HAS THE U.S. CANNED SPAM?

Elizabeth A. Alongi*

I. LETTING SPAM OUT OF THE CAN

Spam[1] was born in Arizona in April 1994 when two Phoenix attorneys sent an advertisement over the Internet to some 8,000 Usenet newsgroups.[2] The ad reached over twenty million people, and the resulting irate response crashed their Internet Service Provider's ("ISP") computer.[3] Although the ad did not result in new clients for the attorneys, the marketing technique gained widespread popularity among companies trying to sell a variety of products, from moneymaking schemes and pornography to health, weight loss, and sexual dysfunction products.[4]

Since its inception in 1994, the use of spam has grown exponentially, increasing from eight percent of all e-mail traffic in 2001 to fifty-six percent in 2003.[5] Today, Spam is considered a mainstream marketing option, into which companies poured $1.3 billion in 2002.[6] Conversely, estimates place the costs to

---

* J.D. candidate, University of Arizona James E. Rogers College of Law, 2004. The Author would like to thank her family for their inspiration, advice and support.

1. For the purposes of this Note, spam, unsolicited commercial e-mail ("UCE"), and unsolicited bulk e-mail ("UBE") will be used interchangeably. For a discussion of the differences, see David E. Sorkin, *Technical and Legal Approaches to Unsolicited Electronic Mail*, 35 U.S.F. L. REV. 325 (2001).

2. Credence E. Fogo, *The Postman Always Rings 4,000 Times: New Approaches to Curb Spam*, 18 J. MARSHALL J. COMPUTER & INFO. L. 915, 915 (2000).

3. *Id.* An ISP is an organization that provides access to the Internet. Techweb, *Internet Service Provider*, *at* http://www.techweb.com/encyclopedia/defineterm?term=Internetserviceprovider (last visited Feb. 21, 2003).

4. Christopher Scott Maravilla, *The Feasibility of a Law to Regulate Pornographic, Unsolicited Commercial E-Mail*, 4 TUL. J. TECH. & INTELL. PROP. 117, 119 (2002); Nat'l Office for the Info. Econ. of the Commonwealth of Australia, *Spam Interim Review Report*, *at* http://www.noie.gov.au/projects/confidence/Improving/Spam/Interim_Report/major_problems_caused_by_spam (last visited Nov. 9, 2002).

5. Jonathan Krim, *FTC Files Suit Against Sender of Porn 'Spam,'* WASH. POST, Apr. 18, 2003, at E1; *Federal Anti-Spam Law Guts Tough State Remedies*, USA TODAY, Dec. 23, 2003, at A14.

6. Joanna L. Krotz, *The 11th Commandment: Thou Shalt Not Spam*, *at* http://www.bcentral.com/articles/krotz/138.asp?format=print (last visited Sept. 30, 2002).

corporations and ISPs at $11.9 billion in the United States and Europe for the same time period.[7] This estimated cost includes lost productivity, more expensive servers and additional bandwidth,[8] customer support for disgruntled users, time spent deleting messages, time spent by people who mistakenly click on spam messages, and time spent tracking down messages deleted by spam filters.[9] America Online ("AOL") estimates that eighty percent of its inbound e-mail is spam.[10] In a twenty-four hour period, AOL blocks 1.5 to 1.9 billion spam messages, and still thirty to forty percent of messages that reach in-boxes are spam.[11] The average Internet user receives about twenty-eight spams per day.[12] The cost to ISPs totals at least $500 million per year.[13] ISPs spend at least ten percent of their operating costs on filtering bulk messages, responding to customer complaints, purchasing additional bandwidth to process traffic, and buying more computers for message storage.[14] ISPs pass these costs on to consumers at a rate of $2–3 of the monthly Internet fee.[15] Additional costs accrue due to the investigation and prosecution of fraudulent spam—spam sent with false claims or false identities. The Federal Trade Commission ("FTC") receives 120,000 consumer complaints daily[16] and estimates that sixty-six percent of spam contains false information.[17] It announced in November 2003 that it had taken more than 285 criminal and civil law enforcement actions against internet scams and deceptive spam.[18]

Consumers, ISPs, states and countries continue to struggle with problems created by spam. Consumers buy the latest filtering software, create safe lists, block senders and create new e-mail accounts to avoid spammers' mailing lists. ISPs hire employees to screen spam, install filtering programs, terminate spammer accounts, and file lawsuits.[19] Some of the more imaginative remedies proposed

---

7. Mitch Wagner, *Reports: Spam Costs $11.9 Billion; Users Favor Legal Ban*, *at* http://www.internetwk.com/shared/printableArticle.jhtml?articleID=6000048 (last visited February 21, 2003).

8. Bandwidth is the transmission capacity of an electronic pathway—a communications line, computer bus, or computer channel—measured in bits or bytes or cycles per second. Techweb, *Bandwidth*, *at* http://www.techweb.com/encyclopedia/defineterm?term=bandwidth (last visited Feb. 24, 2003).

9. Wagner, *supra* note 7.

10. Paul Davidson, *Facing Dip in Subscribers, America Online Steps Up Efforts to Block Spam*, USA TODAY, Apr. 17, 2003, at 3B.

11. *Id.*

12. Hon. Jefferson Lankford, *Spam: The End of E-Mail?*, ARIZ. ATTORNEY, July/Aug. 2003, at 14.

13. *Id.*

14. Edwin L. Klett & Rochelle L. Brightwell, *Spam Mail: An Electronic Nuisance to Be Reckoned With*, 4 NO. 11 LAWYERS J. 11, 11 (May 31, 2002).

15. *Id.*

16. Krim, *supra* note 5.

17. *FTC Study Finds Deception in 66 Percent of Spam*, 20 COMPUTER & INTERNET LAW. 34, 34 (2003).

18. Heather Fleming Phillips, *The Do-Not-Underestimate FTC Chairman; Muris Pushed Through Telemarketing Law, Now Is Going After Fraudulent Spammers*, SAN JOSE MERCURY NEWS, Jan. 2, 2004, at 1.

19. Fogo, *supra* note 2, at 920–22.

include putting spammers in a cell to read every word of every spam message ever sent (perhaps "cruel and unusual punishment"),[20] and installing a button that "traces spam back to the computer it came from and causes it to explode in a big orange fireball. Or melt into a smoking black puddle."[21] Although these last solutions seem ridiculous, they illustrate the frustration felt by the average spam recipient. A consumer can expect to receive 2,200 spam e-mails per year.[22] If it takes ten seconds to look at each one to ensure that it is spam, six hours each year will be spent "canning" spam.[23]

To date, many states and countries have enacted different kinds of legislation to regulate spam.[24] The state of Arizona recently addressed the problem by enacting its own legislation to regulate commercial electronic mail.[25] In response to nationwide concern regarding the problems created by spam, several bills were introduced in the House of Representatives and Senate to regulate headers, opt-out instructions, and sexually explicit material.[26] The United States recently adopted the CAN-SPAM Act as an answer to the problems of spam.[27]

This Note will first examine other countries' attempts to control spam and the steps individuals have taken using technology and traditional causes of action. It will then look at the laws passed by many states and the CAN-SPAM Act recently passed by the United States Congress. Finally, it will discuss the problems faced in trying to solve international problems with a national solution and whether the CAN-SPAM Act is up to the challenge.

II. INTERNATIONAL ATTEMPTS TO CAN SPAM

Because the Internet is a worldwide medium, the most effective way to combat spam might be worldwide regulation. Someday, an effort to combat spam through treaties may be coordinated. In the meantime, many countries have begun adopting laws that regulate spam.

---

20. Stephen J. Harhai, *A Modest Proposal on Spam: How Can We Deal With the People Who Trash Our Inboxes? Possible Punishments and Solutions*, 29 LAW PRAC. MGMT. 16 (2003).

21. Leonard Pitts, *African Revenge: Steady Diet of Spam*, ARIZ. DAILY STAR, May 7, 2003.

22. Don Passenger & Jeff Kirkey, *Un-Canned Spam*, 82 MICH. BAR J. 36, 36 (2003). This Author received twenty spams on Oct. 1, 2003, to a Hotmail account. Some of the misleading subject lines include "Account inf here," "Re: what happened next," and "what do you think about this." There were three ads for viagra, four ads for insurance, one for mortgage refinancing, four for pornography, and seven in which the product could not be determined from the subject line (on file with Author).

23. Passenger & Kirkey, *supra* note 22, at 36.

24. For a comprehensive overview, see David E. Sorkin, *Spam Laws*, *at* http://www.spamlaws.com (last visited Oct. 6, 2003).

25. ARIZ. REV. STAT. §§ 44-1372 to 44-1372.05 (2003). The Arizona House of Representatives unanimously passed S.B. 1280 on April 3, 2003. *House Unanimously Passes Spam Protection*, ARIZ. DAILY STAR, Apr. 4, 2003, at A13.

26. Klett & Brightwell, *supra* note 14, at 19.

27. Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, 15 U.S.C. §§ 7701–7713 (2004).

A. European Union

The European Parliament voted to ban spam, passing the Directive on Privacy and Electronic Communications ("Directive") in May 2002.[28] The Directive prohibits unsolicited commercial communications sent by e-mail, fax, or automated calling machines without the prior permission of the user.[29] Direct marketing material may only be sent to those who have given prior consent (opt-in), except in the case of an existing commercial relationship, wherein the recipient must be offered a free opt-out option.[30] Mail without a valid return address or with concealed identity is prohibited.[31] The rationale for the Directive is two-fold: 1) that subscribers should be given safeguards against intrusion to their privacy; and 2) that these forms of communication are inexpensive and easy to send, but impose a burden and/or cost on the recipient.[32] European Union members that have enacted opt-in legislation include Austria, Denmark, Finland, Germany, Greece, and Italy.[33] Belgium and Spain enacted opt-out legislation.[34] There is not yet data reflecting the effectiveness of these laws.

B. United Kingdom

On June 17, 2003, Microsoft announced that it filed two cases in the United Kingdom ("UK") in its efforts to combat and deter spam, alleging that harvesting e-mail account names and other illegal spamming practices violated the UK Misuse of Computers Act of 1990.[35] The Misuse of Computers Act forbids unauthorized access to computer material.[36] A person is guilty if he causes a computer to perform any function with the intent to secure access to any program or data held in any computer, the access is unauthorized, and he knows the access is unauthorized at the time he commits the act.[37] Penalties consist of fines and/or imprisonment for up to six months.[38] Under this statute, Microsoft argues that hacking into servers to harvest account names amounts to unauthorized access.[39] If Microsoft is successful, the Misuse of Computers Act may discourage spammers targeting the UK.

---

28. Council Directive 2002/58/EC, 2002 O.J. (L 201) 37 [hereinafter Directive on Privacy and Electronic Communications]; *see also* Nat'l Office for the Info. Econ. of the Commonwealth of Australia, *Spam Interim Review Report*, *at* http://www.noie.gov.au/projects/confidence/Improving/Spam/Interim_Report/key_issues (last visited Nov. 9, 2002); Sorkin, *supra* note 24.

29. Directive on Privacy and Electronic Communications, *supra* note 28.

30. *Id.*

31. *Id.*

32. *Id.*

33. Eurocauce, *Fighting European Spam*, *at* http://www.euro.cauce.org/en/countries/index.html (last visited Nov. 9, 2002); *see also* Sorkin, *supra* note 24.

34. Eurocauce, *supra* note 33.

35. Computer Misuse Act, 1990, c. 18; *Microsoft Files 15 Lawsuits Against Spammers in the US and UK*, 20 COMPUTER & INTERNET LAW. 28, 28 (2003).

36. Computer Misuse Act, 1990, c. 18 § 1.

37. *Id.* § 1(1) & (2).

38. *Id.* § 3.

39. *Microsoft Chooses Mishcons for Assault Against Spammers*, LAW., June 23, 2003, *available at* 2003 WL 61848586.

C. Japan

Japan passed legislation in July 2002 requiring senders to inform recipients when an e-mail consists of unsolicited advertising and to give instructions on how future ads may be rejected.[40] It also prohibits sending e-mail to consumers who opt-out and sending e-mail to nonexistent addresses.[41] Complaints from people who receive junk mail on mobile phones provided the impetus for new legislation in Japan,[42] where up to ninety percent of text messages on cellular phones are spam.[43] If a sender does not comply with the government-issued cease and desist order, a fine of up to half a million yen may be imposed.[44] In the first court decision against Japan spammers, a Tokyo company was ordered to pay a mobile e-mail service, DoCoMo, 6.57 million yen.[45] Four million of that was to reimburse DoCoMo for the expense of returning e-mails sent to its network addressed to phone numbers that did not exist.[46] The remaining 2.57 million yen compensated DoCoMo for consultation and legal fees connected to the case.[47] The results of this first case should prove a deterrent to Japanese spammers.

D. South Korea

South Korea suffers from the flood of spam as well. In 2001, an average Internet user in South Korea received 4.7 spams per day; by March of 2003, the number increased to 50 per day.[48] In 2002, the Korea Information Security Agency documented 90,786 reports complaining of unsolicited spam and 15,290 reports of obscene and harmful materials.[49] The total in 2002 amounted to 326-times the 325 cases reported in 2000.[50] As of April 2003, the number was already 47,000.[51] Obscene e-mail now accounts for sixty-three percent of reported spam, raising concerns about harmful effects on children.[52] Since Korea presently relies on an opt-out system, anyone can send unsolicited advertising until the account holder requests that they stop.[53] In response to the increasing social and economic damage caused by spam, the Ministry of Information and Communication formed a joint management committee to assist the government in solving the problem.[54] Some

---

40. *Law on Unsolicited Email Takes Effect*, JAPAN TODAY, July 1, 2002.
41. *Id.*
42. *Id.*
43. Jonathan Turley, *Congress Has to Take Action to Stem Spam*, NEWSDAY (N.Y.), Apr. 23, 2003, at A33.
44. Toru Takahashi, *2 New Laws Aimed at Cutting Spam*, DAILY YOMIURI, July 1, 2002, *available at* 2002 WL 19074087.
45. *DoCoMo Wins Spam-Mail Fight in Tokyo Court*, SAIGON TIMES DAILY, Mar. 27, 2003, *available at* 2003 WL 4470291 (6.57 million yen converts to 54,420 U.S. dollars).
46. *Id.*
47. *Id.*
48. *Canning the Rising Cost of Spam*, JOINS.COM, May 31, 2003, *available at* 2003 WL 62907057.
49. *Id.*
50. *Id.*
51. *Id.*
52. *Id.*
53. *Id.*
54. *Id.*

spam-related laws have been revised to increase penalties for those who send harmful materials to children, but they are not proving effective.[55] The new joint management committee hopes to have a bigger impact.[56]

E. Australia

Recent reports estimate that spam costs industry in Australia approximately $960 per employee in lost productivity each year.[57] The Australian government adopted the Spam Act of 2003, which went into effect April 11, 2004.[58] The maximum penalty that may be imposed is $2,200 per incident for individuals (up to $44,000 per day) or $11,000 per incident for corporations (up to $220,000 per day).[59] The legislation includes requiring vendors to identify themselves with accurate names and genuine physical and electronic addresses, creating an opt-in system that bans messages unless the users have consented to receive messages or there is an established business relationship, and banning e-mail harvesting software.[60] Officials acknowledge that such legislation is likely not enough to stem the tide completely, so they are coordinating a response that includes legislation plus filtering technology and industry participation, as well as working with international organizations to develop global guidelines and cooperation.[61]

F. Canada

Canada has yet to adopt anti-spam legislation, relying instead on privacy legislation, market competition and individual lawsuits to control spam.[62] Michael Geist, a Canadian law professor and e-commerce director, noted that Canada needs to review its policy because it fails to relieve consumers of spam costs.[63] A consumer can choose a service provider based on how their ISP counters spam, but every provider must still expend resources to combat spam and pass those costs on to consumers.[64] Therefore, consumers must still pay not to receive spam. Privacy laws were not written to combat spam, and apply only to brokers who sell e-mail

---

55. *Id.* Penalties now consist of fines up to ten million won or two-year's imprisonment. *Id.*

56. *Id.*

57. Garry Barker, *Spam Legislation Unlikely to Stem the Tide*, AGE (Melbourne), Apr. 22, 2003, at 1.

58. Graeme Samuel & Lin Enright, *ACCC Joins International Campaign to Reduce Spam*, MONDAQ BUS. BRIEFING, Mar. 3, 2004, *available at* 2004 WL 69982553.

59. Nat'l Office for the Info. Econ. of the Commonwealth of Australia, *Spam—Frequently Asked Questions*, *at* http://www.noie.gov.au/projects/confidence/Improving/Spam/Info.htm#extent (last visited Apr. 5, 2004).

60. *Id.*

61. *Id.* In fact, the Australian government recently entered into an anti-spam agreement with South Korea to exchange information. Adam Turner, *Spam Fight to Go Global*, AGE (Melbourne), Feb. 24, 2004, at 2.

62. Michael Geist, *Time to Hit Delete Key on Weak Spam Policy*, *at* http://theglobeandmail.com/servlet/ArticleNews/printarticle/gam/20020530/TWGEIS2 (last visited May 30, 2003).

63. *Id.*

64. *Id.*

lists, not the spammers who use the lists.[65] Illustrating the legislation's ineffectiveness, the first criminal case involving the use of spam resulted in acquittal because the Crown could not prove criminal intent, only a pecuniary motive.[66] According to Professor Geist, market solutions and current legal remedies in Canada fail to effectively combat spam.[67]

Attempts to control spam by the European Union, Japan, South Korea, Australia, and Canada demonstrate the wide-reaching significance of this international problem. Because spam is sent and received internationally, the most effective way to control the proliferation of spam would arguably be international laws and treaties. So far, regulations have been patchwork attempts to solve the problem and different solutions are being tested in different countries. It is too soon to tell which, if any, are affecting the desired result.

III. INDIVIDUAL ATTEMPTS TO CAN SPAM

Consumers and service providers have long waged a battle with spam. A recent survey found that eighty percent of Internet users are "very annoyed" by spam and seventy-four percent are in favor of making bulk e-mail illegal.[68] Consumers employ various measures to cut down the amount of spam received—deleting spam, employing spam filters, changing e-mail addresses, and keeping e-mail addresses private.[69] Service providers use service agreements that prohibit spamming, professionals who monitor e-mails and block mass mailings of spam ("spam catchers"), spam-blocking software, and litigation.[70] Spammers respond by finding ways to circumvent filters, including forging their e-mail address so that the recipient cannot find its origin ("spoofing") and sending anonymous e-mail ("remailing").[71] Because only the larger ISPs can afford litigation, many spammers have begun targeting smaller service providers without the resources to litigate.[72]

Using spam is cheap and it works—only one consumer in 10,000 needs to respond for the spammer to make a profit.[73] The number of spams sent daily is approximately thirteen billion.[74] Estimates put the profitability of spam at twelve percent of the $138 billion internet commerce marketplace.[75] Some predict that

---

65. *Id.*

66. The Queen v. Hamilton, [2002] 3 Alta. L.R.4th 147. The case involved mass advertising of documents for sale that would instruct the buyer how to make bombs, break into homes, and generate credit card numbers. *Id.*

67. Geist, *supra* note 62.

68. Stefanie Olsen, *Net's New Year Resolution: Outlaw Spam*, *at* http://msn.com.com/2102-1106-979108.html (last visited Jan. 7, 2003).

69. Peter Briden, *Spam: The Dark Side of Internet E-Mail*, 4 No. 11 LAWYERS J. 10, 10 (2002).

70. Kenneth C. Amaditz, *Canning "Spam" in Virginia: Model Legislation to Control Junk E-Mail*, 4 VA. J. L. & TECH. 4, 15–17 (1999).

71. *Id.* at 16.

72. *Id.* at 17.

73. *Id.* at 18.

74. Chris Gaither, *Firms Scramble in Face of Spam Law There's Little Time to Tweak Marketing*, BOSTON GLOBE, Dec. 29, 2003, at C1.

75. Paul Rubell, *New Federal Law to Take Effect, But Will Spam Be Conquered?*, 230 N.Y. L.J. 16, 16 (2003).

spam will continue to proliferate until the Internet's usefulness for e-mail disappears because it is no longer quick and useful.[76] One 2002 study estimated that the number of e-mails will grow from 31 billion a day to 60 billion a day by 2006, and advertising e-mails will increase from 33% to 50% of the e-mail sent.[77] The free market, technology and self-regulation have failed to slow the growth of spam, to mitigate cost-shifting, or to uphold user privacy.[78]

Internet Service Providers first attempted to stop spammers by bringing suit under existing causes of action, such as common law trespass to chattels, the Lanham Act,[79] and the Computer Fraud and Abuse Act (CFAA).[80]

A. Trespass to Chattels

Trespass to chattels has been resurrected as a viable cause of action to combat spam, with mixed results. In California, in *Ferguson v. Friendfinders*,[81] the Court of Appeals dismissed the trespass to chattels claim because the plaintiff failed to demonstrate actual damage.[82] In *Intel v. Hamidi*,[83] the California Supreme Court concluded that Intel did not demonstrate an injury to its personal property, or to its legal interest in that property, to support an action for trespass to chattels,[84] even though Hamidi, a disgruntled past employee, sent 200,000 e-mail messages to Intel employees, distracting employees from their assigned tasks and undermining the utility of their computer network.[85]

Trespass to chattels has met with more success as a means to ban spam under Virginia and Ohio law. AOL sued Joseph Melle in the Eastern District of Virginia, alleging trespass to chattels, in addition to others causes of action.[86] The court found that Melle (acting as creator and operator of TSF Industries) improperly sent unauthorized bulk e-mail advertisements to AOL subscribers totaling over sixty million e-mails in the course of ten months.[87] He then continued to send e-mails after being notified by AOL in writing to cease and desist these activities,[88] causing AOL to expend technical resources and staff time to defend its computer system and membership against the spam.[89] These facts established a trespass to chattels in violation of Virginia common law.[90]

---

76. *Id.*
77. Christopher Saunders, *Study: E-Mail to Double by 2006*, *at* http://www.clickz.com/news/article.php/1471801 (last visited Nov. 10, 2002).
78. Amaditz, *supra* note 70, at 20.
79. 15 U.S.C. § 1125 (2003).
80. 18 U.S.C. § 1030 (2003).
81. 94 Cal. App. 4th 1255 (2002), *rev. denied* (2002).
82. *Id.* at 1260.
83. 30 Cal. 4th 1342 (2003).
84. *Id.* at 1360.
85. *Id.* at 1367 (Brown, J., dissenting).
86. Am. Online, Inc. v. IMS, 24 F.Supp.2d 548, 549 (E.D. Va. 1998).
87. *Id.* at 549.
88. *Id.*
89. *Id.*
90. *Id.* at 550.

In 2001, the Northern District of Iowa also examined trespass to chattels under Virginia law when AOL sued National Health Care Discount, Inc. ("NHCD").[91] The court found NHCD liable for the actions of its contract e-mailers and held that their actions constituted trespass to chattels.[92] The court issued a permanent injunction against sending electronic mail messages to or through AOL, its network or its members, compiling AOL member addresses, and accepting prospective customer information generated using e-mail sent to or through AOL, its network or its members.[93] After considering various ways of measuring damages, the court awarded AOL the amount of $2.50 per thousand messages for the 135 million messages sent, totaling $337,500, plus interest and attorney fees.[94]

In Ohio, CompuServe brought action against Cyber Promotions for sending e-mail solicitations to CompuServe subscribers, claiming trespass to chattels.[95] The court noted that a plaintiff can sustain an action for trespass to chattels without showing substantial interference with its right to possession.[96] Liability can be predicated on harm to "personal property or diminution of its quality, condition, or value."[97] The court examined evidence that CompuServe's value in its computer equipment is wholly derived from the extent to which it serves its subscribers.[98] Handling mass mailings places a tremendous burden on its equipment.[99] The defendant's practice of disguising the origin of its messages causes an even bigger burden because CompuServe servers are forced to store undeliverable e-mail messages, trying in vain to return them to an address that does not exist.[100] The court then found the value of CompuServe's equipment to be diminished despite the lack of physical damage caused by defendant's conduct.[101]

CompuServe also argued that recovery is justified for a trespass that causes harm to something in which the possessor had a legally protected interest, namely damage to their business reputation and goodwill, demonstrated by customer complaints totaling fifty per day.[102] Cyber Promotions argued that CompuServe consented to community use of their servers by allowing subscribers to receive messages from individuals and entities located anywhere on the Internet,

---

91. Am. Online, Inc. v. Nat'l Health Care Discount, Inc., 174 F.Supp.2d 890 (N.D. Iowa 2001).

92. *Id.* at 900.

93. *Id.* at 902.

94. *Id.* at 901. The court considered that the cost of delivering an email is $.00078 and that AOL charges banner advertisements at an average of $8.56 per thousand impressions. The court concluded that charging $.00078 would not adequately compensate AOL for its damages, but $8.56 would over-compensate AOL, and so $2.50 per thousand emails would be appropriate to compensate AOL for the use of its computer system. This amount was approximately the same that NHCD paid its e-mailers. *Id.*

95. CompuServe, Inc. v. Cyber Promotions, Inc., 962 F.Supp. 1015, 1017 (S.D. Ohio 1997).

96. *Id.* at 1022.

97. *Id.*

98. *Id.*

99. *Id.*

100. *Id.*

101. *Id.*

102. *Id.* at 1023.

in effect arguing that the trespasser had consent to use the property.[103] However, the court found that any privilege ended when CompuServe notified the defendant that its use of CompuServe equipment was unacceptable.[104] The court granted a preliminary injunction enjoining Cyber Promotions from sending any unsolicited advertisements to any e-mail address maintained by CompuServe during the pendency of the action.[105]

These cases indicate that trespass to chattels can be a viable cause of action in the context of ISP equipment, even absent physical injury to property, when evidence indicates bulk mailings constitute a burden to the ISP's business operations or harms its goodwill.

B. Lanham Act—Damage to Trademarks

In addition to trespass to chattels, AOL has also used a cause of action for false designation of origin and dilution of trademark under the Lanham Act against spammers. [106] False designation of origin is a violation of the Lanham Act,[107] which was enacted to provide national protection to trademarks in order to secure the owner's goodwill in his business and protect the ability of consumers to distinguish among competitors.[108] The elements of false designation are: 1) the violator employed a false designation; 2) the false designation deceived as to origin, ownership, or sponsorship; and 3) the plaintiff believed that he was likely to be damaged by such an act.[109] In this case, the messages sent contained "aol.com" in their headers, creating a false designation.[110] AOL members were deceived into thinking that AOL sponsored or approved the bulk e-mailing activity.[111]

The court also found that the false designation caused damage to AOL, amounting to trademark dilution.[112] Dilution of trademark is another violation of the Lanham Act.[113] A dilution claim requires a showing of the ownership of a distinctive mark and a likelihood of dilution.[114] The court found that AOL clearly owns the distinctive "AOL" mark because it is registered with the United States Patent and Trademark Office and is used by AOL and recognized throughout the world in association with its products and services.[115] The court held that the mark was diluted by tarnishment, because of the strong likelihood of dilution by negative association. [116] AOL subscribers associated the junk e-mailing practices

---

103. *Id.* at 1023–24.
104. *Id.* at 1024.
105. *Id.* at 1028.
106. Am. Online, Inc. v. IMS, 24 F.Supp.2d 548, 549 (E.D. Va. 1998).
107. 15 U.S.C. § 1125(a)(1) (2003).
108. *IMS*, 24 F.Supp.2d at 551.
109. 15 U.S.C. § 1125(a)(1).
110. *IMS*, 24 F.Supp.2d at 551.
111. *Id.*
112. *Id.*
113. 15 U.S.C. § 1125(c).
114. *Id.*
115. *IMS*, 24 F.Supp.2d at 552.
116. *Id.*

of the defendant with AOL, as demonstrated by the 50,000 complaints to AOL about the defendant's spamming.[117] America Online thus prevailed under these Lanham Act theories.

C. Computer Fraud and Abuse Act

America Online also achieved a victory against spam using the Computer Fraud and Abuse Act ("CFAA") in *America Online, Inc. v. National Health Care Discount, Inc.* ("NHCD").[118] To prevail on a civil claim under the CFAA, a plaintiff must prove that: 1) the person or entity intentionally accessed a computer; 2) they exceeded authorized access; 3) they obtained information; 4) the computer was a "protected computer;" and 5) their conduct involved an interstate communication.[119] The court found that when NHCD's e-mailers harvested e-mail addresses of AOL members and sent them unsolicited bulk e-mail messages, they were accessing AOL's computers.[120] AOL clearly advises members that they are not authorized to harvest e-mail addresses or send bulk e-mail, so they exceeded authorization.[121] Under the CFAA, a plaintiff must prove damage, impairment to the integrity or availability of data, aggregating at least $5000 in value in a one-year period.[122] The court found that even though NHCD's spam was only a fraction of spam sent to AOL's members, AOL proved that it caused substantial loss, exceeding $5000 in 1997, 1998, and 1999.[123] The use of the CFAA led to a victory for AOL, demonstrating the benefits of creative lawyering and seeking damages under a variety of causes of action. But the available causes of action were not enough to slow the growing use of spam, so ISPs and consumers turned to state legislators.

IV. STATE LAWS AND CONSTITUTIONAL OBJECTIONS

Consumers and ISPs turned to local regulation of spam in the absence of a national regulatory scheme. A majority of states enacted spam legislation to regulate commercial e-mail or adopted bar rules addressing unsolicited commercial e-mail sent by attorneys.[124] Many of these laws prohibit the use of

---

117. *Id.*

118. Am. Online, Inc. v. Nat'l Health Care Discount, Inc., 174 F.Supp.2d 890 (N.D. Iowa 2001); 18 U.S.C. § 1030 (2003). The plaintiff also succeeded under trespass to chattels. *See* discussion *supra* notes 91–94 and accompanying text.

119. *Nat'l Health Care Discount*, 174 F.Supp.2d at 899.

120. Am. Online, Inc. v. Nat'l Health Care Discount, Inc., 121 F.Supp.2d 1255, 1273 (N.D. Iowa 2000).

121. *Id.*

122. 18 U.S.C. § 1030(e)(8)(A) (amended 2001).

123. *Nat'l Health Care Discount*, 174 F.Supp.2d at 899.

124. *See* David E. Sorkin, *Spam Laws: Summary*, *at* http://www.spamlaws.com/state/summary.html (last visited Sept. 30, 2002). *E.g.*, COLO. RULES OF PROF'L. CONDUCT R. 7.3(d) (West 2003) (requiring "this is an advertisement" at the beginning and end of any electronic communication); FLA. RULES OF PROF'L. CONDUCT R. 4-7.6(c)(3) (West 2003) (requiring "legal advertisement" in the subject line of electronic mail communications); LA. RULES OF PROF'L. CONDUCT R. 7.2(b)(iii)(B) (West 2003) (requiring "This is an advertisement for legal services" in the subject line of an electronic mail communication); N.M. RULES OF PROF'L. CONDUCT R. 16-701(D) (West 2003) (requiring "LAWYER

false or missing routing information,[125] and some require opt-out information.[126] Several require labeling on subject lines, such as "ADV" for advertisements[127] or "ADV:ADLT" for sexually explicit materials.[128] Some laws apply only to messages sent from computers or service providers located within the state,[129] while others apply to messages sent to state residents from outside the state, if the sender has reason to know that the message is being sent to a state resident.[130]

ADVERTISEMENT" at the beginning of the advertisement); WYO. RULES OF PROF'L. CONDUCT R. 7.3(b) (West 2003) (requiring "Notice: This is an advertisement" to appear on the first page, in bold and in a type size and legibility to be conspicuous).

125. *E.g.*, COLO. REV. STAT. ANN. § 6-2.5-103(2) (West 2003); CONN. GEN. STAT. ANN. § 53-451(b)(7) (West 2003); DEL. CODE ANN. tit. 11, § 937(2) (2003); IDAHO CODE § 48-603E(3) (Michie 2003); 720 ILL. COMP. STAT. ANN. 5/16D-3(a)(5) (West 2003); IOWA CODE ANN. § 714E.1(2)(b) (West 2003); LA. REV. STAT. ANN. § 14:73.6(B) (West 2003); MINN. STAT. ANN. § 325F.694(2)(1) (West 2003); N.C. GEN. STAT. § 14-458(a)(6) (2003); R.I. GEN. LAWS § 6-47-2(d) (2003); WASH. REV. CODE ANN. § 19.190.020(1)(a) (West 2003).

126. *E.g.*, CAL. BUS. & PROF. CODE § 17538.4(a) (West 2003) (requiring toll-free number or valid email address in the first text of the message); COLO. REV. STAT. ANN. § 6-2.5-103(5) (requiring free opt-out mechanism); IDAHO CODE § 48-603E(3) (prohibiting sending to senders who requested to decline receiving advertisements); IOWA CODE ANN. § 714E.1(2)(d) (requiring an email address for recipient to opt-out); MINN. STAT. ANN. § 325F.694(4) (requiring toll-free number, valid return email address or another easy-to-use method to opt-out); MO. ANN. STAT. § 407.1123.1 (West 2003) (requiring toll-free number or return email address so recipient may opt-out); R.I. GEN. LAWS § 6-47-2(a) (requiring toll-free number or email address so recipient may opt-out); TENN. CODE ANN. § 47-18-2501(a) (2003) (requiring establishment of toll-free number or return email address so recipient may opt-out).

127. *E.g.*, CAL. BUS. & PROF. CODE § 17538.4(g); COLO. REV. STAT. ANN. § 6-2.5-103(4); MINN. STAT. ANN. § 325F.694(3); S.D. CODIFIED LAWS § 37-24-6(13) (Michie 2003); TENN. CODE ANN. § 47-18-2501(e).

128. *E.g.*, CAL. BUS. & PROF. CODE § 17538.4(g) (ADV:ADLT); MINN. STAT. ANN. § 325F.694(3) (ADV—ADULT); S.D. CODIFIED LAWS § 37-24-6(13) (ADV:ADLT); TENN. CODE ANN. § 47-18-2501(e) (ADV:ADLT); WIS. STAT. ANN. § 944.25(2) (West 2003) (ADULT ADVERTISEMENT).

129. *E.g.*, CAL. BUS. & PROF. CODE § 17538.4(d) (delivering documents to California resident via service or equipment located in California); COLO. REV. STAT. ANN. § 6-2.5-105 (West 2004) (sending messages to a Colorado resident via service or equipment located in Colorado); IOWA CODE ANN. § 714E.1(5) (transmitting mail to or through a network located in Iowa); 815 ILL. COMP. STAT. ANN. 511/10(b) (West 2003) (delivering mail to Illinois resident via service or equipment located in Illinois); MINN. STAT. ANN. § 325F.694(1)(b) (sending messages through ISP facilities located in Minnesota to a Minnesota resident); TENN. CODE ANN. § 47-18-2501(f) (delivering documents to a Tennessee resident via a service or equipment located in Tennessee).

130. *E.g.*, DEL. CODE ANN. tit. 11, § 937(4) (conducting acts outside the state is sufficient if the defendant was aware of a reasonable possibility the message would go to a Delaware resident); R.I. GEN. LAWS § 6-47-2(a) (transmitting from a computer in Rhode Island or to an address that the sender knows or has reason to know is held by a Rhode Island resident); WASH. REV. CODE ANN. § 19.190.020(1) (transmitting from a computer in Washington or to an address that the sender knows or has reason to know is held by a Washington resident).

From the few cases litigated since enactment of anti-spam laws, it appears that courts will find legislation that regulates some aspects of spam constitutional. To date, the most common concerns regarding the constitutionality of spam laws have been whether they violate the commerce clause, the First Amendment right of free speech, or the requirements of personal jurisdiction.[131] The United States Supreme Court has yet to address these issues, but lower courts that reviewed state legislation have found the laws enforceable.[132]

A. Dormant Commerce Clause Challenges

1. Washington

A Washington court imposed a fine of almost $100,000 in the first case brought under a law that makes it illegal to send messages that mask the identity of the sender or that contain false or misleading information in the subject line.[133] Beginning in 1997, Jason Heckel, an Oregon resident, began sending unsolicited commercial e-mails selling a booklet entitled "How to Profit from the Internet."[134] In 1998, Heckel sent between 100,000 to 1,000,000 messages per week and sold 30 to 50 booklets per month.[135] In June 1998, the Washington State Attorney General's Office began receiving consumer complaints alleging that Heckel's messages contained misleading subject lines and false transmission facts in violation of Washington's Consumer Protection Act ("the Act"). [136] Washington notified Heckel of the existence of the Act and informed him of procedures bulk e-mailers must follow for compliance, but he failed to amend his practices.[137] The complaints kept pouring in, so the state of Washington filed suit.[138]

Washington stated three causes of action—first, that Heckel violated the Act by using false or misleading information in the subject line of his messages ("Did I get the right e-mail address?" and "For your review—HANDS OFF!");[139] second, that Heckel violated the Act by misrepresenting the transmission path of his messages (routing his spam through a dozen different domain names without receiving permission from the owners of those names);[140] and third, that Heckel violated the Act by failing to provide a valid return e-mail address to which recipients could respond (Heckel routinely opened e-mail accounts, sent bulk messages, then cancelled the account within two days of sending the messages).[141]

---

131. *See* Amaditz, *supra* note 70, at 34.

132. *E.g.*, Washington v. Heckel, 24 P.3d 404, 406 (Wash. 2001) (discussing the dormant commerce clause); Intel v. Hamidi, 114 Cal. Rptr. 2d 244 (Cal. App. 2001), *rev. granted* (2002) (discussing the First Amendment right to free speech); Internet Doorway v. Parks, 138 F.Supp.2d 773, 774 (S.D. Miss. 2001) (discussing personal jurisdiction).

133. *First "Spam" Email Case Draws $100,000 Fine*, ARIZ. DAILY STAR, Oct. 19, 2002.

134. *Heckel*, 24 P.3d at 406.

135. *Id.*

136. *Id.* WASH. REV. CODE ANN. § 19.190 (West 2003).

137. *Heckel*, 24 P.3d at 407.

138. *Id.*

139. *Id.*

140. *Id.*

141. *Id.* at 407–08.

The trial court found that the Act violated the Commerce Clause as an unconstitutional burden on interstate commerce.[142]

On appeal, the Washington Supreme Court found that the statute applied equally to in-state and out-of-state spammers.[143] Because the Act was facially neutral, the court applied the balancing test announced by the Supreme Court in *Pike v. Bruce Church, Inc.*:[144] "[w]here the statute regulates even-handedly to effectuate a legitimate local public interest, and its effects on interstate commerce are only incidental, it will be upheld unless the burden imposed on such commerce is clearly excessive in relation to the putative local benefits."[145] The court concluded that the local benefits surpass any burden on interstate commerce.[146] The local harms caused by spammers that would be alleviated by the Act include the burden on ISPs, economic injury suffered by owners of the domain names taken by the spammer, inconvenience to individual Internet users who cannot promptly and effectively respond to messages or opt-out, and the cost-shifting from deceptive spammers to Internet users.[147]

In contrast, the court noted that "the only burden the Act places on spammers is the requirement of truthfulness, a requirement that does not burden commerce at all but actually facilitates it by eliminating fraud and deception."[148] The court dismissed Heckel's arguments that the Act created inconsistency among the states and regulated conduct occurring wholly outside the state of Washington.[149] The court responded by stating that it is inconceivable that any state would ever require spammers to use misleading subject lines or transmission paths, so Washington's requirements would not be inconsistent with other states' laws.[150] Additionally, the Act covers only messages targeting a Washington resident or sent from a computer located in Washington.[151] On remand, though Heckel claimed that he only made $680 from booklet sales, he was ordered to pay a $2,000 fine and $94,000 in legal fees.[152] This examination of the Washington law shows that requiring truthfulness in advertising and notice to the sender that he is targeting consumers within the state results in an effective deterrent to misleading spam that meets the requirements of the Commerce Clause.

2. California

California recently examined its anti-spam legislation in *Ferguson v. Friendfinders*.[153] The California statute at issue regulates conduct by persons or entities doing business in California who transmit unsolicited advertising

142. *Id.* at 408.
143. *Id.* at 409.
144. 397 U.S. 137 (1970).
145. *Id.* at 142.
146. *Heckel*, 24 P.3d at 409.
147. *Id.* at 409–10.
148. *Id.* at 411.
149. *Id.*
150. *Id.* at 412.
151. *Id.* at 413.
152. *First "Spam" Email Case Draws $100,000 Fine*, *supra* note 133.
153. 94 Cal. App. 4th 1255 (2002), *rev. denied* (2002).

materials.[154] The law requires that senders establish a toll-free telephone number or a return e-mail address so that recipients may opt-out of receiving further unsolicited documents.[155] They must also notify the recipient of opt-out information in the first text of the message.[156] Sending further unsolicited material to recipients who opt-out is prohibited.[157] Messages must include "ADV" in the subject line or "ADV:ADLT" if the advertisement pertains to adult material.[158]

Mark Ferguson, a California resident, filed a complaint in 1999 alleging that Friendfinders sent him and others unsolicited e-mail that did not comply with the statute's requirements: the subject lines did not begin with "ADV," the first line of the message failed to contain opt-out information, no valid return e-mail address was included, and the headers were altered to mask the identity of the sender.[159] Ferguson alleged four causes of action: negligence, trespass to chattels, unfair business practice, and unlawful advertising.[160] The trial court dismissed the first two causes of action, finding that Ferguson failed to state a claim for negligence because Friendfinder's actions were intentional and that no actual damage had occurred to support a claim for trespass to chattels.[161] More significantly, the trial court dismissed the third and fourth causes of action because the anti-spam law violated the dormant commerce clause.[162]

On review, the California Court of Appeals held that the statute met the requirements of the U.S. Constitution for several reasons.[163] First, the court found that the statute applies equally to in-state and out-of-state actors who do business in California and transmit unsolicited e-mail to a California resident via equipment located in California.[164] Second, the court found that the statute did not try to regulate the Internet, *per se*, but instead regulated e-mail users who send spam to California residents using equipment located in California.[165] Friendfinders failed to establish that the statute could reach conduct occurring wholly outside the state or that it was impossible to determine the geographic residence of a spam recipient.[166] Third, Friendfinders tried to establish that the California statute conflicts with other statutes enacted in other states, such as Pennsylvania's requirement to use the subject "ADV ADULT" for spam containing sexually

---

154. CAL. BUS. & PROF. CODE § 17538.4(a) (West 2003).
155. *Id.*
156. § 17538.4(b).
157. § 17538.4(c).
158. § 17538.4(g).
159. *Ferguson*, 94 Cal. App. 4th at 1259.
160. *Id.*
161. *Id.* at 1259–60. Trespass to chattels requires some actual damage, unlike trespass to real property where damage is assumed. One who intentionally intermeddles with another's chattel is subject to liability only if harm resulted, either to the condition, quality, or value of the chattel or if the possessor was deprived of the use of the chattel for a substantial time. RESTATEMENT (SECOND) OF TORTS § 218 (1965). See discussion *supra* notes 81–105 and accompanying text.
162. *Ferguson*, 94 Cal. App. 4th at 1260.
163. *Id.* at 1269.
164. *Id.* at 1262.
165. *Id.* at 1264.
166. *Id.* at 1265.

explicit materials.[167] However, the court found that Friendfinders failed to demonstrate that a spammer would be forced to comply with both laws at the same time, and even if they did, Friendfinders could utilize the defense of substantial compliance.[168]

The court then balanced the state's "substantial legitimate interest" in regulating spam (citing the annoyance, waste of time, cost-shifting to recipient, ISP costs, and financial harm caused by deceptive tactics used to disguise sender's identity and the message's true nature) against the burden on interstate commerce.[169] The court cited *Heckel*, stating that requiring truthfulness in advertising does not burden interstate commerce at all "but actually facilitates it by eliminating fraud and deception."[170] The cost of placing "ADV" in the subject line and including a valid return address is "appreciably zero in terms of time and expense."[171] Any conceivable burden to the spammer in honoring a recipient's request to be removed from the mailing list was clearly outweighed by local benefits.[172]

B. First Amendment Implications

1. Private Actors

In addition to the Dormant Commerce Clause, spammers challenged state anti-spam statutes under the First Amendment.[173] Cyber Promotions sought a declaratory judgment that it had the right to send AOL members unsolicited e-mail advertisements.[174] AOL argued that there is no right to send millions of e-mail messages each day to AOL subscribers free of charge, resulting in the overload of AOL's e-mail servers and complaints from AOL members.[175] Cyber Promotions argued that although AOL is not a government entity, its conduct had the character of state action by virtue of its public network for discourse, conversations, and commercial transactions.[176] The court held that although it opened its e-mail to the public, it did not do so by performing any municipal power or essential public service and did not "stand in the shoes of the State."[177] Cyber Promotions also argued that AOL's e-mail constitutes an exclusive public function because there is no alternative avenue of communication for Cyber Promotions to send its e-mail to AOL members.[178] The court proposed several alternative routes, including posting advertisements on the World Wide Web, mail through the United States Postal Service, telemarketing, television advertising, newspapers, magazines, and passing

---

167. *Id.* at 1266.
168. *Id.*
169. *Id.* at 1267.
170. *Id.* at 1269.
171. *Id.*
172. *Id.*
173. Cyber Promotions, Inc. v. Am. Online, Inc. 948 F.Supp. 436 (E.D. Pa. 1996).
174. *Id.* at 438.
175. *Id.*
176. *Id.* at 442.
177. *Id.*
178. *Id.* at 442–43.

out leaflets and finally concluded that AOL was not a state actor.[179] Because AOL was not a state actor, Cyber Promotions had no right under the First Amendment to send unsolicited e-mail to AOL's members and AOL could block any attempts by Cyber Promotions to do so.[180] This decision indicates that as private actors, service providers may adopt whatever viable means they find to block spam without running afoul of the First Amendment.

2. Government Actors

In order for state actors to regulate speech, an important state interest must be articulated. One interest that has been cited in regulating commercial speech is cost-shifting. In e-mail advertising, the advertiser is able to shift the cost from the advertiser to the consumer.[181] Advertisers can send one message or a million for the same cost.[182] In contrast, spam now costs service providers an estimated $500 million in the United States and Europe because of the need for additional bandwidth, technical support, and servers.[183] The service providers pass the cost on to consumers at the rate of $2–3 per month.[184]

In 1995, the Ninth Circuit Court of Appeals held that cost-shifting was an interest sufficient to ban unsolicited faxes.[185] In *Destination Ventures*, a company that sent advertisements by facsimile ran afoul of the Telephone Consumer Protection Act of 1991 ("TCPA"). The TCPA bans unsolicited faxes that contain advertisements.[186] Destination Ventures asserted that the TCPA violated the First Amendment and sought declaratory and injunctive relief.[187] Destination Ventures argued that the government could not single out advertisements for regulation when other unsolicited faxes produce the same cost-shifting.[188] The court held that because Congress's goal was to prevent cost-shifting of advertising costs, regulating faxes containing advertising was justified.[189] The ban applied to any organization and was a reasonable means to achieve the goal, thus satisfying the First Amendment requirements.[190] Some anti-spam legislation used the TCPA as a model, comparing the cost-shifting used by spammers to that of advertisement faxes. Using cost-shifting as justification for banning spam could pass constitutional muster.[191]

---

179. *Id.* at 443–44.
180. *Id.* at 445.
181. Gary Miller, *How to Can Spam*, 2 VAND. J. ENT. L. & PRAC. 127, 127 (2000).
182. *Id.* at 128.
183. Olsen, *supra* note 68.
184. Klett & Brightwell, *supra* note 14, at 11.
185. Destination Ventures, Ltd. v. Fed. Communications Comm'n, 46 F.3d 54 (9th Cir. 1995).
186. *Id.* at 55. 47 U.S.C. § 227(b)(1)(C) (2003).
187. *Destination Ventures*, 46 F.3d at 55.
188. *Id.* at 56.
189. *Id.*
190. *Id.*
191. Miller, *supra* note 181, at 128–29.

Recently, the Tenth Circuit examined the First Amendment implications of the "do-not-call" registry when telemarketing companies challenged FTC regulations.[192] In response to a mandate by Congress, the FTC created a national database as a method of preventing unwanted telemarketing calls.[193] In doing so, the FTC exempted charitable and political organizations from the do-not-call requirements.[194] The court examined the FTC regulations and the level of protection afforded commercial speech.[195] It reviewed the level of protection that commercial speech receives under the three-part test set out in *Central Hudson*.[196]

First, the government must assert a substantial interest that the regulation will achieve.[197] The government asserted interests in protecting the privacy of individuals in their homes and protecting consumers against abusive and fraudulent solicitation.[198] The court accepted these as substantial governmental interests.[199] Second, the regulation must directly advance that governmental interest.[200] Telemarketers asserted that the registry is unconstitutional because it does not apply to charitable and political callers, but the First Amendment does not require the government to regulate all aspects of a problem.[201] "[S]o long as a commercial speech regulation materially furthers its objectives, underinclusiveness is not fatal."[202] The court found that the national do-not-call list directly advances the goals of reducing intrusions into personal privacy and the risk of telemarketing fraud and abuse.[203] The court noted that with 50 million telephone numbers registered, the do-not-call list prevents telemarketer calls that would total approximately 6.85 billion per year.[204] The court also noted the list prohibits a significant number of all calls and the type of calls that Congress determined to be most to blame for the problems the regulation seeks to redress.[205]

Finally, the regulation must be narrowly tailored so that it does not restrict more speech than necessary to achieve its purpose.[206] The court held that the do-not-call list is narrowly tailored because it does not regulate more protected speech than necessary—only calls targeted at unwilling recipients.[207] It prohibits calls aimed at consumers who affirmatively indicated they do not want to receive

---

192. Mainstream Mktg. Serv. v. Fed. Trade Comm'n, 358 F.3d 1228 (10th Cir. 2004).
193. *Id.* at 1233–34.
194. *Id.* at 1238.
195. *Id.* at 1239.
196. Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n, 447 U.S. 557 (1980).
197. *Mainstream Mktg.*, 358 F.3d at 1237.
198. *Id.*
199. *Id.*
200. *Id.* at 1238.
201. *Id.*
202. *Id.* at 1239.
203. *Id.* at 1240.
204. *Id.*
205. *Id.*
206. *Id.* at 1242.
207. *Id.*

calls, thus protecting them from an invasion of privacy.[208] The court compared the do-not-call list to the do-not-mail list examined by the Supreme Court in *Rowan v. United States Post Office*, and decided that the list merely "permits a citizen to erect a wall…that no advertiser may penetrate without his acquiescence."[209] The court also noted that the list only restricts one avenue of communication and does not prevent the use of other media.[210] The court concluded that the do-not-call list is consistent with First Amendment protection of commercial speech.[211]

Regulating spam combines the important government interest noted in *Destination Ventures* of preventing cost-shifting from advertisers to consumers with the important government interests of preventing fraud and invasions of privacy noted in *Mainstream Marketing*. With ISPs passing the cost of spam onto consumers at the rate of $2–3 per month and the fraudulent or deceptive spam at sixty-six percent of all commercial e-mail, these important interests are easily demonstrated.[212] As long as regulations are narrowly tailored and advance the government's goal, spam laws should stand up to First Amendment challenges.

C. Out-of-State Spammers and Personal Jurisdiction Problems

Some courts have examined the issue of whether states may properly obtain jurisdiction over those who violate anti-spam statutes, since many would-be defendants reside outside the state or outside the United States.[213] Although these statutes have not been tested outside the United States, recent case law supports the conclusion that states can reach offenders in other states.

1. Long-Arm Jurisdiction and Out-of-State Spammers

Internet Doorway, an ISP, brought a tort suit against a non-resident sender of e-mail that advertised pornographic web sites.[214] Connie Davis, a Texas resident, sent e-mail to people all over the world, including Mississippi residents, with a falsified header that made the e-mail appear to have been sent from an Internet Doorway account.[215] Internet Doorway asserted claims for violations of the Lanham Act[216] and trespass to chattels.[217] Davis moved to be dismissed from the action due to a lack of personal jurisdiction.[218] The court examined two requirements for personal jurisdiction—the state's long arm statute must be satisfied and the exercise of personal jurisdiction must not offend traditional

---

208. *Id.*
209. *Id.* (quoting Rowan v. United States Post Office Dep't, 397 U.S. 728, 738 (1970)).
210. *Id.* at 1243.
211. *Id.* at 1245.
212. Klett & Brightwell, *supra* note 14, at 11; *FTC Study Finds Deception in 66 Percent of Spam*, *supra* note 17, at 34.
213. Amaditz, *supra* note 70, at 52.
214. Internet Doorway, Inc. v. Parks, 138 F.Supp.2d 773, 774 (S.D. Miss. 2001).
215. *Id.*
216. 15 U.S.C. § 1125 (2003).
217. *Internet Doorway*, 138 F.Supp.2d at 774.
218. *Id.*

notions of fair play and substantial justice.[219] Under the Mississippi long arm statute, a court may exercise personal jurisdiction over a defendant who: 1) makes a contract with a state resident to be performed in the state, 2) commits a tort in whole or in part in the state, or 3) does business or performs work or service in the state.[220] The court found that Davis committed a purposeful act that occurred in Mississippi, just as if she had sent a letter to a Mississippi resident via U.S. Mail advertising a product or service.[221] As such, Davis was doing business within the contemplation of the Mississippi long arm statute.[222]

Under the tort prong of the long arm statute, the tort was complete when the recipient opened it, not when Davis transmitted it.[223] Because the injury took place in Mississippi, the underlying tort claim can be seen to take place, in part, in Mississippi.[224] In addition, the court found that exercise of personal jurisdiction would not violate Davis' due process rights.[225] Under the court's analysis, a single contact can satisfy the minimum contact requirement, and the burden then shifts to the defendant to prove that jurisdiction would be unfair, which she failed to do.[226] Davis manipulated the e-mail to show that it was being sent from an Internet Doorway account, then sent e-mails to people all over the country and the world; therefore, Davis had to be aware that the e-mail would be received and opened in numerous fora, including Mississippi.[227] Accordingly, the court found that by "sending an e-mail solicitation to the far reaches of the earth for pecuniary gain, one does so at her own peril, and cannot then claim that it is not reasonably foreseeable that she will be haled into court in a distant jurisdiction."[228]

A Virginia court also considered the issue of personal jurisdiction in *Verizon Online Services, Inc. v. Ralsky*.[229] Verizon, an ISP, brought an action against defendants based on their transmission of spam through its network, which operates seven servers in Virginia.[230] Verizon alleged the transmissions overwhelmed its servers causing delays in processing e-mail and provoking consumer complaints.[231] The defendants, Michigan residents, transmitted millions of unsolicited bulk e-mails addressed to Verizon subscribers through the Verizon computer network advertising goods and services, including credit repair tools, new car buying services, diet pills, computer programs, and online gambling.[232] The defendants used non-existent e-mail user names and domain names in the "to" line, employed false registration information to obtain e-mail addresses, used false

---

219. *Id.* at 775.
220. *Id.*
221. *Id.* at 776.
222. *Id.*
223. *Id.* at 777.
224. *Id.*
225. *Id.* at 779.
226. *Id.*
227. *Id.*
228. *Id.*
229. 203 F.Supp.2d 601 (E.D. Va. 2002).
230. *Id.* at 604.
231. *Id.*
232. *Id.* at 607.

information in the "from" line, sent e-mail from accounts obtained through false registration or hacking into third party accounts, relayed spam through third party servers, used false information to obtain web sites connected to the hypertext in their spam messages, and falsely claimed that the links found in their messages were used for opting-out when they were actually used to confirm addresses for further spamming.[233]

The defendants sought dismissal based on a lack of personal jurisdiction, but the court found sufficient minimum contacts to satisfy due process.[234] The court examined personal jurisdiction in a two-step inquiry—whether the Virginia long arm statute is satisfied and whether the long arm statute's reach complies with due process requirements.[235] The court found that it could exercise personal jurisdiction over a defendant that causes a tortious injury in Virginia if: 1) he regularly does or solicits business; 2) he engages in any other persistent course of conduct; or 3) he derives substantial revenue from goods used or consumed, or services rendered, in Virginia.[236] The court found that using Verizon's e-mail servers caused injury in Virginia and that the defendants' purposeful, persistent, commercial conduct satisfied the long arm statute.[237]

The court then addressed due process, asking whether haling the defendants into a Virginia court would "offend traditional notions of fair play and substantial justice."[238] The defendants claimed they did not purposefully avail themselves of the laws and privileges of Virginia because they did not knowingly target Virginia residents.[239] However, the court rejected that argument because the defendants sent millions of e-mails to solicit business at no cost to them, while causing a tort where the recipients are located. Therefore, they should have reasonably expected to be haled into court in any state where they caused injury.[240] Moreover, the court stated that finding a lack of jurisdiction would allow spammers to send bulk messages "with impunity, avoiding personal jurisdiction simply by alleging they did not know the exact location of an ISP's e-mail servers, yet knowing full well their conduct harmed those computers and the ISP's business. Fundamental fairness does not favor that result and neither does the Due Process Clause of the Constitution."[241]

2. Long-Arm Jurisdiction and International Spammers

The Arizona Supreme Court decision in *Uberti v. Leonardo* may be used as an example of extending personal jurisdiction to defendants overseas.[242] *Uberti*

---

233. *Id.* at 608
234. *Id.* at 604.
235. *Id.* at 609–10.
236. *Id.* at 610.
237. *Id.* at 611.
238. *Id.*
239. *Id.* at 612.
240. *Id.*
241. *Id.* at 620.
242. 892 P.2d 1354 (Ariz. 1995). Arizona exerts personal jurisdiction to the maximum extent allowed by the federal constitution. *Id.* at 1358; *see also* Edias Software v. Basis Int'l, 947 F.Supp. 413, 416 (1996).

involved a product liability action brought against an Italian corporation that manufactures handguns.[243] The court examined whether the defendant met minimum contacts with the state and whether it would be reasonable to exercise jurisdiction over a company located in Italy.[244] The court found that the defendant knowingly and intentionally manufactured its products for sale in the United States.[245] The guns were designed for the western United States and knowingly marketed to that area through a distributor.[246]

The defendant argued that he focused on the United States in general and not specifically on Arizona.[247] However, the court noted that if a company could avoid jurisdiction under that argument, no individual state could assert jurisdiction solely because the defendant did not target a particular state.[248] The defendant also argued that it did not know the extent of its distributor's sales efforts.[249] The court answered that because the defendant did not make itself aware of or restrict the sales effort, it could not use lack of knowledge as a defense.[250] The court concluded that minimum contacts were met, and that because Arizona has a strong interest in protecting its citizens from defective products, because the witness and the accident scene were in Arizona, and because of the progress in international communication and transportation, it would not be unreasonable to try the case in Arizona.[251]

Although spam does not cause the potentially lethal harm of defective handguns, courts may apply the same reasoning to find personal jurisdiction over spammers, especially those who commit harm, such as fraud. Because spammers send out messages, targeted not to one specific state but throughout the United States, it would be unjust to allow them to escape liability because they target consumers generally rather than consumers in just one state. The company that hires spammers, like the gun company that hired distributors, may find itself liable even though it does not know the extent of the spammer's sales efforts. As long as the spammer causes harm within the United States, a court should be willing to try the case in the state where the harm occurred.

As demonstrated above, courts seem quite willing to find personal jurisdiction when spammers send millions of messages to unknown destinations in an effort to obtain customers, as long as the plaintiff can demonstrate harm, either in tort law or violations of anti-spam law. Personal jurisdiction requirements vary depending on the requirements of individual states, so other states may not follow the cases mentioned above. However, the sheer quantity of messages sent make it reasonable for a spammer to know that it is likely that a message will reach a

---

243. *Uberti*, 892 P.2d at 1356.
244. *Id.* at 1358
245. *Id.* at 1360.
246. *Id.* at 1362.
247. *Id.*
248. *Id.*
249. *Id.*
250. *Id.* at 1363.
251. *Id.* at 1364.

resident of an anti-spam state, thus satisfying the general requirement under the U.S. Constitution of fundamental fairness.

D. Arizona's Anti-Spam Law

Ten years after giving birth to spam, Arizona unanimously voted to regulate it.[252] The resulting statute prohibits falsifying transmission information or other routing information.[253] It also forbids false or misleading information in the subject line, and using a third party's Internet address or domain name without their consent.[254] The statute requires the use of "adv:" as the first four characters in the subject line of unsolicited commercial electronic mail.[255] It also mandates the use of an opt-out procedure for recipients and restricts the sale or transfer of a recipient's e-mail address to another person or organization for the purpose of sending commercial e-mail.[256] The statute applies to any person doing business in Arizona and any person who transmits e-mail in the following method: 1) from a computer located in Arizona; or 2) to an address the sender knows or has reason to know is held by an Arizona resident; or 3) to a computer service with equipment or its principal place of business in Arizona.[257] The statute allows damages of $10 for each unsolicited e-mail or $25,000, whichever is less, plus costs and attorney fees, and does not provide liability against service providers.[258] An injured service provider may recover attorney fees, costs, and the greater of $10 per e-mail or $25,000.[259]

Like the spam statutes enacted by other states, the Arizona statute would certainly have been challenged under the dormant commerce clause, the first amendment, and the requirements of personal jurisdiction. But before that could happen, the United States passed the CAN-SPAM Act, which preempted state laws regulating spam.

V. THE CAN-SPAM ACT

Once states began regulating spam, a growing consensus emerged in favor of federal legislation.[260] Although several bills were proposed, the federal government failed to enact legislation to address the problems of spam until very recently. The proposals before the House of Representatives last year included: the Criminal Spam Act of 2003,[261] the Wireless Telephone Spam Protection Act,[262] the

---

252. The Arizona House of Representatives unanimously passed S.B. 1280 on April 3, 2003. *House Unanimously Passes Spam Protection*, *supra* note 25.

253. ARIZ. REV. STAT. § 44-1372.01(A)(1) (2003).

254. § 44-1372.01(A)(2)–(3).

255. § 44-1372.01(B)(1).

256. § 44-1372.01(B)(2).

257. § 44-1372.01(E).

258. § 44-1372.02(A)–(C) (2003).

259. § 44-1372.02(D).

260. Amaditz, *supra* note 70, at 20.

261. S. 1293, 108th Cong. (2003) (criminalizing the sending of predatory and abusive e-mail).

262. H.R. 122, 108th Cong. (2003) (prohibiting the use of wireless telephone systems to transmit unsolicited commercial messages).

REDUCE Spam Act,[263] the SPAM Act,[264] the RID Spam Act,[265] and the Anti-Spam Act of 2003.[266] Because none of these measures were adopted, it is difficult to say how effective they would have been in deterring spam, but they do illustrate a variety of approaches.

The bill that did become law is the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, or the CAN-SPAM Act.[267] CAN-SPAM regulates commercial e-mail, any e-mail whose primary purpose is to commercially advertise or promote a commercial product or service.[268] It requires that commercial e-mail contain opt-out provisions, including clear and conspicuous notice that the recipient may decline to receive future e-mails from the sender and a valid e-mail address for the sender.[269] After a recipient opts out, transmission of additional commercial e-mail is prohibited.[270] The law prohibits false or misleading transmission information and deceptive subject headings.[271] Using prohibited spamming techniques to promote a business is not allowed even if the business uses a third party spammer to send e-mail on its behalf.[272] A party who did not commit an offense may still have violated the statute if they own more than half of the entity that committed the violation or had actual knowledge of the violation and received an economic benefit from the violation.[273] Certain violations may be subject to treble damages, increasing the maximum of $2,000,000 to $6,000,000.[274] These aggravated violations include address harvesting, automated creation of multiple e-mail accounts, and relay through a computer or computer network without authorization.[275] The FTC, states or the federal government, and ISPs may enforce CAN-SPAM provisions.[276] The FTC is also charged with

263. Restrict and Eliminate the Delivery of Unsolicited Commercial Electronic Mail or Spam Act of 2003, H.R. 1933, 108th Cong. (2003) (reducing unsolicited commercial electronic mail and protecting children from sexually oriented advertisements).

264. Stop Pornography and Abusive Marketing Act, S. 1231, 108th Cong. (2003) (prohibiting transmission of unsolicited commercial electronic mail to persons who place their e-mail address on a national No-Spam Registry and imposing requirements on content to prevent fraud and deception).

265. Reduction in Distribution of Spam Act of 2003, H.R. 2214, 108th Cong. (2003) (requiring identification as advertisement and opt-out instructions).

266. H.R. 2515, 108th Cong. (2003) (requiring identification as advertisement and opt-out instructions).

267. This bill was passed by the Senate on November 25, 2003, and the House of Representatives on December 8, 2003. The President signed the bill on December 16, 2003, and it went into effect on January 1, 2004. 15 U.S.C. §§ 7701–7713 (2004).

268. 15 U.S.C. § 7702(2).

269. 15 U.S.C. § 7704(a)(3)(A).

270. § 7704(a)(4).

271. § 7704(a)(1) & (2).

272. 15 U.S.C. § 7705(a).

273. § 7705(b).

274. 15 U.S.C. § 7706(f)(3)(C).

275. 15 U.S.C. § 7704(b).

276. 15 U.S.C. § 7706.

investigating and implementing a Do-Not-E-Mail Registry.[277] Perhaps most importantly, state anti-spam statutes are superceded by CAN-SPAM.[278]

Although the legislation has been in effect for only two months, it has already been heavily criticized. First, it is likely CAN-SPAM will be challenged under the First Amendment. Unlike regulation by a private actor, like America Online,[279] CAN-SPAM constitutes government restriction on commercial speech. Similar to the do-not-call registry examined in *Mainstream Marketing*,[280] CAN-SPAM is regulation of commercial speech. The government must demonstrate a substantial interest in regulating the speech, it must prove that the restrictions imposed will directly advance its interest, and it must prove that the regulation is narrowly tailored so that it does not regulate more speech than necessary.[281] The government has a strong interest in preventing invasion of consumer privacy, fraud and cost-shifting. Regulating commercial e-mail by requiring marketers to provide opt-out provisions and to honor opt-out requests prevents both invasion of privacy and cost-shifting. Since it is estimated that two-thirds of spam contains false information, requiring truthful information, subject headings, and return addresses is narrowly tailored to address the government's interest in preventing fraud.[282]

The second complaint about CAN-SPAM is that it preempts state laws, some of which had more stringent requirements and heavier penalties. CAN-SPAM does not preempt state laws concerning fraud or computer crimes, but it does preempt laws regulating e-mail.[283] It preempted a Virginia statute that went into effect in July 2003 that made it a felony to send bulk e-mails that disguise their origins or return addresses.[284] On December 11, 2003, Virginia brought its first felony indictment against two alleged spammers who face possible penalties of five years in prison and fines of $2500 each.[285] The prospect of a felony conviction and a prison sentence could have proven more of a deterrent than CAN-SPAM's monetary damages. By going into effect on January 1, 2004, CAN-SPAM also preempted California's opt-in statute, set to become effective the same day. California's opt-in statute prohibited sending e-mail to recipients who have not

---

277. 15 U.S.C. § 7708.

278. 15 U.S.C. § 7707(b) §; s*ee also* Am. Bar. Ass'n, *Overview of the CAN-SPAM Act*, BULL. L ./SCI. & TECH., Jan. 2004, at 1; Mintz, Levin, Cohn, Ferris, Glovsky & Popeo, P.C., *CAN-SPAM Act of 2003 Signed into Law by President Bush: Sets First "National Standards" for Commercial E-Mail*, CLIENT ALERT, Dec. 22, 2003, *at* http://www.mintz.com/images/dyn/publications/BFAlert122203.pdf; Baker & McKenzie, *U.S. CAN-SPAM Act Imposes New Federal Requirements on Corporate E-Mail Marketing*, N. AM. PRIVACY, Jan. 2004, *at* http://www.bmck.com/ecommerce/can-spam-act-memo.pdf.

279. *See* Cyber Promotions, Inc. v. Am. Online, Inc. 948 F.Supp. 436 (E.D. Pa. 1996); *supra* notes 173–180 and accompanying text.

280. Mainstream Mktg. Serv. v. Fed. Trade Comm'n, 358 F.3d 1228 (10th Cir. 2004), discussed *supra* notes 192–211 and accompanying text; Anita Ramasastry, *Why the New Federal "CAN Spam" Law Probably Won't Work*, FINDLAW'S WRIT, Dec. 3, 2003, *at* http://writ.news.findlaw.com/scripts/printer_friendly.pl?page=/ramasastry/20031203.html.

281. *Mainstream Mktg.*, 358 F.3d at 1237.

282. *FTC Study Finds Deception in 66 Percent of Spam*, *supra* note 17, at 34.

283. 15 U.S.C. § 7707(b) (2004).

284. Rubell, *supra* note 75.

285. *Id.*

given their express consent or do not have a preexisting business relationship with the sender.[286] It also applies to the sender of the e-mail as well as the business whose products are the subject of the e-mail.[287] The statute allows the spam recipient, as well as the attorney general and ISPs to bring suit for damages, up to $1 million per incident, plus attorney fees and costs.[288] By preempting the California statute, CAN-SPAM disempowered thirty-four million potential enforcers of anti-spam legislation.[289] Companies in California that were going to lose business due to the requirements of the opt-in statute have now been legitimized and look forward to prospering under CAN-SPAM. [290] CAN-SPAM now makes spamming legal as long as companies follow its guidelines.[291]

Another problem with CAN-SPAM is that it is an opt-out statute. In efforts to curb spam, recipients have been warned not to opt-out because spammers use opt-out responses to validate e-mail addresses, making an address the target of even more spam.[292] Will consumers trust that the statute makes opt-out valid, and will enough businesses honor opt-out rather than use the information to send more spam? Also, spam is often transmitted from or through countries that have not yet enacted anti-spam legislation, such as Russia and China.[293] Since CAN-SPAM has been enacted, no decrease in spam has been detected,[294] and AOL reports that there has been a ten percent shift in spam origins to overseas internet addresses.[295] It is unlikely that CAN-SPAM will have any effect on these foreign transmissions other than to encourage more spammers to move overseas. Another concern with opt-out is its inconsistency with regulation of spam by other countries, such as the European Union, that have adopted opt-in regimes. An international, unified approach to curb spam would arguably be more effective than a patchwork of different solutions.

Finally, CAN-SPAM removes spam regulation from the states to the federal government before a clear consensus could be reached on the most effective solution. States play a role as "many laboratories" to discover the best solution to a problem when each adopts its own legislation or declines to legislate at all. As Justice Brandeis stated, "It is one of the happy incidents of the federal system that a single courageous state may, if its citizens choose, serve as a laboratory; and try novel social and economic experiments without risk to the rest

---

286. CAL. BUS. & PROF. CODE § 17529.2 (West 2003).

287. *Id.*

288. CAL. BUS. & PROF. CODE § 17529.8 (West 2003).

289. Dan Lee, *Little Hope Seen for Spam Relief; New Federal Law Not Stopping Flood of Bulk E-Mail*, SAN JOSE MERCURY NEWS, Jan. 24, 2004, at 1.

290. Carrie Kirby, *Anti-Spam Law May Benefit Some E-Marketers / Local Companies Pleased It Goes After Mailers Who Disguise Identity*, S.F. CHRON., Jan. 2, 2004, at B1.

291. *Id.*

292. Rubell, *supra* note 75.

293. *Id.*

294. Anick Jesdanum, *Filtering Firms Say Anti-Spam Law Ineffective*, ARIZ. DAILY STAR, Jan. 12, 2004, at A1. In fact, a spam-filtering company, Brightmail, noted that in the week after the law took effect, fifty-eight percent of incoming email was spam. *Id.*

295. *Tech News Roundup*, SAN JOSE MERCURY NEWS, Jan. 8, 2004, at 2.

of the country."[296] In 2003, new approaches were proposed, such as opt-in and empowering spam recipients to sue spammers in California[297] and felony sentences in Virginia.[298] Some states passed legislation so recently they had not yet pursued enforcement.[299] There has not been enough litigation for courts to review and determine which approaches meet constitutional muster and which ones fail. That a wide variety of bills were proposed in 2003 demonstrates that although everyone recognizes that spam is a problem, not everyone agrees which solution is best.

VI. CONCLUSION

With the number of e-mails per day up to almost fifty per user, and the cost of dealing with spam at $18 billion per year worldwide,[300] it is easy to see how Congress was motivated to put an end to this scourge of the Internet. However, in joining other nations attempting to regulate e-mail and eliminate spam, the United States may have jumped on the bandwagon too soon. Instead of taking advantage of its many laboratories and choosing an effective solution that has shown it can withstand constitutional challenges, Congress instead chose CAN-SPAM. In the next few years, CAN-SPAM will demonstrate whether it is effective legislation that can renew the Internet as an efficient communication medium. A key element is whether Congress will provide funds to the FTC for enforcement. However, if it does not prove effective, what will replace it that is up to the challenge?

If CAN-SPAM is ineffective and the states have been preempted, the solution, other than another federal attempt, may lie in technology. Less than a month after CAN-SPAM went into effect, Bill Gates announced that his company, Microsoft Corporation, could eradicate spam within two years.[301] Microsoft is investigating ways for users to charge senders a fee before accepting messages, a way of charging Internet "postage."[302] It is also studying "challenge-response" technology where senders get an automatic response from recipients asking for verification that the sender is a real person.[303] Challenge-response has already been adopted by some ISPs such as Earthlink and Mailblocks, but being adopted by Microsoft's MSN and Hotmail services, with more than 100 million users, could have a much bigger effect in removing the profitability from bulk e-mailing.[304]

Spam is an effective marketing tool because a sender can mail a million messages for the same cost as one. If the marketplace alters so that sending a million messages costs a million times more than sending one message, spam loses

---

296. New State Ice Co. v. Liebmann, 285 U.S. 262, 311 (1932) (Brandeis, J., dissenting).

297. CAL. BUS. & PROF. CODE § 17529.8 (West 2003).

298. VA. CODE ANN. § 18.2-152.3:1B (Michie 2003).

299. *See, e.g.*, ARIZ. REV. STAT. § 44-1372.01 (2003), discussed *supra* at IV.D.

300. Craig Spann, *Tougher Laws to Restrict Junk E-Mail*, COURIER MAIL, Apr. 17, 2003, at 9.

301. Jonathan Krim, *Gates Wants to Give E-Mail Users Anti-Spam Weapons*, WASH. POST, Jan. 27, 2004, at E1.

302. *Id.*

303. *Id.*

304. *Id.*

its profitability when one consumer in ten thousand responds. If routing mechanisms change to require sender verification, instead of sending a million messages at a touch of a button, the spammer will be forced to hold legitimate e-mail accounts in order to receive and take the time to respond to each challenge before the message will get to a consumer. Clearly, to get rid of annoying spam, the answer is to make it a money-losing scheme. Myriad solutions exist; we just need to have the patience to discover which one works.