mortgages and credit cards.[48] In this same study, 40% of all the spam contained false information in the body of the message, 33% exhibited false information in the "from" line of the message, and 22% in the "subject" line of the message.[49] Among all the messages sampled, two-thirds contained some form of deception.[50] Furthermore, the study found that only 63% of the "remove me" or "unsubscribe" options in the messages actually worked.[51]

These statistics demonstrate the increased costs e-mail recipients must incur. False information in the body of the message, subject line, and sender line will inevitably lead some recipients to open the message, only to discover that the e-mail is of a completely unexpected and undesirable nature. As a result, recipients cannot rely on such signals to determine whether the e-mail is spam. Instead, they will have to expend time and energy to physically sort through the e-mail to determine which ones are truly spam.

---

45. Blanke, *supra* note 8, at 305.

46. Recently, the Nigerian e-mail fraud has emerged as an example of a "get rich quick" scheme gone awry. This scheme occurs when a criminal sends out thousands of spam messages luring recipients to pay certain fees in exchange for helping the sender, disguised as a high ranking official, transfer millions of dollars to the spam recipient. According to the FBI, in 2001, about 2,600 people in the United States reported problems with the Nigerian e-mail fraud, and of that number, sixteen claimed financial losses totaling $345,000. Additionally, in some cases, recipients have been lured to Nigeria to pay for the fees. Upon their arrival, victims are held against their will, beaten, and blackmailed. The frequently offensive and even dangerous contents found in spam messages differentiate it from traditional modes of advertising that usually do not result in such deception and risk. *See, e.g.*, Michelle Delio, *Meet the Nigerian E-Mail Grifters*, WIRED-NEWS, July 17, 2002, *at* http://www.wired.com/news/culture/0,1284,53818,00.html; Aaron Larson, *Nigerian Email Fraud—419 Scams*, EXPERTLAW, June 2004, *at* http://www.expertlaw.com/library/pubarticles/Consumer_Protection/spam_email_fraud2.html.

47. Christopher Scott Maravilla, *The Feasibility of a Law to Regulate Pornographic, Unsolicited, Commercial E-Mail*, 4 TUL. J. TECH. & INTELL. PROP. 117, 118 (2002).

48. Blanke, *supra* note 8, at 305-06.

49. *Id.* at 306.

50. *Id.*

51. *Id.*

C. From Consumers to Advertisers—How Spammers Generate Profits

Despite the fact that some spammers send out millions of e-mails per day, not all of them generate profits in the same way. While some spammers—especially those whose messages are most familiar to consumers—generate profits through sales of products or services, others profit from paid advertisements. Still others may employ illegal means to obtain profit.

Although many spammers turn a quick profit by selling products and services directly,[52] some spammers generate profits by spamming on behalf of other businesses. One such company, BulkingPro.com, sends spam messages for other businesses.[53] It also provides clients with technical support and monthly improvements designed to "penetrate tough domain filters and spam blocking techniques."[54] One bundle offered by the company features spamming to 50 million e-mail addresses for a mere $299.[55] Such low costs undoubtedly appeal to businesses attempting to reach consumers quickly and cheaply.

Other spammers who rely on advertisers for funding engage in even more disruptive tactics. Some spam messages invite recipients to click on website links provided in the e-mail.[56] When a recipient clicks on the link, various browser windows pop up simultaneously.[57] The perpetrator's website then disables the victim's "back" and "window close" buttons while

---

52. *See, e.g.*, AL COOLEY, ASTARO INTERNET SECURITY, THE COCKTAIL APPROACH TO SPAM PROTECTION 3 (2004) (citing that spammers on average yield only around 0.005% of purchases from spamming, meaning that out of 1 million messages sent, only about fifty will result in purchases; however, because the costs of emailing millions of recipients can be as low as $300, the potential for profits is high), *available at* http://www.astaro.com/content/download/164/747/file/The_Cocktail_Approach_To_Spam_Protection_en.pdf; Stephen Baker, *The Taming of the Internet*, BUS. WK., Dec. 15, 2003, at 78 (reporting that 7% of U.S. Web surfers have purchased a product or service from an unsolicited spam message).

53. *E-mail Spam: How to Stop It from Stalking You*, CONSUMER REPORTS.ORG, *at* http://www.consumerreports.org/main/detailv2.jsp?CONTENT%3C%3Ecnt_id=322715&FOLDER%3C%3Efolder_id=162693 (last visited Mar. 12, 2005); *see* Bob Sullivan, *Who Profits From Spam? Surprise*, MSNBC NEWS, Aug. 8, 2003, *at* http://msnbc.msn.com/id/3078642.

54. *Id.* (quoting BulkingPro.com sales pitch).

55. *Id.*

56. John Harms & Michael Howden, *The Internet's Dark Side*, *at* http://www.troblewith.com/stellent/groups/public/%5C@fotf_troubledwith/documents/articles/twi_013927.cfm?channel=Parenting%20Teens&topic=Internet%20Concerns&sssct=Background%20Info (last visited Mar. 2, 2005).

57. *Id.*

more windows advertising related goods or services appear on-screen.[58] This technique is known as "mousetrapping."[59] These spammers lure spam recipients to mousetrapping websites, and are funded by advertisers who display banners on those websites.[60] Typically, these advertisers employ contract spammers who are paid based on the number of victims who actually click on the advertisements.[61] Such disruptive spam messages can ultimately lead to consumer confusion as users expend time and energy in escaping the mousetrap.

While such methods of funding spammers perpetuate annoyances for many spam recipients, other spammers resort to illegal means to fund themselves, most notably through identity theft. Some spammers send messages disguising themselves as system administrators, requesting recipients to change their passwords to a specified one, and threatening suspension of the recipients' accounts for failure to do so.[62] Variations on this type of message also include spammers posing as a person in authority, requesting recipients to send copies of passwords or other sensitive personal or financial information.[63] Once spammers obtain this information, they can place charges on credit cards, ruin credit ratings, and cause other financial injuries to unsuspecting victims.[64] The losses incurred by victims go beyond just simple annoyance in receiving spam messages, and could include very damaging financial injuries.

Spammers employ a variety of techniques to generate profits ranging from those which are mere annoyances to those that are illegal. However, regardless of the funding method, all of these techniques result in the congestion of e-mail systems and inboxes.

---

58. *Id.*; *see also*, Golden Gate Univ., *Spam and Scams*, *at* http://internet.ggu.edu/university_library/spam_scam.html#trap (last updated Nov. 3, 2003).

59. Golden Gate Univ., *supra* note 58.

60. *Id.*

61. Ed Falk, *Spam Glossary*, *at* http://www.rahul.net/falk/glossary.html#mousetrap (last visited Mar. 2, 2005).

62. Stephanie Austria, *Forgery in Cyberspace: The Spoof Could be on You!*, 5 PGH J. TECH. L. & POL'Y 2, para. 9 (2004).

63. *Id.*

64. *See generally*, Jennifer Lynch, Note, *Identity Theft in Cyberspace: Crime Control Methods and Their Effectiveness in Combating Phishing Attacks*, 20 BERKELEY TECH. L.J. 259 (2005) (providing an in-depth discussion of "phishing" and obtaining sensitive information); *Phishing: Identity-theft Spam*, CONSUMER REPORTS.ORG, Sept. 2004 (providing a general discussion of phishing and tips to combat it), *at* http://www.consumerreports.org/main/detailv4.jsp?CONTENT%3C%3Ecnt_id=464561&FOLDER%3C%3Efolder_id=162693&ASSORTMENT%3C%3East_id=333133.

D. Who Spams?

It is believed that most spam originate from a small group of hard-core spammers.[65] These hard-core spammers might number as few as two hundred.[66] Some of these spammers profit by sending out millions of messages per day.[67] One such spammer, Jeremy Jaynes, sent out at least 10 million e-mails per day through sixteen high-speed lines.[68] Although Jaynes averaged one sale out of every 30,000 e-mails he sent, he nevertheless made up to $750,000 per month with overhead expenses of only $50,000.[69] Not only are such spammers irritating because they send millions of messages per day, but they are also dangerous because much of their spam contains fraudulent information and pitches bogus goods and services.[70] One idea peddled by Jaynes was a scheme to earn $75 by working at home as a Federal Express refund processor, an idea that Jaynes charged spam recipients $39.95 to learn.[71] This fraudulent scheme resulted in over 10,000 credit card orders in one month alone.[72] Big time spammers like Jaynes are the pernicious spammers whom legislation and policing should focus on first because of the propensity of these spammers to rely on fraudulent schemes to make a profit.

Aside from individuals, some businesses are also pernicious spammers. As briefly noted above, BulkingPro.com sends millions of spam messages each day for other businesses.[73] Many of these companies claim that their e-mail lists are directed toward certain target demographic groups and are updated regularly to ensure that all e-mail addresses are functioning.[74] Although these claimed practices appeal to potential adver-

---

65. Ron Wyden & Conrad Burns, *Why We've Finally Canned Spam*, CNET NEWS.COM, Dec. 16, 2003, *at* http://news.com.com/Why+we've+finally+canned+spam/2010-1028_3-5125699.html.

66. *Id.*

67. *Id.*

68. Associated Press, *Prolific Spammer's Strategies Come to Light in Trial*, TAIPEI TIMES, Nov. 17, 2004, at 12.

69. *Id.*

70. *See World's Top 10 Spammers*, MSNBC, *at* http://www.msnbc.com/news/wld/tech/brill/Top10Spammers_dw.htm (last visited Mar. 2, 2005); *supra* Part I.B.

71. *See* Charles Arthur, *E-mail Spammers Face Nine Years in Jail*, BELFAST TEL., Nov. 5, 2004 (discussing the punishment of Jeremy Jaynes and his sister Jessica DeGroot for their involvement in spamming fraudulent schemes to millions of e-mail recipients).

72. *Id.*

73. *E-mail Spam: How to Stop It from Stalking You*, *supra* note 53; *see* Sullivan, *supra* note 53.

74. *See, e.g.*, Ad-Site.com, *at* http://www.ad-site.com/eMailLists.php (last visited Mar. 2, 2005); InetGiant, *at* http://www.inetgiant.com/email_blaster.html?source=goog

tisers, companies such as BulkingPro.com also rely on deceptive practices. BulkingPro.com's website and literature offer updated lists of proxy servers,[75] information on inserting random characters into e-mail to pass spam filters, and "other new tricks to get past aggressive domain filters."[76] Not only are these businesses contributing to the mass volume of spam sent to consumers and other businesses, but they also are employing questionable tactics while doing so.

In addition to the hardcore spammers, there are small-time spammers, who range from teenagers in basements to legitimate businesses.[77] Some small-time spammers are legitimate businesses trying to develop their clientele through the use of e-mail as a form of marketing.[78] Most of these businesses are small businesses seeking cost-effective strategies to increase readership and familiarity with their products.[79] Even well-established businesses, such as MasterCard, send out bulk e-mail advertising their services.[80] Also on the rise is political spam sent for political purposes such as spreading a certain candidate's platform or soliciting votes.[81] For these entities, spamming is a cost-effective way to generate profits, increase the company's consumer base, and to acquaint potential voters with a certain political party or candidate.

II. EARLY SPAM REGULATION

In combating spam, recipients have utilized a variety of tools, some more effective than others. The simplest methods included self-regulation and self-help. Recipients also resorted to common law suits to regulate spammers. Because these methods were generally inadequate, the need for

---

&keyword=email+list (last visited Mar. 2, 2005); MyOpt, *at* http://www.myopt.com/?source=google (last visited Mar. 2, 2005).

75. *See E-mail Spam: How to Stop It from Stalking You*, *supra* note 53 (describing proxy servers as computers that spammers can use to transmit e-mail anonymously).

76. *Id.*

77. Saul Hansell, *Finding Solution to Secret World of Spam*, N.Y. TIMES, May 5, 2003, at C8.

78. Rachel Henwood, *Spam—A Global Epidemic*, AD.WRIGHT!, Sept. 2, 2004, *at* http://www.adwright.com/portal/comm/control.cfm?ID=716.

79. Linda Formichelli, *When Spam Burns You: Why Unsolicited Bulk E-Mail Is Bad News*, *at* http://www.twowriters.net/spam.htm (last visited Mar. 2, 2005).

80. *Id.*

81. *See generally*, Seth Grossman, *Keeping Unwanted Donkeys and Elephants Out of Your Inboxes: The Case for Regulating Political Spam*, 19 BERKELEY TECH. L.J. 1533 (2004) (discussing the nature of political spam and its exemption from federal spam legislation, and suggesting model legislation to curb political spam).

more effective approaches spurred the growth of state legislation. This Part provides a brief account of these approaches to combating spam.

A. Self-Regulation and Self-Help: Vigilantism on the Internet

When spamming first began, recipients resorted to self-regulation and self-help to inhibit spammers from operating.[82] Recipients would "mail-bomb" the sender by sending a massive volume of e-mail to retaliate against the sender, resulting in a complete overload of the sender's mail-box.[83] This prevented any prospective client from contacting senders for their advertised products.[84] Others recipients issued direct complaints to ISPs while some created their own software to filter and automatically delete spam messages.[85] Still others established anti-spam groups with hopes of stigmatizing spammers into retirement.[86] Groups such as the Mail Abuse Prevention System provided both legal and technical advice on blocking spam.[87] These groups also established blacklists of servers that were friendly or indifferent to spam and provided these lists to ISPs so that they could block mail sent from those servers on the blacklist.[88]

The effectiveness of each of these methods, if any, was short-lived. Numerous problems with these methods quickly emerged, indicating the long-term ineffectiveness of such approaches. Mailbombing soon proved to be ineffective as spammers quickly learned to forge false return addresses in their e-mail headers.[89] As a result, mailbombs clogged the inboxes of innocent users and even collapsed smaller ISP servers.[90] The creation of blacklists also created problems. For example, a political rival or a commercial competitor could easily and anonymously place a particular individual or company on the list of spammers, thereby removing that person's ability to communicate via e-mail.[91] Thus, the ineffectiveness of self-regulation encouraged the development of various legal approaches to combating spam.

---

82. *See* Magee, *supra* note 12, at 337.
83. *Id.* For definition of "mailbomb," see *MailBomb Definition*, MONSTER ISP, *at* http://www.monster-isp.com/glossary/mailbomb.html (last visited Mar. 2, 2005).
84. *See* Magee, *supra* note 12, at 337.
85. *Id.*
86. *Id.* at 342.
87. *Id.* at 337.
88. *Id.*
89. *Id.* at 341.
90. *Id.*
91. *Id.* at 342.

B. Common Law Theories

Spam recipients next turned to common law theories to bring spammers to justice. Breach of contract,[92] trademark dilution,[93] and false designation of origin[94] were some of the common law theories alleged against spammers. One of the more successful theories is the doctrine of trespass to chattels.[95] A plaintiff advancing this theory must have incurred "actual injury" as a result of the spammer's intermeddling in order for the claim to

---

92. *See generally* Hotmail Corp. v. Van Money Pie Inc., No. C98-20064 JW, 1998 U.S. Dist. LEXIS 10729, at *1 (N.D. Cal. Apr. 16, 1998) (finding that defendants breached the Hotmail user agreement to refrain from spamming when they created a number of Hotmail accounts with the specific purpose of sending spam to thousands of Internet e-mail users advertising pornography, bulk e-mailing software, and get-rich-quick schemes).

93. *See* Am. Online, Inc. v. IMS, 24 F. Supp. 2d 548, 552 (E.D. Va. 1998). In *America Online, Inc. v. IMS*, the court found that plaintiffs successfully advanced a trademark dilution claim under 15 U.S.C. § 1125(c) of the Lanham Act when defendant spammers used the letters "aol.com" in their headers. Under this theory, an owner of a mark is entitled to relief against another person's commercial use of the mark "'if such use begins after the mark has become famous and causes dilution of the distinctive quality of the mark.'" *Id.* (quoting 15 U.S.C. § 1125(c)). To set forth a claim for dilution, plaintiff must show: (1) the ownership of a distinctive mark; and (2) a likelihood of dilution. *Id.*

94. *See id.* at 548-51 (finding that plaintiffs successfully advanced a false designation of origin claim under 15 U.S.C. § 1125(a)(1) of the Lanham Act because many of defendant spammer's e-mail contained the letters "aol.com" in their headers). The court in *IMS* stated that a false designation of origin contains three elements: "(1) the alleged violator must employ a false designation; (2) the false designation must deceive as to origin, ownership, or sponsorship; and (3) the plaintiff must believe that 'he or she is or is likely to be damaged by such [an] act.'" *Id.* at 551 (citing 15 U.S.C. § 1125(a)(1)). Not only does this claim provide protection of trademarks in order to secure to the owner of the mark the goodwill of his business, but it is also intended to protect consumers and their ability to differentiate among competing products. *Id.* In this case, the court held that any of plaintiff's subscribers could logically conclude that the message containing "aol.com" originated from plaintiff and cause subscribers to believe that plaintiff sponsored or approved of defendant's spam messages. *Id.* at 551-52.

95. *See, e.g.*, Compuserve, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015 (S.D. Ohio 1997); Thrifty-Tel, Inc. v. Bezenek, 54 Cal. Rptr. 2d 468 (Ct. App. 1996); Ashley L. Rogers, *Internet & Technology: Is There Judicial Recourse to Attack Spammers?*, 6 VAND. J. ENT. L. & PRAC. 338, 340 (2003) (discussing that a trespass of chattels in the spam context occurs when spamming "intermeddles" or interferes with the possessory interest of another through unauthorized use of their computer network and that a plaintiff advancing this theory must also "demonstrate an object on which a person could trespass and a mechanism for that trespass to take place" and actual injury); Steven Kam, Note, Intel Corp. v. Hamidi: *Trespass to Chattels and a Doctrine of Cyber-Nuisance*, 19 BERKELEY TECH. L.J. 427 (2004) (analyzing the use of trespass to chattels when protecting e-mail systems).

be actionable.[96] This element has proved to be problematic as various courts have produced different standards as to what constitutes actual injury. While a California court held that a mere formula or a statistical average of the damages is insufficient,[97] an Ohio court held that the tremendous burden imposed upon plaintiffs was sufficient proof of actual injuries.[98] These inconsistent rulings are problematic because they impose starkly different burdens on plaintiffs who may have similar trespass to chattels actions against spammers.

Additionally, plaintiffs may run into other problems when filing common law actions. Spammers often operate outside the United States or disguise their identities, making it difficult to locate them or bring them into court.[99] Another difficulty in filing lawsuits is that only those with sufficient resources and incentives will be able to endure what may be a lengthy trial. As a result, many individual spam recipients will have neither the desire nor the ability to maintain lawsuits against spammers.

C. State Law Regulation

In 1997, Nevada was the first state to pass a statute regulating unsolicited commercial e-mail.[100] Other states such as California, Washington, and Virginia quickly followed.[101] These states became models for others, and there are currently thirty-six states that have a statute aimed at combating spam.[102]

Most of these statutes primarily target fraudulent or misleading spam.[103] These statutes prohibit falsifying the point of origin and transmis-

---

96. Intel Corp. v. Hamidi, 71 P.3d 296, 302-04 (Cal. 2003).

97. *Thrifty-Tel*, 54 Cal. Rptr. 2d at 475.

98. *Compuserve*, 962 F. Supp. at 1023.

99. *See* Brian Morrisey, *AOL Files Spam Suits*, CLICKZ NEWS, Apr. 15, 2003 (indicating that America Online has filed various lawsuits against spammers with some cases referring to defendants as "John Does" or "unnamed" because of difficulties in ascertaining the spammers' identities), *at* http://www.clickz.com/news/article.php/2190881.

100. *See* NEV. REV. STAT. ANN. §§ 41.330, 41.705-41.735 (Michie 2002 & Supp. 2003); *see also* Magee, *supra* note 12, at 356.

101. *See* CAL. BUS. & PROF. CODE § 17529 (West Supp. 2005); WASH. REV. CODE ANN. §§ 19.190.10 to -.070 (West 1999 & Supp. 2005); VA. CODE ANN. § 18.2-152.3:1 (Michie 2004); *see also* Magee, *supra* note 12, at 356.

102. *See, e.g.*, COLO. REV. STAT. ANN. § 6-2.5-103 (West 2002); IOWA CODE ANN. § 714E.1 (West 2003); TENN. CODE ANN. § 47-18-2501 (2001 & Supp. 2004); Magee, *supra* note 12, at 356. *See generally* David E. Sorkin, *Spam Laws*, http://www.spamlaws.com (showing various state spam laws currently in place) (last revised Dec. 16, 2003).

103. Magee, *supra* note 12, at 356.

sion path of unsolicited commercial e-mail.[104] In addition, such legislation typically prohibits misleading information in the subject line of the message.[105] Most states also require subject lines to begin with "ADV:" for all commercial e-mail solicitations, and "ADV: ADLT" for adult-content e-mail.[106] These statutes focus on the regulation of spam content rather than reshifting spam's costs back onto the senders or decreasing the amount of spam sent.

These state statutes also provide for varying penalties and generally allow individuals to bring a private cause of action against spammers.[107] In some states, spammers who send fraudulent or misleading spam or utilize fraudulent methods in doing so face a combination of both civil and criminal penalties.[108] In other states, the degree of damage also determines the classification of the crime as either a misdemeanor or felony.[109]

Most states also rely on opt-out requirements to discourage spamming rather than an opt-in requirement. Under an opt-in system, spammers can only send e-mail to recipients who have explicitly consented to receiving the e-mail.[110] The opt-in requirement would place the burden on spammers to ask for consent prior to communications with the recipient; most state statutes do not prescribe an opt-in requirement.[111] Instead, most state statutes maintain a more business-friendly opt-out approach. Under this approach, spammers can contact recipients and need only maintain a valid link or e-mail address for recipients to unsubscribe themselves from the

---

104. *Id.*

105. *Id.*

106. *Id.*

107. *See, e.g.*, CAL. PENAL CODE § 502(e)(1) (West 1999 & Supp. 2005); ME. REV. STAT. ANN. tit. 10, § 1497(7) (West Supp. 2004); N.C. GEN. STAT. § 14-458(c) (2003).

108. *See, e.g.*, CAL. PENAL CODE § 502(d)(1) (West 1999) (punishable by a fine not exceeding $10,000, or by imprisonment in state prison for 16 months, or two or three years, or by both that fine and imprisonment); MICH. COMP. LAWS. ANN. § 445.2507(7)(1) (West Supp. 2004) (punishable by imprisonment for not more than 1 year or a fine of not more than $10,000, or both).

109. *See, e.g.*, N.C. GEN. STAT. § 14-458(b) (2003). In North Carolina, any person falsely identifying with the intent to deceive or defraud recipient or forget commercial electronic mail transmission information or routing information in connection with transmission of unsolicited bulk commercial electronic mail is guilty of a Class 3 misdemeanor. *Id.* If there is damage to property of another valued at less than $2,500, offense will be classified as a Class 1 misdemeanor. If the damage is greater than $2,500, then offense punishable as a Class I felony. *Id.*

110. Blanke, *supra* note 8, at 308.

111. *See* CAL. BUS. & PROF. CODE §§ 17529 to .9, 17538.45 (West Supp. 2005); *see also* Blanke, *supra* note 8, at 308 (stating that California recently became the first state to approve an opt-in approach).

mailing list.[112] Although the volume of spam would be lessened significantly more through the use of an opt-in system, most states have chosen to rely on the less restrictive opt-out requirement.

While state statutes share a common goal of regulating spam, their differing approaches points to a key weakness in a state-centered approach to regulating spam.[113] Although some states like California require that spam messages contain a statement informing recipients of the spammer's contact information, other states like Iowa are much less strict and require only that messages provide an e-mail address that is "identifiable" which recipients can contact.[114] As a result, a spammer under Iowa law places a heavier burden on the recipient to read through the text to locate the contact information. In addition, although most states require the placement of "ADV" in the subject line of a commercial e-mail, some states require only that subject lines do not contain "false or misleading information."[115] The latter approach makes separating spam messages from legitimate ones more time consuming. Thus, the burdens imposed on both spammers and recipients vary considerably among state statutory schemes.

A more significant problem with state legislation is that the majority of spam is transmitted across state lines.[116] For example, in the majority of circumstances, even if both the sender and recipient are located within the same state, the spam will most likely be routed through a server located in another state.[117] This may result in confusion as to which state law should apply and how far each state's protection can and should extend.[118] Such weaknesses signaled the need for a more cohesive, federal approach.

III. FEDERAL LEGISLATION: CAN-SPAM ACT AS THE MOST PROMISING ANSWER?

A. Overview of the CAN-SPAM Act

The ineffectiveness of vigilantism and common law theories and a lack of uniformity among state spam legislation gave rise to a more centralized,

---

112. *See, e.g.*, N.D. CENT. CODE §§ 51-27-01 to -09 (2003); 73 PA. CONS. STAT. ANN. §§ 2250.1 to .8 (West Supp. 2004); Blanke, *supra* note 8, at 308 (noting that twenty-four states have an opt-out requirement).

113. *See* Graydon, *supra* note 19, at 98.

114. *Id.* at 99.

115. *Id.* at 100-01.

116. *See* David E. Sorkin, *Spam Legislation in the United States*, 22 J. MARSHALL J. COMPUTER & INFO. L. 3, 7 (2003).

117. *Id.*

118. *Id.*

focused, federal approach: the CAN-SPAM Act. The Senate passed the first version of the Act on October 23, 2003. Following two modifications to the bill by the Senate and the House, President George W. Bush signed the Act into law on December 16, 2003.[119]

Although the Act targets spam, it is solely applicable to spam messages which are commercial in nature.[120] "Commercial electronic mail message" under the Act includes "any electronic mail message the primary purpose of which is commercial advertising or promotion of a commercial product or service"[121] and excludes "transactional or relationship message[s]."[122] Thus, the Act is not applicable to messages associated with an ongoing, existing business relationship or to those messages that the recipient has specifically requested from the spammer.[123]

The provisions of the Act parallel many of those found in state statutes aimed at reducing spam, especially fraudulent spam. However, the Act does not provide for a private right of action.[124] Rather, only the U.S. Department of Justice, the FTC, state attorneys general, and ISPs have the ability to institute actions.[125] Violators of the Act face potential fines up to $2 million and possibly treble damages if the spammer "committed the violation willfully and knowingly."[126] Some provisions in the statute include:

- The prohibition of misleading or false information and subject headings in e-mail messages. It is unlawful for any person to initiate the transmission, to a protected computer, of a commercial e-mail message that is materially false or materially misleading.[127]
- Unsolicited commercial e-mail must be clearly identified as advertisements for products or services. Furthermore, sexually oriented messages require warning labels.[128]
- The senders' e-mail must contain a functioning return e-mail address or other Internet-based mechanism, clearly and conspicuously displayed so that recipients may reply to the e-mail and re-

119. Trussell, *supra* note 11, at 181.
120. Sorkin, *supra* note 116, at 10.
121. 15 U.S.C.A. § 7702 (Supp. 2004).
122. *Id.*; *see* Sorkin, *supra* note 116, at 110.
123. Blanke, *supra* note 8, at 307.
124. Trussell, *supra* note 11, at 183.
125. *Id.*
126. 15 U.S.C.A. § 7706(f)(3)(B)-(C).
127. *Id.* § 7704(a)(1)-(2).
128. *Id.* § 7704(d).

quest not to receive future commercial e-mail messages from that sender at the e-mail address where the message was received.[129]

- Spammers are prohibited from utilizing automated means to establish multiple e-mail accounts solely to send out spam and from engaging in automated means that generate e-mail addresses (bulk solicitation).[130] Examples of such techniques include address harvesting[131] and dictionary attacks.[132]

- The creation of a plan and a timetable by the FTC for a Do-Not-E-mail list, similar in scope to the Do-Not-Call list within six months of the Act's enactment. The FTC is required to establish and implement the plan within nine months after the passage of the Act. If the FTC is unable to establish and implement the plan, then it must explain to Congress why it cannot do so.[133]

- Criminal penalties against spammers who send predatory and abusive commercial e-mail, including those who send obscene messages, child pornography, or messages used to perpetrate identity theft, if such offenses involve the sending of large quantities of e-mail.[134]

B. Criticism of CAN-SPAM

Soon after the passage of the Act, criticism erupted over what had appeared to be a promising federal effort to combat the ever-increasing problems associated with spam. Some opponents see the Act as merely symbolic—an Act with no teeth because it merely provides a set of guidelines on how to spam legally rather than addressing the disruptive, cost-shifting

129. *Id.* § 7704(a)(3).

130. *Id.* § 7704(b).

131. *Id.* § 7704(b)(1)(A)(i) (defining "address harvesting" as usage of e-mail addresses obtained via an automated means from an Internet website or proprietary online service operated by another person, and such website or online service included, at the time the address was obtained, a notice stating that the operator of such website or online service will not give, sell, or otherwise transfer addresses maintained by it to another party for purposes of initiating, or enabling others to initiate e-mail messages).

132. *Id.* § 7704(b)(1)(A)(ii) (defining "dictionary attacks" as the usage of e-mail addresses of recipients obtained using an automated means that generates possible e-mail addresses by combining names, letters, or numbers into numerous permutations).

133. *See id.* § 7708; *see also* Trusell, *supra* note 11, at 181-83.

134. 15 U.S.C.A. § 7703.

structure of spam.[135] These critics raise myriad concerns, emphasizing that the Act neutralizes stricter state statutes because of its preemptive effect and the impossibility of creating a sustainable Do-Not-E-Mail list. Other critics believe that the harsh penalties imposed by the Act are disproportionate to the crime. Still others are concerned with the Act's impact on the First Amendment right of spammers to engage in commercial speech and question the constitutional validity of the Act. Nevertheless, the Act is not without its proponents, who believe that some of the criticized aspects of the Act only contribute to its efficiency and potential for success in combating spam.

1. Preemption of State Statutes That May Provide More Protection

One of the primary criticisms against the Act is that it preempts stricter state laws.[136] For example, California's law contained an opt-in provision, a stricter standard than the Act's opt-out standard.[137] As previously described, spammers under the opt-in approach would be prohibited from sending e-mail to recipients who do not have a preexisting business relationship with the sender or to people who have not provided their express consent to receive their messages.[138] This approach is more beneficial to recipients since an opt-out system is triggered only after the message has been sent and after the damage has been done. In addition, critics are wary of opt-out links in e-mail because recipients, by clicking on the link, are validating their e-mail addresses.[139] Consequently, spammers become aware of valid e-mail addresses, which may result in an even greater flood of spam for those e-mail accounts.[140] In addition, California's law would have provided recipients with the right to file private, individual lawsuits, a right absent from the federal Act.[141] Such criticism casts doubt on whether the federal law actually affords better protection than existing state laws.

---

135. *See, e.g.*, Thomas K. Ledbetter, Comment, *Stopping Unsolicited Commercial E-Mail: Why the CAN-SPAM Act Is Not the Solution to Stop Spam*, 34 SW. U. L. REV. 107, 112-14 (2004).

136. *See* 15 U.S.C.A. § 7707(b); *see, e.g.*, Elizabeth A. Alongi, Comment, *Has the U.S. Canned Spam?*, 46 ARIZ. L. REV. 263, 287 (2004).

137. Alongi, *supra* note 136, at 287-88.

138. *Id.*; *supra* Part II.C.

139. Alongi, *supra* note 136, at 288.

140. *Id.*

141. *See* CAL. PENAL CODE § 502(e)(1) (West 1999 & Supp. 2005); *see also* Sharon D. Nelson & John W. Simke, *Hi-Tech in the Law Office: The Basics of Spam & Strategies for Defense*, ALASKA B. RAG, Winter 2004, at 26.

Many proponents of the Act believe that the adoption of a uniform federal law is more favorable than having a wide variety of state spam laws.[142] Undoubtedly many of these proponents are businesses who find it difficult to comply with disparate state laws.[143] For marketers, having a uniform federal law might make their operations more cost efficient as they would only have to comply with one set of standards and requirements when distributing e-mail messages.[144] In assessing the advantages of the Act, it is important to recognize that some of its most vocal supporters are those spammers who will directly benefit from the legislation.

2. Criminal Penalties

Criticism has also been directed towards the possible penalties imposed under the Act. Under the Act, excessive spamming is punishable as a felony, thereby making it a criminal act.[145] Some criminal defense lawyers and civil libertarians believe that the penalty is too harsh and does not fit the crime.[146] They believe that spamming does not constitute misconduct that harms people—conduct that is ordinarily criminal.[147] These critics point out that spam does not even harm trees.[148]

Proponents of the Act believe the severe penalties will deter excessive spamming.[149] They emphasize that there exists only a relatively small number of hard-core spammers who are sending out millions of e-mails daily.[150] They believe that these spammers will discontinue or at least decrease the amount of e-mails they send because they are reluctant to risk criminal prosecution under the Act.[151] In addition, proponents of the Act assert that the severity of punishment under the Act is similar to those penalties already imposed under existing state statutes that provide for felony classifications of fraudulent or misleading spam.[152] Although the penalties incurred under the Act may be harsh, perhaps they are necessary as spam becomes an increasingly unwelcome part of our daily lives.

---

142. Trussell, *supra* note 11, at 184.

143. *Id.*

144. *Id.*

145. Paul Festa, *Stiff Spam Penalties Urged*, CNET NEWS.COM, Apr. 14, 2004, *at* http://news.com.com/2100-1028-5191651.html.

146. *Id.*

147. *Id.*

148. *Id.*

149. Wyden & Burns, *supra* note 65.

150. *Id.*

151. *Id.*

152. *See, e.g.*, N.C. GEN. STAT. § 14-458(b) (2003) (criminalizing spammers who engage in deceitful practices with misdemeanor or felony classifications).

3. *Constitutional Concerns*

A major concern raised by critics is that the Act may challenge fundamental free speech rights under the First Amendment.[153] The Act allows the government to regulate commercial speech since enforcement resides with the government.[154] Accordingly, the government must: 1) show a substantial interest in the regulation, 2) prove that the imposed restrictions will advance its interests, and 3) prove that the regulation is narrowly tailored so that it does not regulate more speech than necessary.[155] These are valid concerns, going to the heart of the debate between allowing the free dissemination of information and speech versus the elimination of spam.

Advocates of the CAN-SPAM Act insist that it will pass judicial scrutiny on the First Amendment issue. Ultimately, the government has a valid and strong interest in preventing consumer fraud, invasion of consumer privacy, and realigning costs to the sender—concerns that the Act attempts to address.[156] Requiring spammers to provide and honor opt-out links is an approach to preventing the invasion of consumer privacy and shifting costs back onto the sender.[157] Furthermore, since some studies indicate that two-thirds of spam contains some type of fraud, the Act's requirement of truthful information in subject lines and return addresses will advance the government's interest in fraud prevention.[158] Although the Act will probably be challenged on First Amendment issues, it seems likely that it will be upheld as the government has a substantial interest in spam regulation. Additionally, the Supreme Court has held that the Constitution provides less protection for commercial speech than for other forms of communication.[159] As such, the Act is likely to pass judicial scrutiny under the First Amendment.

4. *Do-Not-E-mail List*

Although the Act proposes a Do-Not-E-mail list, similar to the Do-Not-Call list for telemarketers, the fact that spam is transmitted through the Internet renders this enforcement mechanism less effective. The FTC implemented the Do-Not-Call list as a response to the growing problems

153. Mainstream Mktg. Servs. v. FTC, 358 F.3d 1228, 1236-37 (10th Cir. 2003) (citing Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n, 447 U.S. 557, 564 (1980)).

154. *Id.*

155. *Id.*

156. *Id.*

157. *Id.*

158. Alongi, *supra* note 136, at 287.

159. Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n, 447 U.S. 557, 562-63 (1980).

associated with telemarketers. Although the list has been challenged by telemarketers as a violation of their First Amendment rights, the Tenth Circuit upheld the constitutionality of the list, a decision that the Supreme Court refused to reconsider.[160] The CAN-SPAM Act proposes a similar scheme, a scheme struck down by the FTC as ineffective.[161]

Since Internet identities are difficult to track, a Do-Not-E-mail list would likely be of little practical value. In the telemarketing world, the list is more effective since centralized telephone lines allow authorities to trace phone calls to the violating telemarketer.[162] In contrast, e-mail systems run across borders and are far more decentralized, making spam more difficult to trace.[163] In addition, spammers regularly use stolen computers and e-mail accounts to spam, making enforcement of such a list difficult.[164] Not only is enforcement of such a list extremely difficult in the context of spam, but it also could lead to even more pernicious spamming. The list could fall into the wrong hands—a spammer's hands—thereby enabling the wrongdoer with a very powerful list of *valid* e-mail addresses to spam.[165] Although the Act sets out to protect consumers through the creation of a Do-Not-E-mail list, the medium in which spam operates limits the potential utility of such a list.

5. *Insufficiency of Litigation Under the CAN-SPAM Act*

Although many cases brought under the Act are still pending, it appears that at least in the early stages of prosecution, courts are reluctant to dismiss charges against spammers. The FTC has hauled spammers into court alleging that their e-mail contained false and misleading information.[166] While these cases are being litigated, courts have enjoined these spammers from sending further e-mail until a verdict is reached.[167] The courts imposed these injunctions reasoning that there was good cause to

160. Mainstream Mktg. Servs. v. FTC, 358 F.3d 1228, 1232-33 (10th Cir. 2003), *cert. denied*, 125 S. Ct. 47 (2004).

161. *See* 15 U.S.C.A. § 7708 (Supp. 2004); Bob Sullivan, *Do-Not-Spam List Won't Work, FTC Says*, MSNBC NEWS, June 15, 2004, *at* www.msnbc.com/id/5216554.

162. Sullivan, *supra* note 161.

163. Marc Simon, *The CAN-SPAM Act of 2003: Is Congressional Regulation of Unsolicited Commercial E-Mail Constitutional?*, 4 J. HIGH TECH. L. 85, 106 (2004).

164. Sullivan, *supra* note 161.

165. *Id.*

166. *See, e.g.*, FTC v. Bryant, No. 3:04-cv-897-J-32MMH, 2004 U.S. Dist. LEXIS 23315 (M.D. Fla. Oct. 4, 2004); FTC v. Harry, No. 04C 4790, 2004 U.S. Dist. LEXIS 15588 (N.D. Ill. July 27, 2004).

167. *Bryant*, 2004 U.S. Dist. LEXIS 23315, at *10-*11; *Harry*, 2004 U.S. Dist. LEXIS 15588, at *8-*9.

believe that the spammers had violated the Act.[168] These decisions are promising and may lead to a decreased volume of false and misleading e-mail. However, they do very little to address the central complaint of spam recipients: receiving any quantity of spam at all, regardless of whether they were false or misleading.

Other suits brought against spammers have settled out of court, leading to the question of whether such settlements will sufficiently deter spammers. In the first suit filed by any state under the Act, a Florida spammer paid $25,000 to settle a lawsuit alleging violations of the Act.[169] State officials alleged that the spammer violated the Act by using fake return addresses to conceal the e-mails' origin, that the messages failed to provide recipients an easy way to opt-out of the mailings, and did not clearly identify itself as an advertisement.[170] Upon a cursory review, it may seem that the Act is performing its function of ensuring that only legitimate spam is sent. However, some spammers will probably continue to send misleading or false messages and risk being caught if they can generate significant profits. Additionally, even if spammers are caught, they might be able to settle out of court for what they may consider to be an insignificant penalty, and risk further criminal prosecution under the Act. These possibilities point to further shortcomings of the Act.

The Act has also been used offensively by spammers. In *White Buffalo Ventures, LLC v. University of Texas*, the defendant spammer unsuccessfully argued that the Act preempted private mechanisms of enforcement.[171] In that case, a spammer sent approximately 55,000 spam messages promoting LonghornSingles.com to members of the University of Texas with e-mail addresses ending in "utexas.edu."[172] Messages ending in utexas.edu are accumulated on computer servers owned and operated by the plaintiff University.[173] When the University received notice of the spam, it asked the defendant to discontinue sending spam pursuant to the University's general anti-solicitation policy.[174] The spammer did not com-

168. *Bryant*, 2004 U.S. Dist. LEXIS 23315, at *10-*11; *Harry*, 2004 U.S. Dist. LEXIS 15588, at *8-*9.

169. Hiawatha Bray, *Spammer to Pay $25,000 Settlement*, BOSTON GLOBE, Oct. 8, 2004, at D3.

170. *Id.*

171. White Buffalo Ventures, LLC v. Univ. of Texas, No. A-03-CA-296-SS, 2004 U.S. Dist. LEXIS 19152, at *5-*15 (W.D. Tex. Mar. 22, 2004).

172. *Id.* at *2.

173. *Id.*

174. *Id.* at *3-*4.

ply and brought suit claiming, in part, that the Act preempts any private regulation of spam.[175]

The court decided in the University's favor, holding that while the Act has preemptive effects, such preemption does not extend to private mechanisms of enforcement.[176] The court noted that although the Act preempts any state spam law, the Act also provides that it

> should not be "construed to have any effect on the lawfulness or unlawfulness, under any other provision of law, of the adoption, implementation, or enforcement by a provider of Internet access service of a policy of declining to transmit, route, relay, handle, or store certain types of electronic mail messages."[177]

The court stated that it was unclear whether the University's anti-solicitation policy is a state regulation and so should not be preempted by the Act.[178] It further held that the University's role as an Internet access provider to campus members enabled it to implement private spam policies as authorized under the Act.[179] As suggested by this case, private mechanisms of spam regulation may survive in a court of law, and Internet access providers may be able to continue implementing their own spam regulations.

Although most of these cases focus on the transmission of false and misleading messages under the Act, e-mail users are also concerned with decreasing the amount of spam. Various surveys suggest that the problems associated with spam have not been curbed since the Act's passage. One survey indicates that after the implementation of the Act, 53% of respondents noticed no changes in the amount of spam received, 24% received even more, and only 20% received less spam.[180] Other studies demonstrate that less than 10% of all spam sent comply with the Act.[181] Even ISPs such as MSN reported no decrease in spam after the passage of the Act.[182] These statistics suggest that the Act alone will be insufficient to address the problems associated with spam.

---

175. *Id.* at *5-*6.

176. *Id.* at *8-*14.

177. *Id.* at *12.

178. *Id.* at *12-*13.

179. *Id.* at *13.

180. *See* Dave Gussow, *Users Say Law's No Help As They Drown in Spam Flood*, ST. PETERSBURG TIMES (Fla.), Mar. 18, 2004, at 1D (margin of error on this study is plus or minus 3%).

181. *Id.*

182. Jonathan Sidener, *Spam Still Exploding from Can Despite Law to Ban Junk E-Mail*, SAN DIEGO UNION-TRIBUNE, Mar. 17, 2004, at A1.

6. *Additional Concerns*

One great fear among critics is that the CAN-SPAM Act simply legitimizes, and thus, will increase the amount of spam sent, because the Act provides guidance on how to spam legally.[183] The legitimization of spam could increase the costs associated with it as recipients expend even more time and energy in sorting and deleting an ever increasing volume of unsolicited commercial e-mail.[184] Some believe that the implementation of the Act is a direct result of lobbying efforts by legitimate businesses who urged Congress to "redefine the spam problem as being about dishonesty rather than the negative effects of massive volumes of unwanted e-mail."[185] As such, the Act may provide more businesses with the right to send more e-mail so long as they conform to the Act.

Furthermore, the cloak of anonymity offered to spammers through the Internet might lessen the force of the Act. Unlike other forms of advertising such as telemarketing, spammers are difficult to track.[186] In *Federal Trade Commission v. Phoenix Avatar*, expert testimony indicated that e-mails contain an "electronic postmark" that allows it to be traced back to the computer of origin.[187] Once the originating computer has been identified, then other means can be employed to identify the actual sender.[188] However, spammers often utilize "an open proxy," a computer that, with or often without the owner's knowledge, accepts connections from anyone and forwards those e-mails as if the messages had originated from the open proxy.[189] Consequently, spam messages are difficult to track. Such devices employed by spammers make enforcement of the Act difficult. The fines imposed under the Act may never be realized if authorities are unable to locate and hold spammers responsible. Thus, the Act may not deter spammers, especially the most pernicious ones because they can easily escape capture.

Although the Act contains numerous provisions aimed at prohibiting misleading subject lines and false return e-mail addresses, it does not reshift spam's costs back onto senders. At best, the Act will simply replace misleading or fraudulent spam messages in our inboxes with more legiti-

---

183. *See* Trussell, *supra* note 11, at 187.

184. *See id.*

185. Ray Everett-Church, *It's Not Called 'Can' Spam for Nothing*, CNET NEWS.COM, Dec. 16, 2003, *at* http://news.com.com/It's+not+called+'Can'+Spam+for+nothing/2010-1028_3-5125192.html.

186. Sullivan, *supra* note 161.

187. No. 04 C 2897, 2004 U.S. Dist. LEXIS 14717, at *22 (N.D. Ill. July 29, 2004).

188. *Id.*

189. *Id.* at *23.

mate e-mail messages from perhaps more legitimate advertisers. However, this will still result in increased disk usage on recipients' systems, loss of productivity as recipients will still have to sift through their e-mail and delete those that are spam messages, and the purchase of e-mail filters which consumers will still need. The cases pending against spammers under the Act address fraudulent or misleading spam rather than the sheer quantity of spam received. Although one of the problems with spam is that it is often fraudulent or misleading, spam also poses an annoyance to a large extent because of its high-volume nature and cost-shifting structure. Considering the limitations of the various legislative solutions implemented to date, the most effective response to the spam problem might be a combination of legislative and non-legislative solutions that will address all the concerns e-mail users and ISPs have about spam.

IV. THE NEED FOR MORE PROGRESSIVE SOLUTIONS BEYOND THE CAN-SPAM ACT

Although the CAN-SPAM Act has been somewhat successful in bringing spammers to justice, it is obviously not without its shortcomings. Perhaps the court in *White Buffalo Ventures* most accurately summarized the situation by acknowledging that in implementing the Act, Congress also "recognized [its] limitations" and that spam cannot be solved through "'Federal legislation alone.'"[190] In combating the problems associated with spam, it is imperative that more progressive solutions, especially technology-based ones also be employed.

In addition to the use of filters to weed out spam, more innovative technological solutions are on the rise. Some of the most prominent proposals are those advanced by Bill Gates and Microsoft. One proposal would force e-mail senders to pay for each piece of e-mail sent.[191] Every time a piece of e-mail is sent, a small amount, such as twenty cents, is indicated in the subject line of the e-mail.[192] This amount represents the amount of money a sender is willing to pay the recipient to open and view

190. White Buffalo Ventures, LLC v. Univ. of Tex., No. A-03-CA-296-SS, 2004 U.S. Dist. LEXIS 19152, at *11 (W.D. Tex. Mar. 22, 2004) (quoting 15 U.S.C. § 7701(a)(2)).

191. Kevin Maney, *Gates, Microsoft Look For Ways to Zap Spam*, USA TODAY, June 25, 2003, at 1B, *available at* http://www.usatoday.com/money/industries/technology/2003-06-25-gates_x.htm.

192. *Id.*

the e-mail.[193] It is then up to the recipient to determine whether that amount is sufficient inducement to open the e-mail.[194]

This proposal is like traditional junk mail because it shifts costs back onto advertisers by forcing them to pay postage. Although spammers might still spam, the amount of spam they send might decrease. Additionally, it might result in more efficient business relationships because recipients can open e-mail that are of genuine interest for products that they might indeed purchase. On the other hand, this proposal might not deter spam because undoubtedly the costs imposed would still be less than those associated with traditional junk mail or telemarketing. Unlike telemarketers and junk mail advertisers who incur tremendous costs by hiring employees, operating out of various locations, buying envelopes, and paying for long-distance telephone costs, spammers will still incur much lower overhead costs even if they have to pay a small fee to transmit e-mail.[195]

Unsurprisingly, this proposal has its critics. Some state that it "detracts from [the] ability to speak and to state . . . opinions to large groups of people."[196] Today, there are more and more groups that use e-mail as their primary form of communication.[197] This proposal might unnecessarily burden, for example, dozens of parents coordinating school events or hundreds of cancer survivors sharing tips on coping with the illness.[198] However, Gates's proposal is mindful of this. Under his proposal, recipients can also choose to open e-mail without being paid.[199] This option would then allow recipients to receive e-mail as they do now from familiar senders, such as their family, friends, other parents, and support groups without incurring any charges for the sender.

However, problems might arise with respect to the administration of the proposal, including how recipients will be paid. It is unclear whether senders will issue checks (which could bounce) or whether ISPs will track monetary credits and distribute them when the credits reach a certain amount. In addition, some critics charge that this proposal is highly U.S.-centric because senders in other countries, especially developing countries,

193. *Id.*

194. *Id.*

195. Riggs, *supra* note 20; Stevenson, *supra* note 20.

196. Associated Press, *Gates: Buy Stamps to Send E-Mail*, CNN.COM, Mar. 5, 2004, *available at* http://www.cnn.com/2004/TECH/internet/03/05/spam.charge.ap.

197. *Id.*

198. *Id.*

199. Maney, *supra* note 191.

will probably be unable to afford such payments.[200] As a result, the proposal may need to issue varying monetary amounts depending from which country the e-mail originates. This lack of uniformity will inevitably cause administrative problems. In addition, advertisers could simply relocate their operations to countries that place a lower premium on sending messages. Such administrative problems suggest the need for further development of this proposal.

A similar Microsoft proposal known as the Penny Black project aims to place a non-monetary premium on every piece of unsolicited e-mail.[201] Microsoft summarizes the program as: "If I don't know you, and you want to send me mail, then you must prove to me that you have expended a certain amount of effort, just for me and just for this message."[202] Under this proposal, for every e-mail sent, the sending computer, not the spammers, will have to solve a computational algorithm.[203] This is designed to decrease the amount of spam since it will take a few seconds for the computer to solve each problem.[204] For example, a "price" of ten seconds per e-mail would limit a spamming computer to a maximum of eight thousand messages per day, a significantly smaller amount than the millions of messages sent by spamming computers currently.[205] This would not noticeably burden non-spammers since it takes a large amount of e-mail to actually cause a noticeable time delay.[206] In addition, users can maintain a "safe list," and messages from those on the list will be considered to be solicited and not subject to solving the algorithm.[207] However, it is likely that such a proposal will not hamper spammers who generally use more than just one computer to send messages. As a result, time delay in reality might not lead to a significant decrease in the number of spam sent.

One type of computational algorithm is based on a concept known as Human Interactive Proofs ("HIP"), a program designed to distinguish automated programs from actual human senders.[208] The HIP is an image

200. Associated Press, *supra* note 196.

201. Microsoft Research, *The Penny Black Project*, *at* http://research.microsoft.com/research/sv/PennyBlack (last visited Mar. 2, 2005).

202. *Id.*

203. *Id.*

204. *Id.*

205. *Id.*

206. Maney, *supra* note 191.

207. Cynthia Dwork & Andrew V. Goldberg, *Common Misconceptions About Computational Spam-Fighting*, Microsoft Research, *at* http://research.microsoft.com/research/sv/PennyBlack/spam-com.html (last visited Mar. 2, 2005).

208. Suzanne Ross, *To Err is Not Always Human*, Microsoft Research, *at* http://research.microsoft.com/displayArticle.aspx?id=413 (last visited Mar. 2, 2005).

that contains both numbers and letters,[209] and it might look like the following:

[210]

As evidenced by the figure, the numbers and letters are distorted, and some of the characters are connected by arcs ("segmentation"). While some computers can learn to engage in character recognition regardless of distortion, computers have a more difficult time recognizing segmentation.[211] This proposal would decrease the amount of spam because automated computers and programs that generate spam messages would be unable to solve, or will have to expend considerable time in solving, the algorithm.[212] This program is currently in place at Microsoft's Hotmail, an e-mail service.[213] HIPs on Hotmail are utilized in the sign-up process to ensure that those who sign up are humans, not automated programs used by spammers to obtain numerous e-mail accounts to send their e-mail.[214] Immediately after the implementation of HIP at Hotmail, sign-ups decreased by 20%, a number that could translate into a significant decrease in spam as well.[215]

Another less technological proposal aims to eliminate spam by offering cash bounties to those who locate spammers, a proposal which has received limited support.[216] This program would provide monetary rewards of $100,000 to $250,000 to savvy technology sleuths who report spammers.[217] If this program is implemented, it would mainly focus on rewarding whistle-blowers who are either inside or close to spamming operations.[218] The large monetary rewards are designed to lure whistle-blowers to risk the consequences of coming forward.[219] Critics of the proposal cite that there are already established groups who spend their time finding

209. *Id.*
210. *Id.*
211. *See id.* (explaining that "segmentation" means that the letters and numbers are not clearly separated because of the use of arcs).
212. *See id.*
213. *Id.*
214. *Id.*
215. *Id.*
216. Jonathan Krim, *Cash Bounties For Spammers Win Limited FTC Backing*, WASH. POST, Sept. 17, 2004, at E01, *available at* http://www.washingtonpost.com/ac2/wp-dyn/A27220-2004Sep16.html.
217. *Id.*
218. *Id.*
219. *Id.*

spammers and so there is less incentive to offer cash rewards.[220] Furthermore, critics believe that such a program is inherently flawed because it burdens the FTC and transfers resources away from agency enforcement to private individuals.[221]

While it may take years to implement these more progressive solutions, they at least attempt to shift the costs of spam back onto senders and address the problems associated with its high-volume nature. Proposals such as the Penny Black project and e-mail postage would impose costs on senders much like the costs imposed on advertisers who use traditional methods of advertising. Although some spammers might be willing to incur these costs, it at least may deter some from sending as many spam e-mail. These solutions pick up where self-help and self-regulation methods and the CAN-SPAM Act leave off by addressing the high-volume nature of spam even if the messages are legitimate advertisements from legitimate businesses and attempt to re-shift the costs back onto senders.

V. CONCLUSION

Unlike traditional methods of advertising, the unique characteristics of spam make the problem highly difficult to combat. Spam's low-cost, high-volume nature make it a highly lucrative business since spammers need only generate one positive response out of thousands in order to make a quick profit. Part of what makes spam low cost is its inherent cost-shifting structure. Rather than spammers paying for their advertisements, it is spam recipients—individuals, ISPs, and businesses—who are harboring many of the monetary and non-monetary costs associated with spam, making spam distinct from traditional advertising campaigns that rely on advertisers themselves to incur the costs.

As spam worsens, responses to it have become more sophisticated, ranging from vigilantism to legislation to private-market technological solutions. When spam first became problematic, individual recipients engaged in mailbombing and creating blacklists. In addition, complaints were filed with ISPs. As the problem worsened, state regulation of spam emerged. However, state legislative solutions lacked uniformity and failed to address jurisdictional problems. Passed in 2003, the federal CAN-SPAM Act attempted to address some of the problems associated with earlier efforts at combating spam. The advantages of the Act are that it provides more uniformity than state laws and aims to combat fraudulent or misleading spam. However, critics are quick to point out that the CAN-

220. *Id.*
221. *Id.*

SPAM Act might actually increase spam because it provides a set of guidelines on how to send spam legally. As promising as these approaches appeared at their inception, each of them has significant shortcomings.

Perhaps the solution to spam will lie with more innovative, non-legislative solutions. In this way, progressive solutions such as the Penny Black project, e-postage, and bounty payments might render legislative solutions less of a necessity. While legislation may help in lessening the volume of fraudulent or misleading e-mail, other progressive, non-legislative solutions may help address more directly the mass volume of all spam messages. By reshifting the costs back onto spam senders, progressive solutions may better address spam's unique high-volume, cost-shifting structure.

Ultimately, the most effective method to combating spam is a multi-prong approach, incorporating many of these various solutions. State and federal legislation can be effective in regulating spam sent from legitimate, identifiable businesses. Additionally, technological and other progressive solutions can help to counteract fraudulent spam and the most pernicious, anonymous spammers. A combination of these approaches will ensure not only the legitimacy of spam as a quick and efficient form of communications but also decrease the quantity of spam by re-shifting costs back onto those who should have been paying for it all along—the senders.