Kentucky Law Journal

Volume 94 | Issue 2 Article 5

2005

Has Spam been Fried? Why the CAN-SPAM Act of 2003 Can't: Regulation of Unsolicited Commercial Electronic Mail and the CAN-SPAM Act of 2003

John W. Daniel
University of Kentucky

Has Spam been Fried? Why the CAN-SPAM Act of 2003 Can't: Regulation of Unsolicited Commercial Electronic Mail and the CAN-SPAM Act of 2003

John W. Daniel [1]

I. Introduction

The CAN-SPAM Act (Controlling the Assault of Non-Solicited Pornography and Marketing Act) of 2003[2] is the first federal legislative attempt to regulate unsolicited commercial e-mail (UCE), also known as spam.[3] Since its enactment, the Act has been overshadowed by criticisms of its ineffectiveness.[4] Critics argue that the Act is ill-equipped to provide the necessary tools to trace and physically locate spammers, and that, even when the spammers are found, the Act fails to provide courts with personal jurisdiction over them.[5] While critics of the CAN-SPAM Act are quick to identify these problems, there have been relatively few proponents of the Act. This Note attempts to fill this void by, first, illustrating how the CAN-SPAM Act creates an effective foundation in the war on spam as it works in conjunction with other federal legislation regulating commercial communications and current case law and by, second, identifying future approaches that Congress and courts may take in combating UCE.

1 J.D. expected 2006, University of Kentucky. I would like to thank my parents, John and Shelia Daniel, for their continued support and encouragement.

2 Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act of 2003, 15 U.S.C.S. §§ 7701–13 (2005).

3 This article treats spam and UCE synonymously. *See generally* David E. Sorkin, *Technical and Legal Approaches to Unsolicited Electronic Mail*, 35 U.S.F. L. Rev. 325 (2001) (analyzing the differences between spam, UCE, and junk mail).

4 *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 (2004); Sameh I. Mobarek, Student Article, *The CAN-SPAM Act of 2003: Was Congress Actually Trying to Solve the Problem or Add to it?*, 16 Loy. Consumer L. Rev. 247 (2004); Lily Zhang, Note, *The CAN-SPAM Act: An Insufficient Response to the Growing Spam Problem*, 20 Berkeley Tech. L.J. 301 (2005).

5 *See* Ledbetter, *supra* note 4, at 115; Amy G. Marino, *Is Spam the Rock of Sisyphus?: Whether the CAN-SPAM Act and Its Global Counterparts Will Delete Your E-mail*, 32 Pepp. L. Rev. 1021, 1035 (2005).

This Note addresses two flaws of the CAN-SPAM Act and provides some indication of how courts might actually be able to overcome these apparent problems of the Act by applying traditional legal theories to Internet law and by identifying potential steps Congress should take to make the Act more effective. Part II provides the historical framework of spam by detailing the numerous problems it has caused which prompted the need for federal legislation.[6] Part III reviews specific causes of action that plaintiffs have used to sue spammers based on separate sources: common law, state legislation, and federal legislation under the CAN-SPAM Act.[7] Part IV addresses the first main hindrance to enforcing the Act: the difficulty of physically locating spammers.[8] Part V provides a potential solution to the second difficulty of obtaining personal jurisdiction over spammers for the U.S. courts to obtain personal jurisdiction by comparing spammers and website operators and analogizing the reasoning that has allowed courts to obtain personal jurisdiction over website operators.[9] Finally, Part VI details how the CAN-SPAM Act has, despite the two most publicized criticisms, been used in lawsuits against spammers.[10]

II. WHY SPAM TASTES SO BAD

Although there is no definitive explanation of how the term "spam" became synonymous with UCE, most literature cites a 1970 Monty Python skit wherein "the word 'spam' is repeated to the point of absurdity in a restaurant menu."[11] Others assert that the term *spam* describes the image of putting SPAM® (the processed meat) into a fan and scattering useless pieces everywhere.[12] Some have reasoned that the term derives from an

6 *See infra* notes 10–24 and accompanying text.

7 *See infra* notes 25–73 and accompanying text.

8 *See infra* notes 74–129 and accompanying text.

9 *See infra* notes 133–198 and accompanying text.

10 *See infra* notes 199–215 and accompanying text.

11 CompuServe Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1018 n.1 (S.D. Ohio 1997); *see also* MARCIA S. SMITH, CRS REPORT FOR CONGRESS: "JUNK E-MAIL": AN OVERVIEW OF ISSUES AND LEGISLATION CONCERNING UNSOLICITED COMMERCIAL ELECTRONIC MAIL ("SPAM"), (April 15, 2003), http://www.usembassy.fi/pdfiles/RS20037.pdf ("It all started in early Internet chat rooms and interactive fantasy games where someone repeating the same sentence or comment was said to be making a 'spam.' The 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."); Dianne Plunkett Latham, *Spam Remedies*, 27 WM. MITCHELL L. REV. 1649, 1649 n.1 (2001) (tracing the reference to spam to an episode of *Monty Python's Flying Circus*).

12 Todd H. Flaming, *The Rules of Cyberspace: Informal Law in a New Jurisdiction*, 85 ILL. B.J. 174, 176 n.30 (1997).

analogy of the lack of functional value of UCE (or "junk mail") to the reputation of SPAM® as lacking nutritional value.[13]

With approximately 140 million Americans, i.e. half of the United States, regularly using e-mail,[14] spam has become much more than just a source of aggravation to Internet consumers and businesses alike. The volume of spam has exponentially increased year after year "threatening to overwhelm not only the average consumer's in-box, but also the network systems of ISPs, businesses, universities, and other organizations."[15] Spam slows down the Internet's delivery speed and costs consumers time and money since web users must pay for the extra time spent online deleting unwanted UCE.[16] The increase in spam has only exacerbated this problem. For example, "e-mail security firm MX Logic reports that spam accounted for 80 percent of all e-mail in 2004, up from 62 percent in 2003."[17] Aside from the annoyance of deleting spam, most spam is false. In April 2003, the Federal Trade Commission (FTC) reported that a study found that sixty-six percent of the spam analyzed contained some kind of fraudulent or misleading information either in the e-mail's routing information, the subject line, or the body of the message.[18]

Initially, internet service providers (ISPs) bear the burden of the increase in spam by needing to update anti-spam software and suffering the consequences of a slower network as they are forced to devote more resources to blocking the increasingly large amount of spam. The United States' largest ISP, America Online, reported in May 2003 that it blocked

13 Robert Craig Waters, *An Internet Primer: (Part II)*, 44 FED. LAW. 72, 72 (March/April 1997).

14 S. REP. NO. 108-102, at 2 (2003), *as reprinted in* 2004 U.S.C.C.A.N. 2348, 2349.

15 *Id.* at 2–3. In September 2001, Internet analysts estimated that spam accounted for only eight percent of all e-mail. As of April 2002, the estimate rose to eighteen percent, and by the end of 2003 over half of all e-mail was expected to be unsolicited commercial e-mail. *Id.* at 2–3. MX Logic, an anti-spam vendor and research group, "found 67 percent of all e-mail to be spam in February" 2004, and by November 2004 the group reported that "75 percent of all e-mail was spam...." Grant Gross, *Is CAN-SPAM Working?: One year after it went into effect, many say the nation's antispam law is ineffective*, PC WORLD, Dec. 28, 2004, *available at* http://www.pcworld.com/news/article/0,aid,119058,00.asp.

16 *See* Derek D. Simmons, *No Seconds on Spam: A Legislative Prescription to Harness Unsolicited Commercial E-mail*, 3 J. SMALL & EMERGING BUS. L. 389, 393 (1999).

17 Tom Spring, *2005 Inbox Forecast: Despite better technology and tougher laws, expect to keep fingering that Delete key next year*, PC WORLD, Dec. 20, 2004, *available at* http://www.pcworld.com/news/article/0,aid,118985,00.asp.

18 FEDERAL TRADE COMMISSION, FALSE CLAIMS IN SPAM: A REPORT BY THE FTC'S DIVISION OF MARKETING PRACTICES 10 (2003), *available at* http://www.ftc.gov/reports/spam/030429spamreport.pdf. The FTC also grouped spam based on categories and prevalence with four categories comprising over half of all spam: investment or get-rich-quick "opportunities" (20 percent); pornographic websites or adult-oriented material (18 percent); credit card or financial offers (17 percent); and health products and services (10 percent). *Id.* at 2.

2.4 billion spam messages per day, approximately eighty percent of its daily inbound e-mails.[19]

While ISPs front the costs of combating spam by paying for advanced spam-filtering technology, creating extra e-mail storage for customer in-boxes, and increasing network bandwidth,[20] these costs are eventually funneled to the end consumer.[21] Some experts estimate that spam costs individual Internet consumers worldwide $9.4 billion each year.[22] It has been estimated that United States businesses lose between $10 billion to $13 billion per year due to spam, mostly from lost productivity, network system upgrades, unrecoverable data, and increased personnel costs.[23] Some authorities predict that spam will cost companies as much as $198 billion by 2007,[24] emphasizing the need for improved regulation.

III. ATTEMPTS AT FRYING SPAM

Initially, plaintiffs used common law causes of action to bring claims against spammers[25] such as trespass on chattels,[26] breach of contract,[27] and even

19 S. REP. No. 108-102, at 2–3. The second largest e-mail provider, Microsoft, "reported ... that its MSN mail and Hotmail services combined block up to 2.4 billion spam messages each day. Earthlink, the third largest ISP in the United States, reported a 500 percent increase in inbound spam over the past 18 months." *Id.* at 3.

20 *See* Tom Spring, *Spam Weapons of Tomorrow: Internet firms turn to technology, not law, to fight the avalanche of spam*, PC WORLD, Mar. 1, 2004, *available at* http://www.pcworld.com/news/article/0,aid,114995,00.asp.

21 *See id.* ISP Bellsouth's director of project management estimated that spam costs a provider three dollars per in-box per year. *See also* S. REP. No. 108-102, at 6 (noting that "*USA Today* reported in April [2003] that research organizations estimate that fighting spam adds an average of $2 per month to an individual's Internet bill").

22 S. REP. No. 108-102, at 6.

23 *See* Press Release, MX Logic, MX Logic Finds That Only 3 Percent of Unsolicited Commercial Email Complies with CAN-SPAM Law (Fed. 10, 2004), http://www.mxlogic.com/news_events/press_releases/02_10_04_CAN-SPAM.html.

24 *See* Bob Sullivan, *Spam Wars—How Unwanted Email is Burying the Internet*, Aug. 6, 2003 http://www.spamsolutions.net/1059.asp (citing a study by the Radicati Group).

25 *See* Latham, *supra* note 11, at 1651.

26 *See generally* Marjorie A. Shields, Annotation, *Applicability of Common-Law Trespass Actions to Electronic Communications*, 107 A.L.R.5th 549 (2003–04); CompuServe Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015 (S.D. Ohio 1997) (plaintiff ISP seeking a cease-and-desist order to stop the defendant from using its network to send unsolicited e-mail advertisements to plaintiff's customers). *But see*, Adam Mossoff, *Spam—Oy, What a Nuisance!*, 19 BERKELEY TECH L.J. 625, 640–41 (2004) (citing Intel Corp. v. Hamidi, 71 P.3d 296 (Cal. 2003) for the proposition that the cause of action for trespass on chattels as used against spammers has reached its zenith).

27 *See* Monique C.M. Leahy & Sonya M. Duchak, *Cause of Action for Breach of Contract and Related Causes of Action Against Bulk E-Mail Sender for Damages Due to "Spamming"*, 13 CAUSES OF ACTION 2D 597 (2005); *see also*, Hotmail Corp v. Van Money Pie Inc., 47 U.S.P.Q.2d (BNA)

nuisance.[28] Plaintiffs then began using state and federal statutes directed at other forms of electronic communications and analogized UCE to these forms.[29] State legislatures were the first to statutorily respond to the spam problem in various ways such as providing individuals with a cause of action directly targeting UCE.[30] Congress then followed by enacting the CAN-SPAM Act of 2003.

A. State and Federal Legislation

Clever plaintiffs used several statutes as the basis for causes of action including false designation of origin,[31] dilution of interest in service marks under the Latham Act,[32] and violations of the Computer Fraud and Abuse Act[33] by exceeding authorized access and impairing computer facilities.[34]

Thirty-eight states have enacted statutes directly targeting spam.[35] To protect individual consumers, the statutes have used a variety of techniques for regulating UCE[36] such as requiring "ADV:" to be the first four characters of the subject line[37] to signal to recipients that the e-mail is an advertisement, prohibiting "false or misleading information in the subject line,"[38] providing mechanisms whereby a person may opt not to receive

---

1020 (N.D. Cal. 1998) (holding that evidence would likely show that defendant breached e-mail service agreement by using plaintiff's e-mail services to facilitate sending spam).

28 *See* Mossoff, *supra* note 26, at 646–58 (explaining why a spam cause of action could rely on nuisance claim).

29 *See infra* notes 31–35 and accompanying text.

30 *See infra* notes 35–41 and accompanying text.

31 *See* 15 U.S.C. § 1125(a)(1) (2000); *see also* America Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444, 449 (E.D. Va. 1998) (noting that "[t]he unauthorized sending of bulk e-mails has been held to constitute a violation of the Lanham Act").

32 15 U.S.C. § 1125(c)(1) (2000); *see also America Online, Inc.*, 46 F. Supp. 2d at 449–50 (plaintiff claimed dilution of mark because of "association with defendants' bulk e-mail practices").

33 18 U.S.C. § 1030 (2000).

34 *See America Online, Inc.*, 46 F. Supp. 2d at 450–51 (holding defendant's unauthorized spamming to be a violation of the Computer Fraud and Abuse Act, 18 U.S.C. §§ 1030(a)(2)(C), (5)(C), by intentionally accessing a computer without authorization resulting in damage to plaintiff's computer network).

35 *See generally* DAVID E. SORKIN, SPAM LAWS: UNITED STATES: STATE LAWS: SUMMARY (2005) http://www.spamlaws.com/state/summary.html (summarizing state anti-spam statutes); Scot M. Graydon, *Much Ado About Spam: Unsolicited Advertising, the Internet, and You*, 32 ST. MARY'S L.J. 77, 98–106 (2000) (discussing the various ways state statutes have attempted to regulate spam).

36 *See* Graydon, *supra* note 35, at 98–106.

37 *See* CAL. BUS. & PROF. CODE § 17538.4(g) (West 1996) (repealed 2003); COLO. REV. STAT. ANN § 6-2.5-103(4) (West 2004); TENN. CODE ANN. § 47-18-2501(e) (2005).

38 815 ILL. COMP. STAT. ANN. 511/10(a)(ii) (West 2005); WASH. REV. CODE § 19.190.020(1)(b) (2000); W. VA. CODE ANN. § 46A-6G-2(2) (LexisNexis 1999).

spam,[39] and, perhaps the most liberal and consumer-friendly provision, imposing violations for spammers who send UCE to state residents.[40]

As cases against spammers filtered through the judicial system, the wide variation among requirements of different states and the nature of e-mail being capable of dissemination across numerous state borders created complex issues regarding compliance with states' statutes. Furthermore, courts were confronted with issues regarding whether the court could exercise personal jurisdiction over nonresident-defendant spammers, such as when an Internet user in one state attempted to bring suit against a spammer located in another state.[41] It quickly became apparent that effective regulation of UCE would require broad jurisdiction that only federal legislation could provide.[42]

Before the CAN-SPAM Act, the federal government had enacted legislation regarding other types of unsolicited commercial communications. For example, the Telephone Consumer Protection Act of 1991 (TCPA) regulated commercial telephone and fax solicitations.[43] The TCPA specifically targeted the use of the telephone and fax machines[44] for unsolicited commercial communications, but some plaintiffs have used the TCPA to attack UCE as well.[45] The TCPA not only provides plaintiffs with a cause of action, but it also provides precedent for upholding Congress's authority to regulate commercial speech, including UCE,[46] by providing the rationale as to why Congressional legislation of electronic communication passes constitutional scrutiny.[47]

In *Destination Ventures, Ltd. v. FCC*,[48] the plaintiffs alleged that the TCPA unconstitutionally restricted commercial speech in violation of the First

39 *See* Graydon, *supra* note 35, at 114.

40 CAL. BUS. & PROF. CODE § 17529.2 (West 1996).

41 *See, e.g.*, Beyond Systems, Inc. v. Realtime Gaming Holding Co., 878 A.2d 567 (Md. 2005) (holding that defendants who had sent spam to business e-mail addresses were not subject to general or specific jurisdiction in Maryland).

42 *See* Graydon, *supra* note 35, at 105.

43 47 U.S.C. § 227(b) (2000) (prohibiting the use of autodialers and prerecorded messages).

44 *See* § 227(b)(1)(C) (prohibiting an advertiser from using "any telephone facsimile machine, computer, or other device to send, to a telephone facsimile machine, an unsolicited advertisement").

45 *See* John Magee, *The Law Regulating Unsolicited Commercial E-Mail: An International Perspective*, 19 SANTA CLARA COMPUTER & HIGH TECH L.J. 333, 347 (2003) (referencing *Destination Ventures* as the case that paved the way for "expansive interpretation of the act to include [UCE]").

46 *See* Gary S. Moorefield, Note, *Spam—It's Just Not For Breakfast Anymore: Federal Legislation and the Fight to Free the Internet from Unsolicited Commercial E-mail*, 5 B.U. J. SCI. & TECH. L. 10 para. 24 (1999).

47 Magee, *supra* note 45, at 347 .

48 Destination Ventures, Ltd. v. FCC, 46 F.3d 54 (9th Cir. 1995).

Amendment.[49] The U.S. Court of Appeals for the Ninth Circuit ruled that the Act was constitutional, finding that the banning of unsolicited advertising through facsimiles met the government's interest in preventing the shifting of advertising costs to consumers.[50]

While many scholars have discussed the imminent constitutional challenges which the CAN-SPAM Act will face in the upcoming years[51] based on the First Amendment protection of freedom of speech,[52]the CAN-SPAM Act will most likely be upheld as a constitutional exercise of Congressional authority under the reasoning in *Destination Ventures* and the similarities between the TCPA and the CAN-SPAM Act. As the infiltration of the Internet and the use of e-mail continue to increase, advertisers capitalize by using the relatively cheap method of sending out large amounts of e-mail to promote their products. Thus, the CAN-SPAM Act will be held to be constitutional because the government's interest in preventing spammers from shifting the costs of advertising to Internet users[53] is just as strong as its interest in preventing advertisers from shifting costs to fax recipients.[54]

Attempts at federal regulation directly targeting UCE is not new. Although over twenty-five bills have been proposed in recent years, the CAN-SPAM Act is the only bill that passed through Congress.[55]

49 *Id.* at 55–56.

50 *Id.*

51 *See generally* Marc Simon, *The CAN-SPAM Act of 2003: Is Congressional Regulation of Unsolicited Commercial E-mail Constitutional?*, 4 J. HIGH TECH. L. 85 (2004) (predicting that the CAN-SPAM Act will be held constitutional against a First Amendment challenge).

52 *See generally* Elizabeth A. Alongi, Note, *Has the U.S. Canned Spam?*, 46 ARIZ. L. REV. 263, 287 (2004) (surmising that the CAN-SPAM Act will be upheld if challenged under the First Amendment on commercial free speech grounds because the government has an interest in preventing fraud and it is narrowly tailored to address that interest).

53 *See supra* notes 14–24 and accompanying text (explaining the extensive costs associated with spam passed on to consumers and businesses alike and that these costs led Congress to enact the CAN-SPAM Act).

54 *See Destination Ventures, Ltd.*, 46 F.3d at 56.

55 *See* DAVID E. SORKIN, SUMMARY OF PROPOSED FEDERAL SPAM LEGISLATION (2005), http://www.spamlaws.com/federal/index.html (detailing over twenty-five bills that were introduced into Congress from 1999–2004 but were not enacted). Congressional proposals in 2003 included: Criminal Spam Act of 2003, S. 1293, 108th Cong. (2003) (criminalizing the sending of predatory and abusive e-mail); Wireless Telephone Spam Protection Act, H.R. 122, 108th Cong. (2003) (prohibiting the use of wireless telephone systems to transmit unsolicited commercial messages); REDUCE Spam Act (Restrict and Eliminate the Delivery of Unsolicited Commercial Electronic Mail or Spam Act) of 2003, H.R. 1933, 108th Cong. (2003) (criminalizing sending UCE with false or misleading header information); SPAM Act (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); Reduction in Distribution of Spam Act of 2003, H.R. 2214, 108th Cong. (2003) (requiring identification for advertisements and opt-out instructions); Anti-Spam Act of 2003, H.R. 2515, 108th Cong. (2003) (requiring identification of advertisements and opt-out instructions).The

B. The CAN-SPAM Act of 2003

The CAN-SPAM Act places several prohibitions and requirements on senders of UCE. For example, the Act prohibits the use of materially false or misleading header information,[56] deceptive subject headings,[57] and failure to contain a functioning return e-mail address.[58] Unless the recipient has given affirmative consent to receipt of the message, the e-mail message itself must provide clear and conspicuous identification that the message is an advertisement, clear and conspicuous opportunity to "opt-out" by declining to receive further commercial e-mail messages, and a valid physical postal address.[59]

The Act provides several mechanisms for enforcement[60] including a cause of action for a state attorney general to seek to up to $2 million in damages.[61] While the Act does bestow some federal agencies with the authority to assert a cause of action,[62] it noticeably excludes private individuals from bringing suits under CAN-SPAM.[63] Criminal penalties under the Act are available under 18 U.S.C. § 1037.[64]

The CAN-SPAM Act incorporates techniques developed by state statutes to create one federal law that preempts any *inconsistent* state law that "expressly regulates the use of electronic mail to send commercial messages."[65] The Act explicitly states that it does not preempt "State laws that are not specific to electronic mail, including State trespass, contract, or tort law; or other State laws to the extent that those laws relate to acts of fraud or computer crime."[66] Thus, the extent to which the CAN-SPAM Act actually preempts state law is unclear. For example, in August 2004, the Virginia attorney general indicted several defendants with felony violations of the

---

CAN-SPAM Act of 2003 was passed by the Senate on November 25, 2003, and the House of Representatives on December 8, 2003. President Bush signed the bill on December 16, 2003 with an effective date of January 1, 2004.

56 *See* 15 U.S.C.S § 7704(a)(1) (2005).

57 *See* § 7704(a)(2).

58 *See* § 7704(5)(a)(3)(A).

59 *See* § 7704(a)(5).

60 *See infra* notes 130–198 and accompanying text.

61 *See* 15 U.S.C.S. § 7706(f).

62 *See* § 7706(b).

63 The Act does not expressly prohibit actions by e-mail consumers; however, it does expressly authorize a cause of action for ISPs. *See* § 7706(g).

64 *See* 15 U.S.C.S. § 7703(b)(1) (approving the U.S. Sentencing Commission's amendment of sentencing guidelines to provide appropriate penalties for violations of 18 U.S.C. § 1037, which addresses criminal sanctions for sending large quantities of unsolicited electronic mail). *Contra* Arminda B. Bepko, Note, *A State-By-State Comparison of Spam Laws*, 13 MEDIA L. & POL'Y 20, 53 (2004) (stating that the CAN-SPAM Act does not contain criminal provisions).

65 15 U.S.C.S. § 7707(b)(1) (2005).

66 § 7707(b)(2). *See also* Bepko, *supra* note 64, at 50; *infra* notes 197–215.

Virginia statute governing the transmission of UCE without any reference to the federal CAN-SPAM Act.[67]

Enforcing the CAN-SPAM Act is delegated to three main entities: the Federal Trade Commission (FTC), state attorneys general, and ISPs.[68] The FTC has the primary responsibility of enforcing the CAN-SPAM Act.[69] Congress deemed violation of the Act an unfair or deceptive Act or practice,[70] and the FTC is given the "same means, and with the same jurisdiction, powers, and duties as though all applicable terms and provisions of the FTC Act were incorporated and made a part of [the CAN-SPAM Act]."[71] State attorneys general also are granted standing to seek remedies against spammers who violate the Act.[72] ISPs may bring suits when a spammer transmits unlawful UCE over the ISP's facilities or violates the Act by harvesting e-mail addresses from a website or online service operated by the ISP.[73]

IV. Addressing Why the CAN-SPAM Act Can't "Can the Spam"

Although the CAN-SPAM Act went into effect on January 1, 2004,[74] MX Logic, an e-mail–security firm, measured CAN-SPAM compliance each

67 *See* Commonwealth v. Jaynes, 65 Va. Cir. 355, 371 (Va. Cir. Ct. 2004) (denying a motion to dismiss predicated on constitutional challenges to the Virginia statute regulating UCE, Va. Code Ann. § 18.2–152.3:1 (2004)). The court's order acknowledged the CAN-SPAM Act, stating that "the Virginia statute can be harmonized with ... the [CAN-SPAM Act]." *Jaynes*, 65 Va. Cir. at 369–70.

68 *See* 15 U.S.C.S. § 7706 (2005).

69 *See* § 7706(a)-(c). Subsection (a) grants enforcement jurisdiction to the Federal Trade Commission if the violation is deemed an unfair or deceptive Act or practice by the Commission under the Federal Trade Commission Act, 15 U.S.C. § 57a(a)(1)(B) (2000) (permitting the FTC to "prescribe rules which define ... acts or practices which are unfair or deceptive"). Subsections (b) and (c) provide several agencies with enforcement capabilities subject to jurisdictional and authority limitations provided by their own statutory grants: the Office of the Comptroller of the Currency, the Federal Reserve Board, the Federal Deposit Insurance Corporation, the Office of Thrift Supervision, the Department of Transportation, the Department of Agriculture, the Farm Credit Administration, the National Credit Union Administration, the Securities and Exchange Commission, and the Federal Communications Commission.

70 § 7706(a). Under the Act, offenses are treated as though they are violations of an FTC Trade Regulation Rule promulgated under Section 18(a)(1)(B) of the Federal Trade Commission Act. 15 U.S.C. § 57a(a)(1)(B).

71 S. Rep. No. 108-102, at 20 (2003), *as reprinted in* 2004 U.S.C.C.A.N. 2348, 2349.

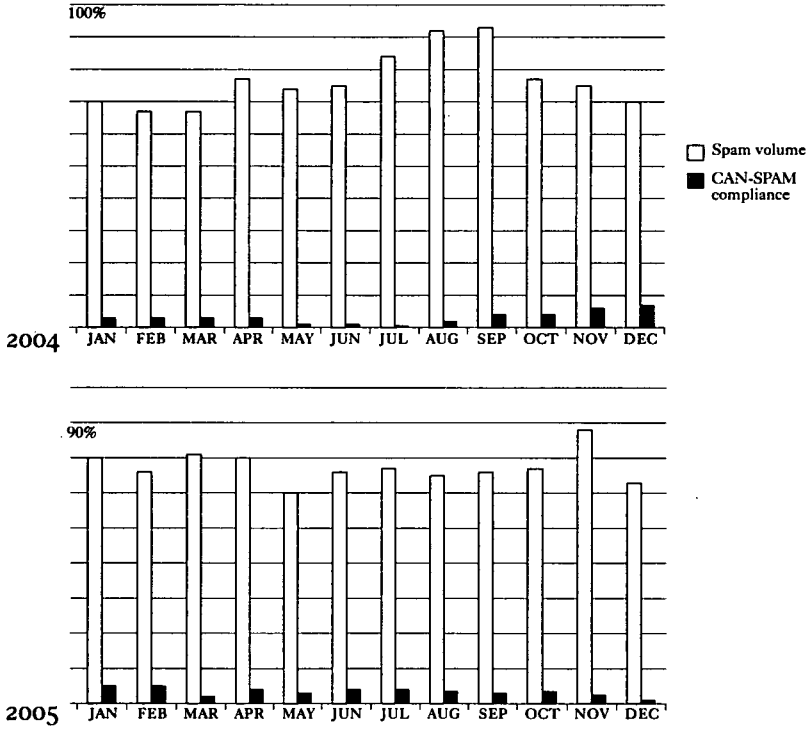
72 § 7706(f)(1).

73 S. Rep. No. 108-102, at 21.

74 CAN-SPAM Act of 2003, Pub. L. No. 108–187, § 16, 117 Stat. 2699, 2718. The portion of the Act providing for the "Do Not E-mail Registry" however did not go into effect on

month since the law went into effect by examining a random sample of 10,000 UCEs each week and found that ninety-seven percent of UCEs failed to comply with the Act.[75] "During 2004, monthly compliance ranged from a low of 0.54 percent in July to a high of 7 percent in December."[76]

FIGURE I
CAN-SPAM COMPLIANCE, 2004–2005



SOURCE: *E-mail traffic through the MX Logic Threat Center. Courtesy MX Logic Inc.*

January 1, 2004. *Id.*

75 *See* Press Release, MX Logic, Inc., On One-Year Anniversary of CAN-SPAM Act, MX Logic Reports 97 Percent of 2004 Spam Failed to Comply with the Law; Spam, Other Email Threats Will Continue to Increase in 2005 (Jan. 3, 2005), http://www.webwire.com/ViewPressRel.asp?aId=869 (quoting MX Logic chief technology officer Scott Chasin as saying "While we applaud the intent of the CAN-SPAM Act, clearly it has had no meaningful impact on the unrelenting flow of spam that continues to clog the Internet and plague inboxes.... In fact, the overall volume of spam increased in 2004, and we fully anticipate continued growth in 2005.").

76 *Id.*

While there is no simple explanation for the continued lack of compliance, two of the reasons that have generated significant attention in the literature involve the Act's inability to track down spammers in cyberspace[77] and the fact that, even when the spammer's location can be determined, complex due process issues may hinder a court's ability to exercise personal jurisdiction.[78]

A. Catch Me If You Can

The first main problem with enforcing the CAN-SPAM Act is the inability to physically locate the spammer. If the CAN-SPAM Act has had any effect on spamming, it has only caused spammers to move their operations offshore or use open relays[79] thus appearing to have moved offshore. In fact, "[b]etween December 31[, 2003] and January 2[, 2004], AOL noticed a 10 percent jump in spam originating overseas,"[80] a clear indication that some spammers took the CAN-SPAM Act seriously enough to "move" their operations outside of the United States. Therefore, one of the most pressing obstacles to overcome in the effort to decrease spam is the need to enhance the technological and legal capabilities so that authorities may trace UCE to its source.

Between eighty to ninety percent of all spam sent worldwide is untraceable to its actual source.[81] Of the spam which does claim to come from a certain area of the world as determined from the message's header information[82] (which can be dubious itself), the majority of spam appears to be sent through e-mail servers located outside the United States[83] which further

77 *See* Latham, *supra* note 11, at 1651.

78 *See* Kenneth C. Amaditz, *Canning "Spam" in Virginia: Model Legislation to Control Junk E-Mail*, 4 VA. J.L. & TECH. 4, ¶ 52 (1999), *available at* http://vjolt.student.virginia.edu/graphics/vol4/home_art4.html.

79 *See infra* notes 94–98 and accompanying text.

80 Tom Spring, *Why Spammers Love the CAN-SPAM Law: Antispam laws make some spamming legal and do little to quell the onslaught*, PC WORLD, Jan. 19, 2004, *available at* http://www.pcworld.com/news/article/0,aid,114363,00.asp.

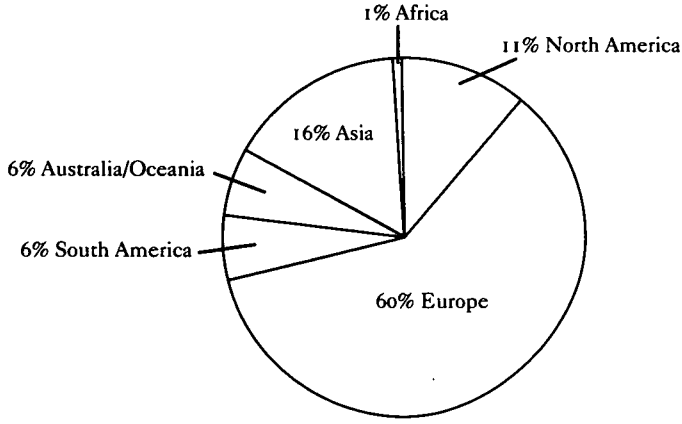
81 Brightmail president Enrique Salem stated in written testimony before the U.S. Senate Committee on Commerce, Science and Transportation that ninety percent of the e-mail it analyzed was untraceable. *See Hearing on Unsolicited Commercial Email Before the S. Comm. on Commerce, Science and Transportation*, 108th Cong. 6 (2003) (written statement by Enrique Salem, president, Brightmail, Inc.), *available at* http://commerce.senate.gov/pdf/salem052103.pdf.

82 Header information is defined as "the source, destination, and routing information attached to an electronic mail message, including the originating domain name and originating electronic mail address, and any other information that appears in the line identifying, or purporting to identify, a person initiating the message." 15 U.S.C.S. § 7702(8) (2005).

83 *See Hearing on Unsolicited Commercial Email Before the S. Comm. on Commerce, Science and Transportation*, 108th Cong. 6 (2003) (written statement by Enrique Salem, president, Brightmail, Inc.), *available at* http://commerce.senate.gov/pdf/salem052103.pdf.

complicates the jurisdictional problems. As the diagram below illustrates, Brightmail,[84] an electronic-communications security firm, found that sixty percent of spam comes from e-mail addresses assigned to Europe (including ten to twelve percent from Russia), and sixteen percent originates in Asia. Although North America receives over half of all spam sent each day, only eleven percent is directly traceable to North America.[85]

FIGURE 2
WHERE SPAM PURPORTS TO ORIGINATE



SOURCE: *http://commerce.senate.gov/pdf/salem052103/pdf*

In September 2004, the FTC submitted the report "A CAN-SPAM Informant Reward System: A Report to Congress," as required by the CAN-SPAM Act,[86] outlining two potential avenues for tracing spammers: the "electronic trail" and the "money trail."[87] Tracing the electronic trail is

84 "Brightmail analyzes data it collects from its 'probe network', more than a million continually monitored e-mail addresses seeded in ISPs around the world. These e-mail addresses never send out e-mail and have never been used in e-commerce, but still attract 300–350 million e-mail messages per month, 100 percent of which can be classified as 'unsolicited'." S. Rep. No. 108–102, at 1 n.2.

85 *See Hearing on Unsolicited Commercial Email Before the S. Comm. on Commerce, Science and Transportation*, 108th Cong. 6 (2003) (written statement by Enrique Salem, President, Brightmail, Inc.), *available at* http://commerce.senate.gov/pdf/salem052103.pdf.

86 *See* 15 U.S.C.S. § 7709 (2005). SEP

87 FEDERAL TRADE COMMISSION, A CAN-SPAM INFORMANT REWARD SYSTEM: A REPORT TO CONGRESS 11 (2004), *available at* http://www.ftc.gov/reports/rewardsys/040916rewardsysrpt.pdf [hereinafter *CAN-SPAM Informant Reward System*].

typically less fruitful than the money trail because of the numerous ways that spammers are able to disguise the true origin of their messages.[88]

1. *Technological Evasion: Tools of a Spammer.*—Spammers have a wide array of technological methods to evade those seeking to trace their e-mails: spoofing, open relays, hijacking servers, and zombie and bot networks.[89]

Spoofing, or "forged spamming," involves providing false e-mail header information so that an e-mail "appear[s] to come from an address other than the one from which it actually came."[90] Any undeliverable messages return to the person whose address was spoofed rather than to the spammer, which causes its own problems.[91] A variation of spoofing occurs when a spammer references a prestigious domain name in the subject line or text of the message in hopes that the recipient will believe that the sender is a reputable business and give more attention to the e-mail.[92] A third form of spoofing involves routing an e-mail through an unsuspecting ISP to create an electronic trail so that the ISP appears to be involved in sending the message.[93]

An open relay is "an unprotected, or 'unsecured,' email server that is configured to accept and transfer email on behalf of any user anywhere, including unrelated third parties."[94]

> If a spammer sends junk e-mail directly, network managers can trace back the connection and deal with the problem. If, instead, the spammer relays the mail, they may be able to obscure their identity. Even if the spammer can't hide completely, they will deflect a significant portion of the complaints away from themselves and towards the administrators of the hijacked host.[95]

88 *See generally* Latham, *supra* note 11, at 1655–1657 (detailing a technical explanation of the complexities of tracing the source of e-mail and why it is so difficult to trace the source of spam).

89 *See CAN-SPAM Informant Reward System*, *supra* note 87, at 12–13.

90 *Id.* at 12.

91 *Id.* "Not only can a spammer send out millions of spoofed messages, but any bounced messages—messages returned as undeliverable—will flow to the person whose address was spoofed rather than to the spammer. As a result, an innocent e-mail user's inbox may become flooded with angry, reactive e-mail, and the innocent user's Internet service may be shut off due to the volume of the complaints." *Id.*

92 *See* Latham, *supra* note 11, at 1650.

93 Verified Complaint at 6, Earthlink, Inc. v. John Does 1–25 and John Does 26–50, No. 04–CV 3142 (N.D. Ga. filed Oct. 27, 2004), *available at* http://www.earthlink.net/about/press/spamlawsuit.pdf.

94 *CAN-SPAM Informant Reward System*, *supra* note 87, at 12.

95 MAIL ABUSE PREVENTION SYSTEM LLC (MAPS), WHAT IS THIRD–PARTY MAIL RELAY? 2 (2001), http://security.ucdavis.edu/ mail_relay.pdf. [hereinafter MAIL ABUSE PREVENTION SYSTEM].

Intentionally misconfigured e-mail servers complicate tracing e-mail to its original sender.[96] The server is open in that it allows incoming messages, originally sent from anywhere, to be relayed through the server to the desired recipient and in the process, the true origin of the e-mail is disguised.[97] For example, a spammer located in the United States is able to use an open relay that is located in any other country to make the spam appear as if it originated in that other country.[98]

Spammers may also "hijack" a server in a practice known as domain-name hijacking, which allows massive amounts of mail to be relayed through an unsuspecting server and causes spam to appear to have originated from the hijacked server.[99] Hijacking allows the spammer to "launder their junk e-mail through third-party relays to enable them to slip through the spam filters" because even the spam filters see the spam as being from a reputable server because of the domain name used in the "from" address.[100]

Spammers may also use devices known as worms or viruses to convert an open or compromised proxy server into a "zombie drone."[101] A zombie drone is a computer that is infected with software, which causes the computer to spew out spam or serve as a relay or proxy for spam, completely unknown to the computer's owner.[102] When numerous zombie drones are controlled by the same spammer, it creates a bot-network, which may have as many as 400,000 drones.[103] When each drone in the network is instructed to generate or relay spam, the aggregate spam-generation rate can be immense.[104] Technology experts expect the number of zombie bot-networks

96 *See CAN-SPAM Informant Reward System*, *supra* note 87, at 12.

97 *See* MAIL ABUSE PREVENTION SYSTEM, *supra* note 95, at 2.

> Spammers use relays to increase the number of messages they can spew. A lowly PC sitting at the end of a phone line can only pump out a limited number of messages. If, however, the spammer can grab a hold of a high-powered mail host, then they can push through hundreds of times more junk mail. Further, if the spammer can relay through several mail servers in parallel, they can flood the net with extraordinary amounts of junk mail.

Id.

98 *See CAN-SPAM Informant Reward System*, *supra* note 87, at 12.

99 Latham, *supra* note 11, at 1650.

100 *Id.*

101 David Bender, *Data Protection: Three "Hot Topics"*, *in* INSTITUTE FOR INTELLECTUAL PROPERTY LAW (PLI'S TENTH ANNUAL), at 48 (PLI Copyrights, Trademarks, and Literary Property Course Handbook Series No. 2909, 2004).

102 *Id.* at 47–48.

103 *See* DAN BONEH, DIFFICULTIES OF TRACING SPAM EMAIL 5 (Sept. 9, 2004), http://www.ftc.gov/reports/rewardsys/expertrpt_ boneh.pdf [hereinafter Boneh Report].

104 *See id.* at 5–6. For more information regarding bot networks and zombie drones that promulgate spam, see Jeff Gelles, *Next big step in thwarting spammers; FTC's next big step to fight spammers*, PHILA. INQUIRER, June 16, 2004, at C1; Saul Hansell, *Spammers Can Run But They Can't Hide*, N.Y. TIMES, Nov. 9, 2003, at C1; Frank Hayes, *ISPs' Spam Fight*, COMPUTERWORLD,

to increase, "providing the infrastructure for a significant increase in the volume of spam that can be distributed."[105] Zombie drones and bot-networks are an increasingly favored method of spamming.[106] An MX Logic report in April 2004 estimated that thirty to fifty percent of spam came through zombie drones; by November and December 2004, that amount had increased to sixty-nine percent.[107]

Finally, spammers may use untraceable Internet connections that cannot be linked to an individual or physical location, such as Internet users who connect "through free (or stolen) wireless connections."[108] In addition, certain universities have on-campus networks which do not require users to identify themselves before logging on, thus allowing users to send e-mail anonymously.[109] Spammers "may also purchase ISP roaming access using false names and untraceable payment methods."[110]

2. *Tracing the Money Trail.*—As an alternative to the electronic trail, the FTC may attempt to trace the money trail to find who is financially benefiting from the spam.[111] For example, a novice spammer may register his e-mail address under his real name and address. Even if the name and address of an e-mail account holder may be false, the account holder's IP address and payment records may provide useful investigative leads.[112]

However, investigating the money trail is especially hindered by privacy limitations regulating the kinds of evidence that may be obtained.[113] For example, the FTC "cannot compel information about the volume of email sent from an email account or copies of complaints an ISP has received about the email account holder."[114] Compelling copies of e-mail in the spammer's e-mail account is difficult because of various court decisions interpreting the Electronic Communications Privacy Act (ECPA).[115]

Mar. 15, 2004, http://computerworld.com/managementtopics/management/helpdesk/story/0,10801,91182,00.html.

105 Press Release, MX Logic, Inc., On One-Year Anniversary of CAN-SPAM Act, MX Logic Reports 97 Percent of 2004 Spam Failed to Comply with the Law; Spam, Other Email Threats Will Continue to Increase in 2005 (Jan. 3, 2005), http://www.webwire.com/ViewPressRel.asp?aId=869 (noting that in the weeks prior to the press release "MX Logic discovered ... [that] as much as 69 percent of daily spam came from zombie PCs").

106 *Id.*

107 *Id. See* Gross, *supra* note 15.

108 Boneh Report, *supra* note 103, at 9.

109 *See id.*

110 *Id.*

111 *See CAN-SPAM Informant Reward System*, *supra* note 87, at 11.

112 *See id.* at 15.

113 *See id.*

114 *Id.* at 14 n. 27.

115 *See* Theofel v. Farey-Jones, 359 F.3d 1066 (9th Cir. 2004), *amending*, 341 F.3d 978 (9th Cir. 2003), *cert. denied*, 125 S. Ct. 48 (2004) (reversing dismissal of a claim under the ECPA

The ECPA[116] places several limits on the types of information that the FTC can obtain from electronic communications services and remote computing services such as ISPs.[117] During an investigation, the FTC "is often unable to obtain essential information about an investigative target's financial transactions from third parties, such as banks, credit card processors, and other payment processors."[118] Spammers also may use offshore processors and banks which can be beyond the reach of the FTC's compulsory process, making its job even more difficult.[119] Legislation before the Senate and House of Representatives would help the FTC reach offshore payment processors and banks in several ways, including by broadening reciprocal information sharing, expanding cross-border investigative cooperation, and providing for international agreements to accomplish these goals when necessary.[120]

The need for further action by Congress is evident. The numerous ways of avoiding detection illustrate that tracing either the electronic or money trail leads to many dead ends.

3. More Technological and Legal Advancements Are Needed to Address Evasion.—Numerous technological advancements have slightly eased the problem, but these advancements have led to temporary solutions because spammers are quite adaptable in their ability to circumvent advances in antispam technology.[121] One of the newest technologies developed by Microsoft, "smart" systems, takes into account the spammer's ability to continually develop new mechanisms to slip through filtering systems.[122] These systems learn from data and grow smarter over time, thereby confronting the ability of spammers to use new tactics to avoid filters.[123] Some U.S. senators have suggested charging Internet postage by taxing each piece of mail that is sent electronically.[124]

---

where defendants had improperly subpoenaed copies of plaintiffs' e-mail in separate litigation).

116 18 U.S.C. §§ 2702–2703 (2000).

117 *See* § 2703(c)(2). Under the ECPA, the Commission can use a civil investigative demand to find six types of information to a domain hosting an e-mail account that was used to send spam. *See also CAN-SPAM Informant Reward System*, *supra* note 87, at 14 n.27.

118 *CAN-SPAM Informant Reward System*, *supra* note 87, at 15.

119 *Id.* at 15 n.34.

120 *See* S. 1234, 108th Cong. (2004); H.R. 4996, 108th Cong. (2004).

121 *See generally* Sorkin, *supra* note 3, at 344–56 (discussing several technical advancements that can be implemented by Internet users and ISPs including filtering and blocking).

122 *See* Ledbetter, *supra* note 4, at 125.

123 *See id.*

124 *See* Grant Gross, *Will Taxing E-Mail Stop Spam?: Congress considers international treaty, tough laws, opt-out registries, and more*, PC WORLD, May 22, 2003, *available at* http://www.pcworld.com/news/article/0,aid,110837,00.asp. Senator Mark Dayton told the Senate Committee on Commerce, Science and Transportation that he thinks "it's worth looking at some very, very

The advancements have largely been focused on preventing spam from being delivered to the recipient or decreasing the overall levels of spam. These technologies and the CAN-SPAM Act lack any means to actually locate those people responsible for the spam. Legislators and developers of antispam technologies need to spend more resources on orchestrating a constitutionally permissible means of locating spammers such as a reduction in the barriers that hinder the FTC's investigations.

Even though the lack of legislation and technology is an obvious detriment to obtaining any type of judgment against a spammer, this has not inhibited lawsuits from going forward. For example, ISP EarthLink filed a complaint in March 2004 against seventy-five "John Does" which were split into five groups classified by the content of their spam: "Prescription Drug Spammers," "Mortgage Lead Spammers," "Cable Descrambler Spammers," "University Diploma Spammers," and "Get Rich Quick Spammers."[125]

In April 2004, the FTC announced the first CAN-SPAM cases against Phoenix Avatar and Global Web Promotions.[126] In March 2005, the U.S. District Court for the Northern District of Illinois approved a settlement between the FTC and Phoenix Avatar, fining the company $230,000 for sending millions of e-mail messages advertising their "bogus" diet patch.[127] Though Phoenix Avatar did not admit guilt, the FTC charged that Phoenix Avatar violated two sections of the CAN-SPAM Act (among other laws).[128] The court found that Phoenix Avatar sent commercial e-mail messages that contained materially false or misleading header information in violation of the CAN-SPAM Act, failed to provide clear and conspicuous notice of the opportunity to receive further commercial electronic mail messages from

small charge for every e-mail sent, so small that it would not be onerous for an individual or business that has regular (e-mail) use, but it would be a deterrent for those who are sending millions and even billions of these e-mails." *Id.*

125 Press Release, Microsoft, America Online, Earthlink, Microsoft and Yahoo! Team Up to File First Major Industry Lawsuits Under New Federal Anti-Spam Law (Mar. 10, 2004), http://www.microsoft.com/presspass/press/ 2004/mar04/03-10CANSPAMpr.asp.

126 *See* Press Release, Federal Trade Commission, FTC Announces First CAN-SPAM Act Cases (April 29, 2004), http://www.ftc.gov/opa/2004/04/040429canspam.htm. A copy of the criminal complaint against Phoenix Avatar is available at http://www.ftc.gov/os/2004/04/040429phhoenixavatarcriminalcmplt.pdf. A copy of the complaint against Global Web is available at http://www.ftc.gov/os/caselist/0423086/040428globalwebcomplaint.pdf.

127 *See* Press Release, Federal Trade Commission, Diet Patch Sellers Settle CAN-SPAM Charges (Mar. 31, 2005), http://www.ftc.gov/opa/2005/03/phoenix.htm. As part of the settlement, the fine was suspended, requiring Phoenix Avatar to only pay $20,000, provided that Phoenix Avatar complies with other provisions of the settlement, such as complying with the CAN-SPAM Act and failing to make false or misleading statements in their advertisements. *Id.*

128 *Id.*

the sender, and failed to include a valid physical postal address of the sender in violation of 15 U.S.C. Section 7704(a)(5)(A).[129]

V. Obtaining Personal Jurisdiction over the Spammer

Even when the physical location of the spammer is found, a second major obstacle in enforcing the CAN-SPAM Act is finding a court which is able to exercise personal jurisdiction over the defendant-spammer.[130] Because this issue is further complicated by the international aspects of the Internet, the scope of this Note is limited to a defendant-spammer found operating in the United States.[131]

It must be noted that personal jurisdiction is not a problem in all situations. A defendant is subject to suit in federal district court in the district in which the defendant resides.[132] Thus, the FTC or resourceful ISPs have little trouble in pursuing a defendant under the CAN-SPAM Act because these entities can pursue the defendant in his home state. However, the Act grants standing not only to the FTC and the large ISPs but also to any "provider of Internet access service adversely affected by a violation." This allows small ISPs to bring a civil action in any district court with jurisdiction over the defendant.[133] ISPs vary greatly in terms of size and financial capital; it seems logical that smaller ISPs may not have the financial resources to locate and bring suit against a defendant spammer in the state in which the defendant resides. Furthermore, it could be argued that smaller ISPs have more of an interest in pursuing spammers because smaller ISPs have more limited capabilities to deal with the negative consequences of spam.[134] The question becomes whether a district court, other than the court in the jurisdiction in which the defendant resides, may exercise personal jurisdiction

129 *See* Default Judgment and Order for Permanent Injunction and Monetary Relief as to Defendants Phoenix Avatar, LLC and DJL, LLC at 3–4, FTC v. Phoenix Avatar, LLC, No. 04C-2897 (N.D. Ill. Mar. 29, 2005), *available at* http://www.ftc.gov/os/caselist/0423084/050331defjudg0423084.pdf.

130 *See* Amaditz, *supra* note 78, ¶ 52.

131 Obtaining personal jurisdiction over a defendant spammer located outside the United States has not been addressed by domestic courts. Given the numerous ways that spammers are able to conceal their identities, it is apparent that any real effort at combating spam will take an international effort. There has been no attempt to apply the CAN-SPAM Act to international spammers. *Uberti v. Leonardo*, 892 P.2d 1354 (Ariz. 1995), provides an example of how a court might find personal jurisdiction over a spammer operating outside the United States. In determining that the court had personal jurisdiction over the international defendant, the court examined whether the defendant had minimum contacts with the state and whether it would be reasonable to exercise jurisdiction over a company located in Italy. *Id.* at 1358.

132 *See* 28 U.S.C. § 1391(b) (2000).

133 15 U.S.C.S. § 7706(g)(1) (2005).

134 *See supra*, Part II.

over the defendant because the defendant has sufficient contacts with the jurisdiction via the defendant's spamming activities.

Arguably, the CAN-SPAM Act caters to the large ISPs by effectively giving them a competitive advantage over smaller ISPs since the large ISPs are more likely to have the resources to bring suit against spammers in the jurisdiction where the spammer resides, whereas smaller ISPs are less likely to have the financial capabilities to sue in any jurisdiction. As an alternative, the small ISP may either attempt to bring suit in the jurisdiction in which the ISP resides or lobby the state attorney general to bring a civil action on behalf of the ISP in a U.S. district court of appropriate jurisdiction.[135]

An ISP or state attorney general may bring an action in any U.S. district court in which venue is proper under 28 U.S.C. § 1391.[136] Section 1391(b) is controlling because jurisdiction is based on a federal statute. It provides that a civil action may be brought in either

> (1) a judicial district where any defendant resides, if all defendants reside in the same State, (2) a judicial district in which a substantial part of the events or omissions giving rise to the claim occurred, or a substantial part of property that is the subject of the action is situated, or (3) a judicial district in which any defendant may be found, if there is no district in which the action may otherwise be brought.[137]

It is apparent that any of the persons given standing under the CAN-SPAM Act may file suit where the defendant spammer resides.[138] The issue then becomes determining how subpart (2) of Section 1391 affects the jurisdictional analysis: what is considered "a judicial district in which a substantial part of the events ... occurred"[139] when dealing with UCE.

In answering the question of whether the exercise of personal jurisdiction is appropriate over spammers, courts will either have to rely on traditional personal jurisdiction analysis or create a new analysis that is tailored to cyberspace or spamming in particular. Under the traditional framework of personal jurisdiction, a court may exercise jurisdiction over a nonresident defendant if either general or specific jurisdiction exists.[140] General jurisdiction may be found when a defendant has engaged in systematic and continuous activities in the forum state.[141] Specific jurisdiction reaches to the limit of due process.[142] This Note focuses on specific jurisdiction, which

135 *See* § 7706(f)(1).

136 § 7706(f)(7)(A).

137 28 U.S.C. § 1391(b) (2000).

138 *See supra* notes 134–41 and accompanying text.

139 § 1391(b)(2).

140 *See* Helicopteros Nacionales de Colom., S.A. v. Hall, 466 U.S. 408, 414 nn.8–9 (1984).

141 *See id.* at 414–16.

142 *See* David L. Stott, Comment, *Personal Jurisdiction in Cyberspace: The Constitutional*

may be used when general jurisdiction is inappropriate and the plaintiff's cause of action arose from the defendant's particular contact with the forum state.[143]

The authority to exercise personal jurisdiction is determined by a two-part test:[144] (1) whether a state's long-arm statute reaches the nonresident defendant[145] and (2) whether the court's exercise of personal jurisdiction is consistent with the Due Process Clause of the Fourteenth Amendment,[146] i.e., whether "the conduct satisfies the 'minimum contacts' requirement of the Due Process Clause of the Fourteenth Amendment."[147]

Courts have also applied this two-part test to determine whether a spammer-defendant's conduct is sufficient for the exercise of personal jurisdiction.[148]

This same test has been applied in the realm of UCE. For example, in *Internet Doorway, Inc. v. Parks*,[149] the district court examined whether it could exercise personal jurisdiction over a nonresident sender of UCE.[150] The court found that the "state's long arm statute must be satisfied and exercise of personal jurisdiction" must be consistent with due process.[151]

A. State Long-Arm Statutes

All states have long-arm statutes or court rules that provide courts with personal jurisdiction over nonresident defendants.[152] While the limits of those

Boundary of Minimum Contacts Limited to a Web Site, 15 J. MARSHALL J. COMPUTER & INFO. L. 819, 823 (1997). Limitations on the exercise of personal jurisdiction differ depending on whether the court seeks to exercise general or specific jurisdiction over a nonresident defendant. General jurisdiction arises from a defendant's substantial in–state contacts. As a result of these contacts, a court may exercise personal jurisdiction over any claim, even if the particular claim does not arise from the substantial contacts of the defendant with the forum state. *Id.* at n.17. However, "[s]pecific jurisdiction ... arises out of a single act by the defendant and is jurisdiction that extends to the limits of minimum contacts." *Id.* at n.18.

143 *Id.* at 823 n.18.

144 *See* Internet Doorway, Inc. v. Parks, 138 F. Supp. 2d 773, 775 (S.D. Miss. 2001).

145 *Id.*

146 *Id.*; *see also* Kulko v. Super. Ct., 436 U.S. 84, 91 (1978).

147 Ensign-Bickford Co. v. ICI Explosives USA Inc., 817 F. Supp. 1018, 1026 (D. Conn. 1993).

148 *See* Internet Doorway, Inc., 138 F. Supp. 2d at 774, 780 (denying defendants' motion to dismiss for lack of personal jurisdiction on claims of violation of the Latham Act and trespass to chattels).

149 *Id.* at 773 (plaintiffs sued based on the Latham Act and trespass to chattels).

150 *Id.* at 775.

151 Alongi, *supra* note 52, at 281. A Virginia court also examined the issue of personal jurisdiction in *Verizon Online Services, Inc. v. Ralsky*, 203 F. Supp. 2d 601 (E.D. Va. 2002) and found that the exercise of personal jurisdiction did not offend due process.

152 *See* Douglas D. McFarland, *Dictum Run Wild: How Long-Arm Statutes Extended to the Limits of Due Process*, 84 B.U. L. REV. 491, 496 (2004).

statutes may vary, over half of the states extend personal jurisdiction to any length that does not offend due process.[153]

In *Inset Systems, Inc. v. Instruction Set, Inc.*,[154] a Connecticut corporation sued a Massachusetts corporation in federal district court. Under the Connecticut long-arm statute[155] then in force, a foreign corporation was "subject to suit in this state ... if the corporation has repeatedly so solicited business, whether the orders or offers relating thereto were accepted within or without the state."[156] The court held that jurisdiction under the long-arm statute was satisfied based on the defendant's Internet advertisements.[157]

When spammers are not physically present in or a resident of the forum state, courts of the state may use the state's long-arm statute to exercise jurisdiction to the extent permitted by the statute and due process in order to reach out of state and compel a nonresident defendant to defend against a lawsuit.[158] When the state's long-arm statute is satisfied, the analysis turns to whether the exercise of personal jurisdiction is consistent with due process.

B. Due Process—Traditional Minimum Contacts and the Internet

In determining whether personal jurisdiction over a nonresident defendant is consistent with due process, the court must find three elements: "(1) the defendant must have sufficient 'minimum contacts' with the forum state, (2) the claim asserted against the defendant must arise out of those contacts, and (3) the exercise of jurisdiction must be reasonable."[159] In fulfilling these requirements, the Supreme Court has said that "it is essential in each case that there be some act by which the defendant purposefully avails itself of the privilege of conducting activities within the forum state, thus invoking the benefits and protections of its laws."[160] When these three ele-

153 *See id.* at 496–97 (noting that six states have long-arm statutes that extend to the boundaries of due process, thirteen states amended an "enumerated acts" statute so that the statute reaches to the limits of due process, and twelve states with "enumerated acts" statutes have had their statute declared to reach to the bounds of due process by their respective state courts).

154 Inset Sys., Inc. v. Instruction Set, Inc., 937 F. Supp. 161 (D. Conn. 1996).

155 CONN. GEN. STAT. § 33-411(c)(2) (repealed 1997).

156 CONN. GEN. STAT. § 33-411(c)(2) (repealed 1997).

157 *See Inset Sys., Inc.*, 937 F. Supp. at 164 (stating that "advertising via the Internet is solicitation of a sufficient repetitive nature to satisfy ... the Connecticut long-arm statute").

158 *See* Stott, *supra* note 142, at 823.

159 Zippo Mfg. Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119, 1122–23 (W.D. Pa. 1997).

160 Hanson v. Denckla, 357 U.S. 235, 253 (1958) (citing Int'l Shoe Co. v. Washington, 326 U.S. 310, 319 (1945)).

ments are satisfied, a court may exercise personal jurisdiction over a nonresident defendant.[161]

1. Nonresident defendant must have sufficient minimum contacts with the forum state.—The plaintiff in a civil suit must show how the defendant purposefully availed itself of the privilege of conducting its Internet activities in the forum state.[162] This question goes to "whether the 'defendant purposefully established' contacts with the forum state."[163]

Purposeful availment may be a difficult standard to meet when a defendant has sent millions of e-mails all over the world, including e-mails to residents of the forum state. Courts have read this requirement narrowly:

> [T]he owner of a website can have some contact with people and entities within a given forum state without taking any purposive step towards the residents of that state or even knowing that a contact has been made. Even sending an e-mail requires some purposive step towards a particular individual, but that often will not be sufficient to constitute purposeful availment.[164]

In determining whether a defendant's contacts are sufficient to find that he purposefully availed himself of the laws and protections of the forum state in a case involving the Internet, a variety of factors come into play. The court is forced to weigh these factors in making its decision.

Factors weighing in favor of exercising personal jurisdiction

(1) income being generated for the defendant through Internet contacts with residents of the forum state;
(2) knowledge by the defendant that the Internet activity will do substantial damage to the plaintiff in the forum state;
(3) the maintenance of a website that produces a high number of "hits" by residents of the forum state;
(4) indiscriminate responses by the defendant to every e-mail sent to the website;
(5) the presence of website content indicating that the website is targeting an audience that includes the forum state, and

161 *See* Stott, *supra* note 142, at 825–26.

162 *See* 4A CHARLES ALAN WRIGHT & ARTHUR R. MILLER, FEDERAL PRACTICE AND PROCEDURE § 1073.1 (3d ed. 2002) (stating "the analysis applicable to a case involving jurisdiction based on the Internet (or any other modern technology) should not be different at its most basic level from any other personal jurisdiction case").

163 *Zippo Mfg. Co.*, 952 F. Supp. at 1123 (quoting Burger King Corp. v. Rudzewicz, 471 U.S. 462, 475 (1985)).

164 WRIGHT & MILLER, *supra* note 162.

(6) the Internet service provider being located in the forum state.[165]

Factors weighing against exercising personal jurisdiction

(1) use of disclaimers, such as that the website is intended for a limited audience;
(2) statements posted on the website directed only at residents of a limited geographic area;
(3) designing the site so that it will not interact with users of the forum state;
(4) a self description of or notice on the website to the effect that it is only "informational";
(5) the absence of evidence of the website being contacted by residents of the forum state; and
(6) the use of forum-selection or choice- of-law agreements that specify a state other than the forum state selected by the plaintiff.[166]

2. Claim asserted against the defendant must arise out of defendant's contacts with the forum state.—This question involves an analysis of the defendant's contacts with the forum state and whether the plaintiff's cause of action arises out of those forum–related contacts.[167] The plaintiff must demonstrate that the cause of action arose from defendant's activities in the forum state; a defendant's physical presence in the jurisdiction is not necessary to establish this prong.[168]

3. Exercise of personal jurisdiction over defendant must be reasonable.—In the third prong of the analysis, the court must be satisfied that the exercise of personal jurisdiction over the defendant, based on the contacts that the defendant has with the forum state, is fair and reasonable.[169]

The issue of fair and reasonable exercise of personal jurisdiction over a nonresident defendant in a case involving the Internet was addressed in *EDIAS Software Int'l v. BASIS Int'l Ltd.*[170] The plaintiff software company filed an action in the plaintiff's home state, claiming defamation and libel,

165 *Id.*

166 *Id.*

167 *See id.*

168 *See* Burger King Corp. v. Rudzewicz, 471 U.S. 462, 476 (1985) (stating that "[s]o long as a commercial actor's efforts are 'purposefully directed' toward residents of another State, we have consistently rejected the notion that an absence of physical contacts can defeat personal jurisdiction").

169 *See* WRIGHT & MILLER, *supra* note 162.

170 EDIAS Software Int'l v. BASIS Int'l Ltd., 947 F. Supp. 413 (D. Ariz. 1996).

based on e-mails sent by the defendant and a press release posted on the defendant's website.[171] In finding that personal jurisdiction over the defendant was fair and reasonable, the court said that the defendant "should not be permitted to take advantage of modern technology through an Internet Web page and forum and simultaneously escape traditional notions of jurisdiction."[172] Courts could also look to the number of hits a webpage receives from residents of a forum state, and to other evidence that Internet activity was directed at the forum state.

C. Application of Minimum Contacts Test to Website Operators: Zippo

Zippo Manufacturing Co. v. Zippo Dot Com, Inc.[173] is one of the leading cases dealing with personal jurisdiction and the Internet.[174] Zippo Manufacturing sued Zippo Dot Com under, *inter alia*, the Federal Trademark Act.[175] In denying the defendant's motion to dismiss for lack of personal jurisdiction, the court set the foundation for how future courts would analyze whether a defendant website operator had sufficient minimum contacts with a forum state to justify exercising personal jurisdiction over him.[176] The issue was whether the website operator's contacts with the forum state, via the Internet, were sufficient to satisfy the minimum contacts requirement of due process.[177]

In *Zippo*, United States District Judge Sean J. McLaughlin synthesized the due process minimum contacts analysis into a sliding scale of activity for differentiating among several levels of contact that an operator of an Internet website may have with a particular forum state.[178] The underlying rationale of the scale is an attempt to create a balancing standard that reflects "the likelihood that personal jurisdiction can be constitutionally exercised is directly proportionate to the nature and quality of commercial activity that an entity conducts over the Internet."[179]

Under this analysis, the court determines whether the website is active, interactive, or passive.[180] One end of the spectrum consists of active websites, such as those in which the website operator conducts business transactions over the Internet: "[i]f the defendant enters into contracts with residents of a foreign jurisdiction that involve the knowing and repeated

171 *Id.* at 414–15.
172 *Id.* at 420.
173 Zippo Mfg. Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119 (W.D. Pa. 1997).
174 *See* WRIGHT & MILLER, *supra* note 162.
175 *Zippo Mfg. Co.*, 952 F. Supp. at 1121.
176 *See* WRIGHT & MILLER, *supra* note 162.
177 *See Zippo Mfg. Co.*, 952 F. Supp. at 1124.
178 *See id.*
179 *Id.*
180 *Id.*

transmission of computer files over the Internet, personal jurisdiction is proper."[181] Passive websites occupy the opposite end of the spectrum and are characterized as "situations where a defendant has simply posted information on an Internet Web site which is accessible to users in foreign jurisdictions."[182] Given that the passive website "does little more than make information available to those who are interested,"[183] an operator of a passive website does not establish sufficient contacts as grounds for exercising personal jurisdiction.[184]

Somewhere between active and passive websites lies the middle ground referred to as interactive websites[185] that allow users to exchange information with a host computer,[186] but the interaction does not rise to the level of continuous and systematic operations that would typify an active website. If the court finds that a defendant operates an interactive website, the exercise of jurisdiction is "determined by examining the level of interactivity and commercial nature of the exchange of information that occurs in the Web site."[187]

Even though the scale has not been endorsed by the Supreme Court as the definitive test for personal jurisdiction over defendants who operate Internet websites, Judge McLaughlin's sliding scale is one way to visualize the continuum of personal jurisdiction and the Internet.[188] While the scale was originally developed to analyze personal jurisdiction issues regarding defendants who operate websites, it is possible that the same scale may be applied to analyze whether a court may exercise personal jurisdiction over a defendant–spammer under the CAN-SPAM Act. As a result, the sliding scale analysis promulgated in *Zippo* can provide several avenues for resolving one of the CAN-SPAM Act's most criticized flaws: the lack of a process to gain personal jurisdiction over a spammer.

D. Application of Minimum-Contacts Test to Spammers

1. Sliding Scale Approach. — In applying *Zippo*'s sliding scale analysis to defendant–spammers, the difficult issue will be determining whether certain activities specific to spamming will be characterized as "active spamming" or "passive spamming."

181 *Id.* (citing CompuServe, Inc. v. Patterson, 89 F.3d 1257 (6th Cir. 1996)).

182 *Id.*

183 *Id.*

184 *Id.*

185 *Id.*

186 *Id.*

187 *Id.*

188 *See* WRIGHT & MILLER, *supra* note 162.

While case law is obviously needed to develop this analysis, in light of the factors discussed in Part V.B.1,[189] the *Zippo* sliding scale,[190] and subsequent cases construing the scale,[191] the following characteristics might be a way of categorizing a defendant spammer's contacts with the forum state: (a) how the spammer obtained the recipients' e-mail addresses; (b) whether, and to what extent, the spammer has entered into contracts with e-mail recipients from the forum state; (c) whether, and to what extent, the spammer has derived financial benefit from residents of the forum state; and (d) whether, and to what extent, the spammer has concentrated his efforts in one state. The goal of this analysis will be to develop factors that will make the nonresident defendant-spammer appear more like the operator of an "active" website as opposed to factors that make him appear more like a "passive" website operator.

Many courts have held that a website will be deemed "active" when it advertises goods and services and provides some mechanism for Internet consumers to actually enter into contracts with the nonresident defendant.[192] The degree of active solicitation by the website operator and whether the website provides a mechanism for allowing Internet consumers to buy goods and services seems to be a strong indication that the website is active and thus exercising personal jurisdiction would be permitted. In *Cybersell, Inc. v. Cybersell, Inc.*,[193] the court found that the website was a passive homepage and that there were no deliberate, directed merchandising efforts toward the state.[194] Thus, a critical distinction is whether, and to what extent, the nonresident defendant is soliciting and actually doing business over the Internet with residents of the forum state.

Similar distinctions may be relevant in analyzing a spammer's activities. The fact that a defendant spammer actually benefits from his UCE will be a strong indication that the defendant has minimum contacts, such as when the UCE actually leads to a commercial transaction. The more transactions that the spammer enters based on his UCE, the more active the spammer appears. The strongest indication of whether the spammer has minimum

189 *See supra* notes 162–66 and accompanying text.

190 *See Zippo Mfg. Co.*, 952 F. Supp. at 1124.

191 *See* Lakin v. Prudential Sec., Inc., 348 F.3d 704, 711 (8th Cir. 2003) (failing to adopt the sliding scale for a case of general jurisdiction); Carefirst of Maryland, Inc. v. Carefirst Pregnancy Ctrs., Inc., 334 F.3d 390, 400 (4th Cir. 2003) (affirming trial court's dismissal for lack of personal jurisdiction stating "in order for [the defendant's] website to bring [the defendant] within the jurisdiction of the Maryland courts, the company must have done something more than merely place information on the Internet"); DakCoII Inc. v. Grand Cent. Graphics, Inc., 352 F. Supp. 2d 990, 997 (D.N.D. 2005) (holding that defendant's website that had "a very high level of interactivity" was sufficient for exercising personal jurisdiction over the defendant).

192 *See Zippo Mfg. Co.*, 952 F. Supp. at 1124.

193 Cybersell, Inc. v. Cybersell, Inc., 130 F.3d 414, 419 (9th Cir. 1997).

194 *Id.* at 419.

contacts would be the number of e-mail messages the spammer directs toward a given forum. However, if the spammer does not appear to target any forum in particular, derives no financial benefit from the spam, and sends a low number of messages, then the spammer seems more passive.

Just as the *Cybersell* court focused on the extent to which a website operator actually enters into contracts with consumers in the particular forum state for determining whether the website is active, interactive or passive, this same factor would carry some weight in the context of spam. However, this factor should not be determinative when dealing with a defendant-spammer because it fails to address the main problem of UCE: the sheer fact that spam is a costly nuisance. Thus, more weight should be given to the extent to which a spammer sends out UCE to a forum state than to the extent to which residents of the forum state actually buy the products being sold in the e-mail.

In *Inset Systems, Inc. v. Instruction Set, Inc.*[195] the court found that "advertising via the Internet is solicitation of a sufficient repetitive nature to satisfy" Connecticut's long–arm statute and due process.[196] In support of its finding that the defendant, a Massachusetts corporation, had established minimum contacts, the court reasoned that the defendant had purposefully availed itself of the privilege of doing business within the forum state because the Internet advertisements reached as many as 10,000 users in Connecticut (the number of Internet access sites in Connecticut) and because an online advertisement is continuously available to any Internet user.[197]

2. Creating a New Minimum Contacts Analysis for Defendant-Spammer and the Internet.—Internet activity will likely continue to grow. Without additional congressional legislation or a decisive Supreme Court case, personal jurisdiction and Internet activity will continue to be in flux, particularly with regards to the CAN-SPAM Act and spamming. While the CAN-SPAM Act is clearly a step towards regulating spam, it needs to be strengthened by supplemental legislation that will confer some basis for allowing small ISPs to bring suit against defendants in the ISP's state, instead of allowing spammers to be shielded by due process protections.[198] Until new legislation or a Supreme Court case endorses one standard, the number of standards construing when personal jurisdiction is appropriate with regard to Internet activities will continue to increase and confuse the courts.

195 Inset Sys. Inc., v. Instruction Set, Inc., 937 F. Supp. 161 (D. Conn. 1996).

196 *Id.* at 164.

197 *Id.* at 165.

198 *See supra* notes 142–72 and accompanying text.

VI. The Future of the CAN-SPAM Act

While this Note has focused on two of the primary criticisms of the CAN-SPAM Act that the literature has acknowledged but never attempted to provide a remedy for, there are other criticisms of the Act that have received significant attention in the literature and therefore were given little attention in this Note. Some critics, for instance, argue that the federal government acted too quickly by not providing enough time for states to serve as the laboratories "without risk to the rest of the country."[199]

Some authors have criticized the CAN-SPAM Act because it actually legalizes some spam as long as the spam follows the guidelines of the Act.[200] Experts claim that there "will be a lot more spam by legitimate marketers because they will be able to point to the federal law and say, 'We are following all the rules.'"[201] The CAN-SPAM Act applies only to *unsolicited, commercial* e-mail messages which are primarily for advertisement of goods or services[202] and therefore does not apply to other forms of spam such as political e-mail; the Act does not prohibit the sending of all unsolicited commercial e-mail but is focused on certain fraudulent and misleading practices.[203]

Some have criticized the CAN-SPAM Act because it removed regulation of spam from the states before the most effective solution could be found,[204] and, in doing so, preempted stronger state laws,[205] such as the laws

199 *See* Alongi, *supra* note 52, at 288; *see also* New State Ice Co. v. Liebmann, 285 U.S. 262, 311 (1932) (Brandeis, J., dissenting) ("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 of the country.").

200 *See* Alongi, *supra* note 52, at 288.

201 David Firestone & Saul Hansell, *Senate Votes to Crack Down on Some Spam*, N.Y. Times, Oct. 23, 2003, *available at* http://web.mit.edu/21w.784/www/BD%20Supplementals/Materials/Unit%20Two/Spam/senate%20contra%20spam%20nyt.html (quoting David Sorkin). *See also* Jacquelyn Trussell, Student Article, *Is the CAN-SPAM Act the Answer to the Growing Problem of Spam?*, 16 Loy. Consumer L. Rev. 175, 187 (2004) ("By regulating spam, the CAN-SPAM Act legitimizes certain types of spam. Many fear that a wave of legitimate spam will be unleashed from companies that previously feared being labeled as spammers.").

202 Glenn B. Manishin & Stephanie A. Joyce, *Overview of Current Spam Law & Policy*, *in* Complying with the CAN-SPAM Act and Other Critical Business Issues: Staying Out of Trouble 9, 13–14 (Practising Law Institute ed., 2004).

203 Shirin Malkani et al., *Understanding the CAN-SPAM Act of 2003*, *in* Institute on Privacy Law (5th Annual): New Developments & Compliance Issues in a Security-Conscious World 482, 483 (Practising Law Institute ed., 2004).

204 *See* Alongi, *supra* note 52, at 288 (discussing how states are analogous to "many laboratories" where various solutions could be tested).

205 *See* Jeremiah Kelman, Note, *E-Nuisance: Unsolicited Bulk E-Mail at the Boundaries of Common Law Property Rights*, 78 S. Cal. L. Rev. 363, 375 (2004); *see also* Grant Gross, *Is CAN-SPAM Working?; One year after it went into effect, many say the nation's antispam law is ineffective*, PC World, Dec. 28, 2004, http://www.pcworld.com/news/article/0,aid,119058,00.asp (discuss-

enacted in California and Virginia. While the exact scope of this preemption is unclear,[206] the Act expressly "supersedes any statute, regulation or rule of a State or political subdivision of a State that expressly regulates the use of electronic mail to send commercial messages,"[207] but it does not preempt general state laws regarding trespass, contract or tort, or laws that relate to acts of fraud or computer crime.[208]

The California statute,[209] which would have gone into effect in January 2004 but was instead preempted by the CAN-SPAM Act, required spammers to obtain consent before sending spam to any recipients, essentially creating an "opt-in" scheme.[210] However, the CAN-SPAM Act takes a more spam-friendly approach by requiring senders of UCE to provide recipients with an opt-out mechanism: a "clear and conspicuous notice of the opportunity ... to decline to receive further commercial electronic mail messages from the sender."[211] The California statute provided another invaluable mechanism for enforcement that the CAN-SPAM Act neglected to adopt: a private right of action to allow spam recipients to bring suit for damages, up to $1 million per incident, plus attorney fees and costs.[212] The CAN-SPAM Act also "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."[213] Obviously, the prospect of a felony conviction and a prison sentence could have proven more of a deterrent than CAN-SPAM's monetary damages.

While the CAN-SPAM Act certainly has critics, the Act has had some success in suits against spammers. In March 2004, the Anti-Spam Alliance, made up of four of the largest ISPs in the United States—America Online, Microsoft, Yahoo, and Earthlink—filed six lawsuits in multiple states against several hundred defendants, basing their suits on the CAN-SPAM Act.[214] The alliance filed a second round of suits in October 2004.[215]

---

ing Laura Atkins,' President of the SpamCon Foundation, assertion that the CAN-SPAM Act "hurt spam-fighting efforts by pre-empting parts of some tougher state laws, including a California opt-in requirement").

206 *See supra* notes 65–73 and accompanying text.

207 15 U.S.C.S. § 7707(b)(1) (2005).

208 § 7707(b)(2).

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

210 *Id.* at § 17529.2(a)–(b).

211 15 U.S.C.S. § 7704(a)(5)(A)(ii) (2005).

212 *See* CAL. BUS. & PROF. CODE § 17529.5 (West 2003); *see also* Alongi, *supra* note 52, at 287–88.

213 Alongi, *supra* note 52, at 287. "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." *Id.*

214 Marguerite Reardon, *Major ISPs Unite in Spam Fight*, CNET NEWS.COM, Mar. 10, 2004, http://news.zdnet.com/2100-1009_22-5172038.html.

215 Marguerite Reardon, *New Round of Spam Suits from AOL, Microsoft, Yahoo*, CNET

VII. Conclusion

The CAN-SPAM Act clearly has problems, which have been well documented. In fact, up to this point, the Act's potential uses have been overshadowed by criticisms of its failings. While recognizing the criticisms and the faults of the CAN-SPAM Act, this Note evaluates these drawbacks and attempts to demonstrate some benefits of the Act by using current case law and analogies of spam to other electronic communications under the TCPA and situations where personal jurisdiction was found against website operators.

Given the nature of the Internet and the easy access that spammers have to anyone's e-mail inbox, it is doubtful that U.S. federal antispam legislation will end spam. However, the Act does provide the first federal cause of action for UCE and has had some success. While the CAN-SPAM Act has not canned spam, further legislation and clever analogies by lawyers will prove that the CAN-SPAM Act provides a solid foundation in the fight against spam.

News.com, Oct. 28, 2004, http://news.com.com/New+ round+of+spam+ suits+from+AOL%2C+Microsoft%2C+Yahoo/2100-1038_3-5431002.html?tag=st.rc.targ_mb.