Regulating Unsolicited Commercial Electronic Mail in the United States and the European Union: Challenges and Prospects

Taiwo A. Oriola*

This Article examines the legislative response in the United States and the European Union to spam proliferation, and their prospects for a successful antispam campaign. The legal regimes on both sides of the Atlantic try to balance the conflicting interests of spam senders and recipients without much success, to the displeasure of both antispam and prospam campaigners. With both sides employing privacy and free speech rights to rally their cause, maintaining an even balance between the two conflicting interests is nigh impossible, and remains the greatest challenge to both the CAN-SPAM Act and the E-Privacy Directive. The failure of regulation in this respect, the Article notes, is symptomatic of the intractable nature of cyberspace, and the obvious limitations of regulatory regime in Internet governance. Using analogous case law, this Article argues that it is unlikely that the U.S. and European courts would hold accurate header information and labeling provisions unconstitutional or violative of freedom of expression, as canvassed by some observers. This Article also highlights the obvious differences between U.S. and E.U. antispam regimes, and argues for the combination of an effective and internationally enforceable antispam regime with cutting edge antispam technology to combat the increasing spam menace.

* LL.M. European Intellectual Property Law (Stockholm); LL.M. Information Technology Law (Stockholm); LL.M., LL.B. (Ife); B.L. (Lagos); Research Scholar, Faculty of Law, National University of Singapore.

I. INTRODUCTION

An e-mail message has been defined as a computer file transferred from one computer to another, over a telephone line using a modem, among several computers on a local area network, or between separate networks that are interconnected.[1] The Internet began with the acceptance of the first Transmission Control Protocol/Internetwork Protocol (TCP/IP) as a de facto worldwide standard in the 1980s and 1990s.[2] In the late 1980s, electronic mail became an integral feature for creating links between information stored in different computers around the world.[3] E-mail messages are transmitted using Simple Mail Transfer Protocol (SMTP), while commercial applications often use protocols that are more complex.[4]

---

1. *See* Brian G. Gilpin, *Attorney Advertising and Solicitation on the Internet: Complying with Ethics Regulations and Netiquette*, 13 J. MARSHALL J. COMPUTER & INFO. L. 697, 719 n.187 (1995). Furthermore, according to a Resolution passed by the United States Federal Networking Council (FNC) in October 1995:

> "Internet" refers to the global information system that—(i) is logically linked together by a globally unique address space based on the Internet Protocol (IP) or its subsequent extensions/follow-ons; (ii) is able to support communications using the Transmission Control Protocol/Internet Protocol (TCP/IP) suite or its subsequent extensions/follow-ons, and/or other IP-compatible protocols; and (iii) provides, uses or makes accessible, either publicly or privately, high level services layered on the communications and related infrastructure described herein.

Barry M. Leiner et al., *A Brief History of the Internet, Part II*, *at* http://www.isoc.org/oti/articles/0797/leiner.html (last visited Apr. 7, 2005).

2. To facilitate internalization of the Internet, Transmission Control Protocol (TCP), as the standard that could provide an orderly, error free flow of data from one computer to another, both intra- and between networks, was accepted in 1973 at Stanford University. This agreement was further refined at a meeting in January 1978 at the University of Southern California, when TCP was split into two separate parts: a host-to-host protocol (TCP) and an Internetwork Protocol (IP). The pair facilitates the passage by IP protocols, of individual packets between machines (from host to packet switch or between packet switches), while the TCP ordered packets into reliable connections between pairs of hosts. *See* MARCUS FRANDA, GOVERNING THE INTERNET: THE EMERGENCE OF AN INTERNATIONAL REGIME 21-23 (2001).

3. *See* W. GRELICH, GOVERNANCE IN 'CYBERSPACE': ACCESS AND PUBLIC INTEREST IN GLOBAL COMMUNICATIONS 39 (1999).

4. David E. Sorkin, *Unsolicited Commercial E-Mail and the Telephone Consumer Protection Act of 1991*, 45 BUFFALO L. REV. 1001, 1006 (1997).

Spam is a word used to describe unsolicited commercial e-mails.[5] It is often referred to as unsolicited commercial e-mail or unsolicited bulk e-mail.[6] The distinction between the two appellations seems academic, and appears relevant only in the context of the volumes of spam sent at a time.[7] Otherwise the distinction is moot, for most spams are invariably commercial in nature, not in the least because antispam legislations worldwide are targeted at commercially oriented unsolicited e-mails. For instance, unsolicited e-mails are conceived in commercial terms by both the United States' Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act)[8] and the European Union Directive on Privacy and Electronic Communications.[9] *A fortiori*, noncommercial electronic messages such as political speech or an importunate unsolicited love message from a distraught lover would appear exempt from regulation, though they are *stricto sensus* spam.[10] A blanket ban that directly affects political speech and other noncommercial electronic messages could raise constitutional questions,

---

5. The use of "spam" as a nickname for these kinds of e-mails allegedly originated from a comedy sketch on the television show known as Monty Python's Flying Circus. A Viking choir had sung "SPAM, SPAM, SPAM" very loudly and drowned other conversation. This is analogous to spam which by its sheer enormity and frequency, has become a nuisance for other Internet users. *See* Hormel Foods Corp., *SPAM and the Internet*, *at* http://www.spam.com/ci/ci_in.htm (last visited Mar. 13, 2005). The first spam was purportedly sent by two Phoenix attorneys in Arizona in 1994 to some 8000 Usenet Newsgroups. The advertisement reached over twenty million people, and the angry response from recipients crashed the computer of the attorney's ISP. Marketers were subsequently attracted to this technique. *See* Elizabeth A. Alongi, Note, *Has the U.S Canned Spam?*, 46 ARIZ. L. REV. 263, 263 (2004).

6. *See* David E. Sorkin, *Technical and Legal Approaches to Unsolicited Electronic Mail*, 35 U.S.F. L. REV. 325, 330-31 (2001).

7. *Id.* at 326-36.

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

9. Council Directive 2002/58/EC, on the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, 2002 O.J. (L 201) 37 [hereinafter E-Privacy Directive].

10. It is not clear whether political spam would become commercial spam if it were sent through a commercial entity. The Australian Prime Minister recently came under fire from the opposition Labor Party for using a commercial software company to send unsolicited e-mails to voters, pitching Liberal Party agenda, and soliciting votes in the run up to the late 2004 national elections. Although political parties were exempted from Australia's spam laws, the Labor Party wanted an investigation by the Australian Communications Authority, to see if the nation's spam laws had been breached by the use of a commercial intermediary (owned by the Prime Minister's son) for transmitting the unsolicited political e-mails. *See Howard Backs Son's Political Spam Campaign*, ABC NEWSONLINE, Aug. 27, 2004, *at* http://www.abc.net.au/news/newsitems/200408/s1186389.htm; *see also* Mark Sweet, *Political E-mail: Protected Speech or Unwelcome Spam?*, 2003 DUKE L. & TECH. REV. 1, ¶ 1, *available at* http://www.law.duke.edu/journals/dltr/articles/2003dltr0001.html (Jan. 14, 2003) (discussing similar situations involving political spam in the United States).

and invoke judicial censure in both the United States and the European Union.[11]

Spam is not specifically defined or mentioned in the European Union Directive 2002/58/EC on Privacy and Electronic Communications,[12] or the CAN-SPAM Act.[13] The Directive uses the terms "unsolicited communications" by "electronic mail," "for the purposes of direct marketing."[14] In U.S. legislation, the word "CAN-SPAM" appears as an alternate title. However, the word "SPAM" merely complements "CAN" as an acronym for the full title of the Act, and bears no connotation to spam as used in linguistic context. Section 3(2)(A) of the CAN-SPAM Act defines a commercial electronic message as "any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service (including content on an Internet website operated for commercial purpose)."[15] Spam would cover all forms of unsolicited commercial e-mails, in the traditional SMTP-based e-mail and other electronic messaging systems such as SMS and Multimedia Messaging Service (MMS).[16]

A definitional crisis could arise in jurisdictions such as the United Kingdom in particular, and the European Union in general, where spam laws adopt an "opt-in" consent-based policy to spam traffic. For instance, Regulation 22(2) of the United Kingdom Privacy and Electronic Communications (EC Directive) Regulations[17] provides, inter alia, that transmissions of unsolicited communications for the purposes of direct marketing could not be done without the previous consent of the

---

11. As it were, observers have fingered the requirement for labeling in the U.S antispam law as a free speech infraction. *See* Jerry Berman & Paula J. Bruening, *Can Spam Be Stopped? Rather Than Legislate a Quick Fix, Congress Needs to Look Harder at Legal and Technical Complexities*, LEGAL TIMES, June 16, 2003, at 76. This point will be elaborated on later in this Article.

12. *See* E-Privacy Directive, *supra* note 9. The E-Privacy Directive introduced the principle of consent-based marketing (opt-in) for electronic mail (including mobile SMS or MMS messages). The deadline for implementing the directive in member states was Oct. 31, 2003. *Id.* art. 17; *see also* Opinion of the Committee of the Regions on the Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions on Unsolicited Commercial Communications or 'Spam', 2004 O.J. (C 318) 24 [hereinafter Spam Communication].

13. 15 U.S.C.A. §§ 7701-7713.

14. *See* E-Privacy Directive, *supra* note 9, art. 13(2)-(3).

15. 15 U.S.C.A. § 7702.

16. *See* E-Privacy Directive, *supra* note 9, art. 13(1).

17. *See* (2003) SI 2003/2426. The Regulation took effect on December 11, 2003, in the United Kingdom. It was made pursuant to the E-Privacy Directive on privacy and electronic communications.

recipients.[18] This is a consent-based ("opt-in") approach to spam traffic, which raises the pertinent issue of when spam is spam. If for instance there was previous consent, unsolicited communication sent subsequent to such consent would, *stricto sensus*, not amount to spam in the absence of evidence that corroborates consent retraction, or negates the recipient's consent.[19]

Spam is a growing phenomenon, whose pervasiveness is as annoying as it is costly for most Internet users and service providers.[20] Significantly, spam, like unwanted letters, is tantamount to a breach of privacy,[21] as it involves the acquisition and transmission of personal data (e-mail addresses), usually without users' consent.[22] According to Edwin L. Klett, consumers both pay for, and suffer great inconvenience in reviewing and deleting spam.[23] Spam costs are incurred by recipients[24] directly through per minute payment for Internet service or indirectly, where Internet service providers pass on the extra costs of antispam software, or the expense of staff hired specifically to filter out unsolicited

---

18. Regulation 22(2) of the United Kingdom Privacy and Electronic Communications (EC Directive) Regulations, SI 2003/2426, provides:

> Except in the circumstances referred to in paragraph (3), a person shall neither transmit, nor instigate the transmission of, unsolicited communications for the purposes of direct marketing by means of electronic mail unless the recipient of the electronic mail has previously notified the sender that he consents for the time being to such communications being sent by, or at the instigation of, the sender.

19. Technically, the previous consent would negate the word "unsolicited" and render the spam not spam. Such consent however is not irrevocable. The phrase "consents for the time being" in Regulation 22(2) implies that the consent is valid only for the duration in which it is given. *See id.* Consent could possibly be vitiated by fraud or misrepresentation.

20. *See* TIM KEVAN & PAUL MCGRATH, E-MAIL, THE INTERNET AND THE LAW 111 (2001).

21. *See* Rowan v. United States Post Office Dep't, 397 U.S. 728 (1970). The United States Supreme Court held that "a mailer's right to communicate must stop at the mailbox of an unreceptive addressee." *Id.* at 736-37. This decision could justify e-mail recipients' right to opt-out of receiving unsolicited e-mails. The plaintiffs in *Rowan* were engaged in the mail order business. *Id.* at 729. They sold, mailed, and distributed items, books, and materials throughout the United States. *See id.* Plaintiffs challenged the constitutionality of the Postal Statute prohibiting pandering advertisement in the mails, and for an injunction restraining the enforcement of the statute. *Id.* at 731. The Court held that the statute did not violate the right of free speech or free press. *Id.* at 738.

22. See Daniel J. Solove, *The Virtues of Knowing Less: Justifying Privacy Protections Against Disclosure*, 53 DUKE L.J. 967, 971-77 (2003); Debra A. Valentine, *About Privacy: Protecting the Consumer on the Global Information Infrastructur*e, 1 YALE SYMP. L. & TECH. 4 (1999).

23. *See* Edwin L. Klett & Rochelle L. Brightwell, *Spam Mail: An Electronic Nuisance to Be Reckoned With*, LAW. J., May 31, 2002, at 11.

24. *See* CAN-SPAM Act § 2(a)(3), 15 U.S.C.A. § 7701(a)(3) (Supp. VI 2004). "The receipt of unsolicited commercial electronic mail may result in costs to recipients who cannot refuse to accept such mail and who incur costs for the storage of such mail, or for the time spent accessing, reviewing, and discarding such mail, or for both." *Id.*

mail.[25] The cost of receiving electronic mail would invariably depend on whether the recipient uses dial-up connections or a broadband connection.[26] According to Jane Weaver, some antispam technologies averaged a cost of $40 a year, and could be beyond the reach of average Internet users.[27]

Additionally, Internet Service Providers (ISPs) also bear spam's economic burdens occasioned by slowed e-mail traffic, overburdened servers and the prospect of losing subscribers.[28] This is illustrated in the U.S. case *CompuServe Inc. v. Cyber Promotions, Inc.*[29] CompuServe had received several complaints from its subscribers threatening termination of subscriptions if unsolicited e-mails were not stopped.[30] The court held that where the defendant engaged in a course of conduct of transmitting a substantial volume of electronic data in the form of unsolicited e-mails to the plaintiff's proprietary computer equipment, the defendant continued such practice after repeated demands to cease and desist, and where the defendant deliberately evaded the plaintiff's affirmative efforts to protect its computer equipment from such use, the plaintiff has a viable claim for trespass to personal property and is entitled to injunctive relief to protect his other property.[31]

However, in terms of frequency and numbers, spam appears stuck in a perpetual spiral climb.[32] For instance, in a single day in May 2003,

---

25. *See* Danielle Cineros, *Do Not Advertise: The Current Fight against Unsolicited Advertisements*, 2003 DUKE L. & TECH. REV. 10, ¶ 10 n.37, *at* http://www.law.duke.edu/journals/dltr/articles/PDF/2003DLTR0010.html (Apr. 29, 2003).

26. *See* Wendy R. Leibowitz, *Do Junkmailers Have Right to Send Unwanted E-mail? A Federal Law Suit Against AOL Presents a Free Speech Case of First Impression*, NAT'L L.J., Oct. 21, 1996, at A7.

27. *See* Jane Weaver, *Kill the Spam, Save My Email*, *at* http://www.msnbc.msn.com/id/3072605 (last visited Mar. 15, 2005).

28. *See* Klett & Brightwell, *supra* note 23. In the fight against spam, ISPs often hire extra hands to help filter out unsolicited e-mails, and take calls on customers' complaints on spam. Combating spam also requires purchasing additional bandwidth to process high-volume traffic, as well as more computers to safeguard system from theft, and cope with extra traffic induced by spam. *Id.*

29. 962 F. Supp. 1015 (S.D. Ohio 1997).

30. *Id.* at 1017.

31. *Id.*; *see also* Steven Kam, Note, Intel Corp. v. Hamidi*: Trespass to Chattels and a Doctrine of Nuisance*, 19 BERKELEY TECH. L.J. 427, 427 (2004). ISPs are increasingly resorting to lawsuits to discourage unsolicited e-mails. Such a lawsuit resulted in a consent judgment of $2,000,000 against a spammer in March 1998. *See* Earthlink Network Inc. v. Cyber Promotions, Inc., No. BC 167502 (Cal. Super. Ct. Mar. 30, 1998).

32. *See* CAN-SPAM Act § 2(a)(2), 15 U.S.C.A. § 7701(a)(2) (Supp. VI 2004) ("The convenience and efficiency of electronic mail are threatened by the extremely rapid growth in the volume of unsolicited commercial electronic mail. Unsolicited commercial electronic mail is currently estimated to account for over half of all electronic mail traffic, up from an estimated

an ISP, AOL Time Warner, blocked 2 billion messages (88 per subscriber) from reaching subscriber accounts.[33] Moreover, January 2004 went on record as the worst month for spam proliferation, with 700 billion worldwide unsolicited e-mails.[34] Furthermore, a recent global estimate puts spam at nearly 70% of all e-mails clogging inboxes worldwide, with a forecast increase to 80% by the middle of 2004.[35] Additionally, a company allegedly sent unsolicited commercial e-mails to 900,000 e-mail addresses two times daily.[36] Moreover, a January 2004 estimate shows unsolicited e-mails jumped from 42% of total e-mail in February 2003 to 60% in January 2004,[37] and there are no indications that the percentage would decrease any time soon, due largely to spam being a cheap and easy advertising medium.[38] Apart from the ordinary Internet users, corporations also bear the financial brunt of unsolicited e-mails. In the United States alone, the annual costs of spam to corporations are an estimated $8.9 billion, while European ISPs lose an estimated $500 million annually to spam.[39] Spam's social and financial injuries are so

---

seven percent in 2001, and the volume continues to rise. Most of these messages are fraudulent or deceptive in one or more respects.").

33. According to the same report, MSN mail-plus Hotmail blocks an average of 2.4 billion spam per day. Jane Black, *Before Spam Brings the Web to Its Knees*, BUS. WK. MAG. ONLINE, June 10, 2003, *at* http://www.businessweek.com/technology/content/jun2003/tc20030610_1670_tc104.htm.

34. According to the data from the United Kingdom based mi2g's Security Intelligence Products and System database, the figure accounted for 58% of all the e-mails sent in the month of January 2004. *IT in Stats: Computer Bugs Munch Their Way Through Company Profits*, FT IT Review, FIN. TIMES, Mar. 3, 2004, at 6.

35. According to an Information Security Analyst firm, MessageLab, antispam legislations seemed to promote rather than discourage spam proliferation. *See Spam Messages on the Increase*, BBC NEWS, *at* http://news.bbc.co.uk/2/hi/technology/3746023.stm (May 25, 2004); *European Anti-Spam Laws Lack Bite*, BBC NEWS, *at* http://news.bbc.co.uk/1/hi/technology/3666585.stm (Apr. 28, 2004).

36. *See* Joshua A. Marcus, Note, *Commercial Speech on the Internet: Spam & the First Amendment*, 16 CARDOZO ARTS & ENT. L.J. 245, 250 (1998).

37. *See* Brightmail Logistics and Operations Centre (Bloc), *at* http://www.brightmail.com/spamstats.html (last visited July 24, 2004). The 60% for January 2004 were further categorized by Brightmail: products—22%, financial—20%, adult—17%, scams—8%, health—7%, leisure—6%, Internet—5%, fraud—4%, political—2%, spiritual—2%, and others—8%.

38. A single message could be sent to multiple recipients at relatively cheap costs. *See* James Gleick, *Hold the Spam*, N.Y. TIMES, Dec. 22, 1996, at 22. Furthermore, according to Larry Bridwell, security lab manager at ICSA Labs, the absence of postage fees as in real mail makes spam very attractive to spammers. The more spam e-mails are sent, the more the unit costs drop. This low cost is instrumental to the exponential increase in spam mails. *See CLSR Briefing*, 19 COMPUTER L. & SECURITY REP. 428, 428-30 (2003).

39. *See* Anick Jesdanun, *Spam Costs U.S Firms About $8.9 Billion Annually, Study Says*, AP ONLINE, *at* http://news.spamcop.net/pipermail/spamcop-list/2003-January/029374.html (Jan. 5, 2003).

overwhelming, that some analysts have likened it to "cyber-terrorism."[40] There is a pervasive fear amongst industry and authorities that spam could stifle and undermine the trust and confidence that are the critical mass for the success of electronic commerce.[41] It is no wonder then that the industry and authorities are now fighting back. The initial counter-measures against spam by network service providers were the use of "contractual prohibitions, rules of 'netiquette,' and various self-help mechanisms."[42] These measures appeared inadequate, hence the renewed legislative and technical initiatives designed to block all loopholes.

This Article examines legislative and technical antispam measures in the United States and the European Union. It identifies the greatest challenge to all antispam measures as the imperatives of balancing the conflicting interests in spam senders' right to send unsolicited commercial messages (which borders on free speech)[43] and spam recipients' right to privacy, or the right not to receive spam (which also qualifies as free speech). Surely, there is a bright line between these conflicting rights on a constitutional landscape laden with litigation mines.[44] This Article will seek to address the following pertinent questions: How have recent legislative and technical measures in the European Union and the United States drawn a balance between these conflicting interests? What are the parameters for delimiting the scope of spammers' and spam recipients' conflicting rights? Would the demarcation survive potential constitutional challenge in the U.S. courts

---

40. *See* Rene Ryman, *The Adverse Impact of Anti-Spam Companies*, COMPUTER & INTERNET LAW. (Aspen Publishers, New York, NY), Jan. 2003, at 15.

41. *See* Spam Communication, *supra* note 12, at 3.

42. David E. Sorkin, Abstract, *Unsolicited Commercial E-mail and the Telephone Consumer Protection Act of 1991*, *at* http://www.sorkin.org/articles/buffalo.html (last visited Apr. 6, 2005). For instance, a French court held a spammer liable for noncompliance with the terms of his contract, to justify the revocation of his contract. The case was *G. v. France Telecom Interactive, S.A.*, T.G.I. Rochefort-sur-Mer, Feb. 28, 2001, obs. J. Manabe. G's claim for the continuation of his access contract with Wanadoo, after the contract had been cancelled by France Telecom because of G's spamming activities to public discussion groups, was dismissed on the ground that article 1135 of the French Civil Code obliges parties to a contract not only to its express statements but also to what customs as a source of law in this field contain. It was established that spamming to public discussion groups, according to netiquette rules, should be considered as contrary to a custom in the Internet World. *See also P.V. and Liberty Surf/Société Free*, T.G.I. Paris, Jan. 15, 2002. The same principle in the *France Telecom Interactive* case was followed there. *See* Sorkin, *supra* note 4, at 1024-27; *see also* Gary S. Moorefield, Note, *SPAM-It's Not Just 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, ¶¶ 15-22 (1999) (discussing the failure of ISPs to prevent spam in the absence of federal antispam legislation).

43. Marcus, *supra* note 36, at 250.

44. *See* Solove, *supra* note 22, at 989-1000; Eric J. Sinrod & Barak D. Jolish, *Controlling Chaos: The Emerging Law of Privacy and Speech in Cyberspace*, 1999 STAN. TECH. L. REV. 1, ¶ 54, *available at* http://stlr.stanford.edu/STLR/Articles/99_STLR_1/index.htm.

or in the European Court of Human Rights? What are the prospects for legitimate marketers under the current antispam regimes on both sides of the Atlantic? How effective are, and what are the prospects for success for antispam legislative and technical measures in the long term? These questions transcend mere rhetoric. Finding satisfactory answers would require a critical evaluation of the full imports of the economic and security threats posed by spam, and the proprieties of the legislative and technical countermeasures in the context of conflicting rights to privacy, free speech, and sustainable electronic commerce.

The Article is divided into seven parts. Part I is the introduction. Part II is on the nature of spam and how it works. Part III is a general discourse on spam regulation, while Part IV deals with antispam regulation in the United States. Part V addresses antispam regulation in the European Union, while Part VI discusses antispam technical measures. Part VII sums up the various discourses and highlights the most plausible strategies for effective spam control. This Article concludes with Part VIII.

II. HOW SPAM WORKS

The spam market is thriving. It is estimated that approximately $1.1 billion is spent on e-mail advertising annually as more and more businesses strive to reach out to customers.[45] E-mail advertising has in turn spawned a new market for trade in e-mail addresses. Senders of unsolicited commercial e-mails usually obtain e-mail addresses from companies that specialize in selling them via CDs.[46] A single CD could contain over 90 million e-mail addresses.[47] These e-mails are usually harvested from newsgroups or chat rooms that are prominent features of certain ISPs such as Yahoo!, AOL, and MSN Hotmail.[48] Furthermore, e-mail addresses could be sourced from the World Wide Web. Spammers often use spambots,[49] or spyware programs, to trawl the Web, searching

---

45. *See* Ryman, *supra* note 40, at 15.

46. *See* Marshall Brian, *How Spam Works*, *at* http://computer.howstuffworks.com/spam2.htm (last visited Mar. 15, 2005).

47. *How Spam Works: How Do Spammers Get Our Information?*, *at* http://www.spam-site.com/how_spam_works.shtml (last visited Mar. 15, 2005).

48. Brian, *supra* note 46.

49. A spambot is a kind of software designed to search and retrieve, by stealth, often sensitive information that is not easily available otherwise. Brian, *supra* note 46; *see also* CAN-SPAM Act § 2(a)(10), 15 U.S.C.A. § 7701(a)(10) (Supp. VI 2004) ("Many senders of bulk unsolicited commercial electronic mail use computer programs to gather large numbers of electronic mail addresses on an automated basis from Internet websites or online services where users must post their addresses in order to make full use of the website or service.").

for "the telltale '@' sign that indicates an e-mail address."[50] It is said that a typical e-mail extractor or spambot could gather up to 15,000 e-mail addresses per hour.[51] Another strategy for harvesting e-mail addresses is to create an attractive Web site specifically dedicated to luring surfers, whose e-mail addresses are sold to spammers.[52] Yet another ingenious way of harvesting e-mail addresses is "a dictionary search" of the e-mail servers of large ISPs.[53] Michelle Delio describes the methodology thus:

> A dictionary attack utilizes software that opens a connection to the target mail server and then rapidly submits millions of random e-mail addresses. Many of these addresses have slight variations, such as "jdoe1abc@hotmail.com" and "jdoe2def@hotmail.com." The software then records which addresses are "live," and adds those addresses to the spammer's list. These lists are typically resold to many other spammers.[54]

The above methodology is facilitated because e-mail addresses are usually out in the open, and vulnerable to poachers.[55] There is evidence of a relative degree of spam outreach success.[56] According to the proprietor of a spam company, about three-quarters of all unsolicited e-

---

50. Brian, *supra* note 46.

51. *Id.*

52. *Id.*

53. Michelle Delio, *Hotmail: A Spammer's Paradise?*, WIRED NEWS, Jan. 9, 2003, *at* http://www.wired.com/news/infostructure/0,1377,57132,00.html.

54. *Id.*

55. *See* Brian, *supra* note 46. Furthermore, the Center for Democracy and Technology has some tips for preventing spam, albeit not fool-proof. It recommends the following: First, avoid posting e-mail addresses at the bottom of Web pages. If this is necessary however, disguise e-mail addresses posted at the bottom of a Web page either by its HTML numeric equivalent or other variations. The Center suggests that an e-mail address such as example@domain.com should be disguised as "example at domain dot com." The HTML numeric variation would appear as "oma&#15;n.co&#109." Second, the Center advises caution in filling out online forms requesting e-mail addresses. Users should check out a company's privacy policy, and exercise their options not to have their e-mail listed or shared with third parties. Third, users are advised to use "disposable e-mail addresses." This would allow for the consolidation of e-mail in a single location, while allowing users to shut off any address that attracts spam. A Google search would reveal a list of e-mail providers that are designed for one time users. Fourth, the Center advises the use of spam filtering technology, which many ISPs and e-mail providers have now embraced. Fifth, it is advised that users should avoid using short e-mail addresses because they are easy to guess by spammers. *See* CENTER FOR DEMOCRACY & TECHNOLOGY, WHY AM I GETTING ALL THIS SPAM? UNSOLICITED COMMERCIAL E-MAIL RESEARCH SIX MONTH REPORT 2-3 (2003), *available at* http://www.cdt.org/speech/spam/030319spamreport.shtml.

56. According to a recent report by Pew Internet & American Life Project, 7% of unsolicited e-mails recipients said they ordered goods or services based on the solicitations in the messages; 33% of recipients said they clicked on a link in unsolicited commercial e-mails. *See* DEBORAH FALLOWS, PEW INTERNET & AMERICAN LIFE PROJECT, SPAM-HOW IT IS HURTING E-MAIL AND DEGRADING LIFE ON THE INTERNET, *at* http://www.pewinternet.org/report/pdfs/PIP_Spam_Report.pdf (Oct. 22, 2003).

mails are read by their recipients. This knowledge is facilitated by a hidden code embedded in each mail that sends back a message each time a mail is opened.[57] Spam companies are springing up in the hundreds, and acting as purveyors of unsolicited e-mails for would-be marketers or advertisers. They send hundreds of thousands unsolicited e-mails to valid e-mail addresses for a fee.[58] According to a report by Mike Wendland, these companies use sophisticated software and various strategies to escape detection and prosecution.[59] Mike Wendland's report in the *Detroit Free Press* highlights the operational efficiency of a particular spam company that moved its headquarters from the United States to the United Kingdom to avoid detection and prosecution in the United States. The U.K. office controls 190 e-mail servers, 110 of which are located in Southfield, 50 in Dallas and 30 more dispersed throughout Canada, China, Russia and India.[60] Each computer is reportedly capable of sending 650,000 messages per hour, and more than a billion per day, all routed through overseas Internet companies who readily provide bandwidth.[61] The report also underscores the jurisdictional problem that plagues spam litigation. Spam companies could set up businesses in countries where there is no regulation, and direct spams at countries where spam is regulated. This scenario renders national legislation ineffectual. For instance, the European Union now knows that the bulk of spams clogging European inboxes are from outside of Europe.[62]

III. REGULATION: A CONUNDRUM

> "The great difficulty of legislation on this subject lies in putting an end to the liberty of fraud without affecting the freedom of commerce."[63]

Regulating the Internet is a tricky affair. The very idea frequently invokes polemical views that are the hallmarks of Internet governance

---

57. See Mike Wendland, *Spam King Lives Large off Others' Emails Troubles*, DETROIT FREE PRESS, *at* http://www.freep.com/money/tech/mwend22_20021122.htm (Nov. 22, 2002).

58. *Id.*

59. *See id.*

60. *Id.*

61. *Id.*

62. *See* Spam Communication, *supra* note 12, at 28. It is said that 90% of Europe's spam problem originates in the United States. *See United States Set to Legalize Spamming on January 1, 2004*, *at* http://www.spamhaus.org/news.lasso?article=150 (Nov. 22, 2003).

63. This quotation related to the challenge of regulating adulterated drugs in nineteenth-century Britain. It has a comparable significance today for spam regulation worldwide. *See* HOUSE OF COMMONS SELECT COMMITTEE ON ADULTERATION OF FOODS, DRINKS AND DRUGS, THIRD REPORT, 1856, 56-7, at 253; JOHN ABRAHAM, SCIENCE, POLITICS AND THE PHARMACEUTICAL INDUSTRY: CONTROVERSY AND BIAS IN DRUG REGULATION 41 (1995).

discourses.[64] There are those who are completely opposed to Internet regulation on fears that such control or regulation could impinge free speech.[65] There are others who favor self-regulation,[66] or technical governance for the cyberspace.[67] They fear that legislation tends to be proactive and could be out of synch with the rapidly advancing and dynamic technology that the Internet represents.[68] The reality however, is that Internet governance is a mixture of self-regulation, technical measures control, and governmental regulation.[69] The real long term challenge is how best to deploy the three strategies to effectively contain spam, a primary objective of this Article.

The antecedence of Internet regulation in the United States is pretty grim, with earlier attempts scuttled by the First Amendment. One regulation that ran into the First Amendment constitutional quagmire was the Communications Decency Act.[70] The Child Online Protection Act of 1998 was to share the same fate in the United States Supreme Court decision of *Ashcroft v. ACLU*.[71] Furthermore, the PROTECT Act of 2003[72] joined the list of failed cyber legislation when it was partially struck down for meddling with the judiciary's sentencing powers for

---

64. In the Internet's formative years, millions of people had shared Tim Berner-Lee's ideal of a highly decentralized universal system of Internet governance. However, the Internet's high propensity for perpetrating crime with complete or near anonymity, and concomitantly low expense and immediacy that transcend time and space, have made regulatory prospects appealing and desirable. FRANDA, *supra* note 2, at 21-23.

65. For instance, the Center for Democracy and Technology and the Citizens Internet Empowerment Coalition (comprising library and civil liberties groups, online service providers, newspapers, book, magazine and recording industry associations, and thousands of individual Internet users) are strong advocates of free speech on the Internet. They reject broadcast-style content regulation of the Internet as evidenced by the Communications Decency Act; and contend that consumer empowerment should be the solution to Internet governance. The Supreme Court struck down the Act on grounds that it impinges the First Amendment and "places an unacceptably heavy burden on protected speech." *See* Reno v. ACLU, 521 U.S. 844, 882 (1997).

66. *See* STUART BIEGEL, BEYOND OUR CONTROL? CONFRONTING THE LIMITS OF OUR LEGAL SYSTEM IN THE AGE OF CYBERSPACE 3 (2001); Neil W. Netanel, *Cyberspace Self-Governance: A Skeptical View from Liberal Democratic Theory*, 88 CAL. L. REV. 395, 397-404 (2000). The author argues that cyberspace self-governance would ultimately fail. *Id.* at 403.

67. *See* LAWRENCE LESSIG, CODE AND OTHER LAWS OF THE CYBERSPACE 3 (1999). Lessig's central thesis is that cyberspace regulation will be determined more by its architecture, or code, than by governmental regulation. *See also* John P. Barlow, *A Declaration of the Independence of Cyberspace*, *at* http://www.eff.org/misc/publications/John_Perry_Barlow/Barlow_0296.declaration.txt (Feb. 9, 1996).

68. Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199, 1200-05 (1998).

69. *See* Jose MA. Emmanuel A. Caral, *Lessons from ICANN: Is Self-Regulation of the Internet Fundamentally Flawed?*, 12 INT'L J.L. & INFO. TECH. 1, 1 (2004).

70. *Reno*, 521 U.S. at 859-60.

71. 124 S. Ct. 2783 (2004).

72. Prosecutorial Remedies and Other Tools to End the Exploitation of Children Today Act of 2003 (PROTECT ACT), Pub. L. No. 108-21, 117 Stat. 650 (2003).

child offenders, in a separation-of-powers constitutional challenge.[73] Given these failed attempts at cyberspace legislation in the United States, it is understandable that Congress tried to avoid running afoul of the First Amendment by consciously maintaining an even balance between freedom of expression (which is crucial to e-commerce, commercial speech, and noncommercial political speech success) and the sanctity and privacy of Internet users, with the CAN-SPAM Act of 2003.[74]

This delicate balancing act appears to permeate the CAN-SPAM Act. For instance, despite Congressional findings that some commercial e-mails are a mix of pornography and deception, often with misleading subject lines designed to induce recipients to read unsolicited mail,[75] the Act nevertheless allows concessions such as the "opt-out" nonconsent based approach to e-mail traffic, which analysts believe gives spammers the upper hand.[76] This balancing act is however justified to accommodate legitimate e-marketers[77] whose advertising outreach could be diminished

---

73. Sections 401(*l*)(1) and (2) of the PROTECT Act require a report by the Justice Department to Congress of any downward departure, other than one for substantial assistance, setting forth the case, facts, the identity of the district court judge, the stated reason for the departure, and the parties' position with respect to the departure. Section 401(j)(3) authorized the Justice Department to promulgate its own policies and procedures for reporting to Congress. *See* United States v. Schnepper, 302 F. Supp. 2d 1170, 1181-82 (D. Haw. 2004). Schnepper was convicted by a jury of five counts of using the Internet to knowingly attempt to transfer obscene material and one count of using the Internet to knowingly attempt to persuade, induce, and entice an individual of less than 18 years of age to engage in sexual activity. *Id.* at 1176. He moved for imposition of sentence without reference to the Sentencing Guidelines, challenging the constitutionality of Guidelines as amended by the PROTECT ACT. *Id.* Judge Kay held:

> Because PROTECT ACT . . . and the amendment to . . . the Guidelines Manual retroactively operate to substantially disadvantage Schnepper, he cannot be denied a downward departure solely because the asserted ground is no longer available for the crimes for which he was convicted. . . . Conversely, new statutory provisions and amendments to the Guidelines Manual that . . . do not "create a sufficient risk of increasing the measure of punishment attached to the covered crimes," may be applied in Schnepper's sentencing without constitutional concern.

Id. at 1186-87 (internal citations omitted); *see also* United States v. Mendoza, No. CR 03-730 DT, 2004 WL 1191118 (C.D. Cal. Jan. 12, 2004). The United States District Court for the Central District of California held that the statute's requirement of reports on individual judges who grant downward departures from the United States Sentencing Guidelines "chills and stifles judicial independence to the extent that it is constitutionally prohibited." *Mendoza*, 2004 WL 1191118, at *6.

74. CAN-SPAM Act §§ 2-14, 15 U.S.C.A. §§ 7701-7713 (Supp. VI 2004).

75. *See* 15 U.S.C.A. § 7701.

76. *See* Adam Mossoff, *Spam—Oy, What a Nuisance!*, 19 BERKELEY TECH. L.J. 625, 636-37 (2004); Jeffrey D. Sullivan & Michael B. De Leeuw, *Spam After CAN-SPAM: How Inconsistent Thinking Has Made a Hash Out of Unsolicited Commercial E-mail Policy*, 20 SANTA CLARA COMPUTER & HIGH TECH. L.J. 887, 887-88 (2004).

77. *See* Berman & Bruening, *supra* note 11.

by the "opt-in" scheme, which gives spam recipients a relatively stronger control on what spam would grace their inboxes.

Curiously, the Act has attracted criticism from those who perceive the Act as too weak to combat spam, as well as those who feel that it violates free speech.[78] The CAN-SPAM Act is thus hedged in, by flailing criticisms of being too weak and too strong, from two opposing groups with different expectations. This is symptomatic of the attendant dissonance in the general discourse on Internet governance, and underscores the absence of unanimity of ideas on the best approach to combating spam.

Part IV will analyze antispam regulations in both the United States and European Union. Their differences will be highlighted, while their prospects for success will be evaluated in the context of relevant international, regional and national legal regimes for Internet governance. The analysis will also examine the relevance of both regulations in the light of recent judicial enforcements as well as the importance of technical antispam measures in the fight against the menace of spam.

IV. ANTISPAM REGULATIONS IN THE UNITED STATES

In the United States, spam is regulated both at the state and federal levels. Over 30 states have in place antispam legislations. These include California, Illinois, Washington, Virginia, Wisconsin, and Delaware.[79] The CAN-SPAM Act has nationwide coverage. Congress acknowledges states' antispam legislation, but finds that their provisions are disparate, and that law-abiding citizens could be confused on which state law to comply with, since e-mail addresses do not specify geographic locations.[80] Congress is justified in doubting the effectiveness of

---

78. *See* Charles H. Kennedy & Christine E. Lyon, *The CAN-SPAM Act of 2003: A New Regime for Email Advertising*, COMPUTER & INTERNET LAW. (Aspen Publishers, New York, NY), Feb. 2004, at 1. The authors noted that the Act has several pitfalls, is ambiguous, and could entrap legitimate businesses that use e-mail as a marketing tool. They reasoned that it would have little impact on unethical businesses that could easily move their servers offshore to avoid the reach of the law. *Id.*; Jim Raposa, *Stop Anti-Spam Laws*, EWEEK ENTERPRISE NEWS & REV., Aug. 11, 2003, *available at* http://www.eweek.com/article2/0%2C3959%2C1216876%2C00.asp.

79. *See* CAL. BUS. & PROF. CODE § 17529 (West 2003); 815 ILL. COMP. STAT. 511 (2000); WASH. REV. CODE § 19.190.060 (2003); VA. CODE ANN. § 18.2-152.3:1 (Michie 2003); WIS. STAT. § 944.25 (2001); DEL. CODE ANN. tit. 11, § 937 (2003).

80. Section 2(a)(11) of the CAN-SPAM Act states:

> Many States have enacted legislation intended to regulate or reduce unsolicited commercial electronic mail, but these statutes impose different standards and requirements. As a result, they do not appear to have been successful in addressing the problems associated with unsolicited commercial electronic mail, in part because, since an electronic mail address does not specify a geographic location, it can be extremely

heterogeneous state spam laws in combating spam which transcends state borders. The first obvious problem is interstate jurisdiction on spam governance. The absence of geographic boundaries in cyberspace has serious implications for Internet governance both nationally and internationally.[81] Unlike the "real world," where geographic borders shape law making and enforcement, cyberspace is fluid, ubiquitous, and lacks the territoriality that defines jurisdictional issues on choice of law and forum for dispute resolution. The legal ramifications of amorphous structural paradigms in cyberspace are highlighted by David R. Johnson and his coauthors, as follows:

> The rise of the global computer network is destroying the link between geographical location and: (1) the power of local governments to assert control over on-line behavior; (2) the effects of on-line behavior on individuals or things; (3) the legitimacy of a local sovereign's efforts to regulate global phenomena; (4) the ability of physical location to give notice of which sets of rules apply. The Net thus radically subverts the system of rule-making based on borders between physical spaces, at least with respect to the claim that cyberspace should naturally be governed by territorially defined rules.[82]

The authors' antidote to jurisdictional problems posed by cyberspace is that it should be construed "as a distinct 'place' for purposes of legal analysis by recognizing a legally significant border between Cyberspace and the 'real world.'. . . Treating Cyberspace as a separate 'space' to which distinct laws apply should come naturally."[83] This proposition however raises many more questions than answers to the jurisdictional problems: Who should be responsible for drafting of the "distinct" cyberspace law? Should it be an international cyber-specific law ratified by the committee of nations? Or should cyberspace self-regulate, by applying the prevailing customary practice on the net? Since disputes are inevitable in all human endeavors, which body should be responsible for settling such disputes? Should we look up to the real world for

---

> difficult for law-abiding businesses to know with which of these disparate statutes they are required to comply.

15 U.S.C.A. § 7701(a)(11).

81. *See* David R. Johnson & David Post, *Law and Borders: The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996). The authors argue that geographic boundaries impact law in several ways. First, they determine who has the power to exercise physical control over physical space and people and things residing in that space; second, they determine where the effects of law are felt; third, they determine the legitimacy of the law makers; and fourth, they give notice or sign posts about the state of the law, and where the rules differ from one geographical location to the other. *Id.* at 1367-68.

82. *Id.* at 1370.

83. *Id.* at 1378-79.

traditional arbiters, or look further in the network of computers for some sort of cyber court?

The concept of an ethereal cyberspace, deserving of a separate jurisdiction, has been described as a "cyberspace fallacy."[84] In dismissing the idea of a separate jurisdiction for cyberspace, Christopher Reed argued:

> If this conception of cyberspace as a separate jurisdiction were well-founded, . . . [c]ompeting claims of national law would be denied on the ground that the transaction occurred exclusively within the jurisdiction of cyberspace, and is thus governed by its laws, customs and practices. The problem with cyberspace is that its constituent elements, the human and corporate actors and the computing and communications equipment through which the transaction is effected, all have real-world existence and are located in one or more physical world legal jurisdictions. These corporeal elements of cyberspace are sufficient to give national jurisdictions a justification for claiming jurisdiction over, and the applicability of their laws to, an internet transaction.[85]

Reed advocates the application of the principle of localization to jurisdictional issues in cyberspace.[86] Localization, he explains, involves ascertaining where a human actor was situated when the relevant act was performed.[87] The localization principle, which is not entirely a new concept, offers a more realistic and pragmatic solution to cyberspace spam governance. It is the underlying concept for managing disputes in the traditional transnational contracts transactions, in the absence of agreements on choice of law between contracting parties.[88] In theory, this principle should work for transnational enforcement of spam laws. For instance, it should be theoretically possible to prosecute or file a lawsuit in Stockholm for unsolicited electronic mail that violates Swedish law though they originate in Hawaii or Beijing. The downside is, not every country has a spam law in 2005. Moreover, transnational spam laws are characteristically disparate, as evidenced by the fundamental differences between the U.S. CAN-SPAM Act and Europe's e-Privacy Directive. This is a vulnerable fault line that could potentially prejudice the

---

84. *See* CHRISTOPHER REED, INTERNET LAW AND MATERIALS 188 (2000).

85. *Id.*

86. *Id.*

87. *Id.*

88. *See* International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), Oct. 26, 1961, art. 4, 496 U.N.T.S. 44, 46; Convention on Jurisdiction and Enforcement of Judgments in Civil and Commercial Matters, Sept. 27, 1968, arts. 2-3, 5, 13-15, 29 I.L.M. 1413, 1418-22 [hereinafter Brussels Convention].

acceptance of spam judgments by national courts in foreign jurisdictions. This point is canvassed in greater detail in the section on transnational enforcement of national spam laws in Part V of this Article.[89]

In the United States, the principle of localization has been applied in interstate enforcement of state spam laws.[90] A Washington court assumed personal jurisdiction on spam that emanated from Oregon, and targeted Washington residents.[91] Increased use of the Internet in the

---

89. *See infra* Part VI.

90. This proposition, however, faces constitutional Commerce Clause and Fourteenth Amendment Due Process Clause hurdles. A state violates the Due Process Clause if it exercises personal jurisdiction over a defendant who does not have adequate contacts with the forum state. *See* World-Wide Volkswagen Corp. v. Woodson, 444 U.S. 286, 291-92 (1980). The fundamentals of due process were highlighted in *Pennoyer v. Neff*, 95 U.S. 714 (1877). Justice Field, who delivered the Court's opinion, held:

> The authority of every tribunal is necessarily restricted by the territorial limits of the State in which it is established. Any attempt to exercise authority beyond those limits would be deemed in every other forum, as has been said by this court, an illegitimate assumption of power, and be resisted as mere abuse.

Id. at 720. He predicated the limitation on territorial powers of states courts on the following two principles: "One of these principles is, that every State possesses exclusive jurisdiction and sovereignty over persons and property within its territory. . . . The other principle . . . is, that no state can exercise direct jurisdiction and authority over persons or property without its territory." *Id.* at 722. *But see* Int'l Shoe Co. v. Washington, 326 U.S. 310 (1945). The "minimum contacts" theory was later formulated by the Supreme Court for determining the propriety of a state court's jurisdiction over a nonresident defendant. The theory would examine whether "the maintenance of the suit . . . offended traditional notions of fair play and substantial justice." *Id.* at 316. The lawsuit was filed by the state of Washington for the defendant's failure to contribute to its employment compensation fund. The company challenged jurisdiction on grounds that it was not doing business in the state. Although the company's headquarters were outside of Washington, it employed about 13 resident salesmen who solicited orders in the state. The Court held that the company was engaged in business sufficient to establish jurisdiction predicted on a new theory, one of minimum contacts. *Id.*; *see* ALLAN REED, ANGLO-AMERICAN PERSPECTIVES ON PRIVATE INTERNATIONAL LAW 340-48 (2003).

91. *See* State v. Heckel, 24 P.3d 404, 406 (Wash.), *cert. denied*, 534 U.S. 997 (2001). Heckel, an Oregon resident, was marketing a forty-six page online booklet entitled "How to Profit from the Internet." The booklet described how to set up online promotional business, acquire e-mail accounts, and send unsolicited electronic mails. From June 1998, Heckel marketed the booklet online by sending between 100,000 to 1,000,000 unsolicited electronic messages per week. He charged $39.95 per booklet, and sold between thirty to fifty copies per month. *Id.* The order form included the Salem, Oregon, mailing address of Heckel's company Natural Instincts. Heckel's messages contained misleading subject lines and false transmission paths. This violated Washington's Consumer Protection Act. *Id.* at 407. After attempting to get Heckel to stop sending his marketing e-mails, the state of Washington filed suit against him, alleging that his sending of unsolicited commercial e-mails violated Washington's Commercial Electronic Mail Act, WASH. REV. CODE § 19.190 (2001). *Id.* The Washington Supreme Court held that the Act limits the harm that unsolicited commercial e-mails cause Washington residents. The Act prohibits the use of misleading subject lines or transmission path of any commercial e-mail message sent to Washington residents or from a computer located in Washington. The Court found further that the local benefits of the Act outweigh any conceivable burdens it places on the sending of unsolicited commercial e-mails. *Id.* at 409. The Court concluded that the Act did not

United States has engendered a corresponding proliferation of Internet-related lawsuits, which often involve interstate jurisdictional issues.[92] U.S. courts have adapted the traditional twin personal jurisdictional tests of physical presence in the forum and purposeful availment, to cyberspace jurisdictional disputes.[93] In recent cases, courts, employing the purposeful availment test, assumed personal jurisdiction over defendants who ran a Web site that was accessible to everyone, including people in the forum state, or defendants who transmitted unsolicited electronic messages to recipients in the forum state, in contravention of state spam laws.[94]

The fact that states are resorting to traditional jurisdictional tests to assume personal jurisdiction over defendants in interstate spam litigation underscores Congress's concerns that law-abiding citizens could be confused as to which of the disparate state spam laws to comply with, because e-mail addresses do not specify geographic locations. This is the rationale for the CAN-SPAM Act's preemption of state spam laws, except when they prohibit "falsity or deception" in commercial e-mail messages. The preemptive section 8(b)(1) of the CAN-SPAM Act provides:

> This chapter 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, except to the extent that any such statute, regulation, or rule prohibits falsity or deception in any portion of a commercial electronic mail message or information attached thereto.[95]

This provision seeks to harmonize state legislation with the federal law. However, a state spam law may not be preempted if it prohibits "falsity or deception" in commercial electronic e-mails.[96] It is still theoretically

---

violate the Dormant Commerce Clause of the U.S. Constitution, and distinguished *American Libraries Ass'n v. Pataki*, 969 F. Supp. 160 (S.D.N.Y. 1997). *Id.* at 412; *see infra* notes 136-143 and accompanying text.

92. Dan L. Burk, *Federalism in Cyberspace*, 28 CONN. L. REV. 1095, 1096-97 (1996).

93. *See, e.g.*, Bensusan Rest. Corp. v. King, 126 F.3d 25, 27 (2d Cir. 1997). The minimum contacts theory of *International Shoe* was interpreted in *Hanson v. Denckla*, 357 U.S. 235 (1958), to mean that "there must be some act by which the defendant purposefully avails itself of the privilege of conducting activities within the forum state." *Id.* at 253. Purposeful availment would cover both the defendant's deliberate conducts and the effects of his conducts. *See* Calder v. Jones, 465 U.S. 783, 789-90 (1984).

94. *See, e.g.*, Maritz, Inc. v. Cybergold, Inc., 947 F. Supp. 1328, 1330 (E.D. Mo. 1996). In *CompuServe, Inc. v. Patterson*, 89 F.3d 1257 (6th Cir. 1996), the court held that the defendant was properly subjected to personal jurisdiction where the defendant had electronically transmitted his product to the forum state and entered into a contract that had a connection with the forum state. *See also Heckel*, 24 P.3d at 406.

95. 15 U.S.C.A. § 7707(b)(1) (Supp. VI 2004).

96. *Id.*

possible for a state attorney general to prosecute spammers under state spam legislation if the law prohibits fraudulent unsolicited commercial e-mails. However, the right of a state attorney to prosecute is still subject to section 7(f)(8), which provides:

> If the Commission, or other appropriate Federal agency under subsection (b) of this section, has instituted a civil action or an administrative action for violation of this chapter, no State attorney general, or official or agency of a State, may bring an action under this subsection during the pendency of that action against any defendant named in the complaint of the Commission or the other agency for any violation of this chapter alleged in the complaint.[97]

In order to avoid conflict with federal agencies on spam governance, other states should follow the example of California's antispam statute which provides that the relevant section, or any part of it, shall become inoperative when "federal law is enacted that prohibits or otherwise regulates the transmission of unsolicited advertising by electronic mail."[98] This has rendered federal preemption of California spam law moot, since the coming into force of the CAN-SPAM Act in January 2004. California's stance in this regard is exemplary. There is no point in keeping a statute perpetually under the shadows of preemptive federal legislation. Adopting the California style could ensure a better coordinated front in the fight against spam. However, the CAN-SPAM Act does not preempt nonelectronic mail state laws, such as contract, tort law, or other state laws relating to fraudulent acts or computer crime.[99] It is theoretically feasible that states can still impact spam governance through statutes that are exempt from preemption, and through common law tort of trespass, as exemplified by *CompuServe*[100] and *Intel Corp. v. Hamidi*.[101]

The CAN-SPAM Act prohibits fraud and allied activities related to e-mails.[102] These include: accessing a protected computer without permission, and intentionally initiating the transmission of multiple commercial e-mail messages from such a computer;[103] using a protected computer for transmitting multiple commercial electronic messages, with the intention of deceiving or misleading recipients or any ISPs as to the

---

97. *Id.* § 7706(f)(8).

98. Ferguson v. Friendfinders, Inc., 115 Cal. Rptr. 2d 258, 260 (Ct. App. 2002) (quoting CAL. BUS. & PROF. CODE § 17538.4 (West 2004)).

99. 15 U.S.C.A. § 7707(b)(2)(B).

100. 962 F. Supp. 1015, 1022 (S.D. Ohio 1997).

101. 71 P.3d 296, 304-07 (Cal. 2003).

102. 15 U.S.C.A. § 7703.

103. 18 U.S.C.A. § 1037(a)(1) (Supp. VI 2004).

origin of such messages;[104] material falsification of header information in multiple commercial electronic messages and intentionally initiating the transmission of such messages.[105] Other prohibitions include: a register that uses information which "materially falsifies the identity of the actual registrant, for five or more electronic mail accounts or online user accounts or two or more domain names, and intentionally initiates the transmission of multiple commercial electronic mail messages from any combination of such accounts or domain names,"[106] falsely representing "oneself to be the registrant or the legitimate successor to the registrant of 5 or more Internet Protocol addresses," and intentionally sending multiple commercial electronic messages from such addresses.[107]

The penalties for conviction for any of these offenses is a fine or imprisonment for not more than 5 years or both, if the offense is committed in pursuance of any felony under the laws of the United States or of any state, or the defendant has had previous convictions for sending multiple commercial e-mail messages, or unauthorized access to any computer system.[108]

Furthermore, the CAN-SPAM Act prohibits the transmission to a protected computer, of a commercial electronic message or a transactional or relationship message that is false or misleading.[109] Moreover, the Act prohibits use of deceptive subject lines,[110] and requires inclusion of a functioning return electronic address[111] by senders of unsolicited commercial electronic messages. Such a return address should bear a clear and conspicuous message requesting not to receive future commercial electronic messages from that sender to the e-mail address where the message was received.[112] However, if such a return address is unable to function temporarily due to technical faults beyond the control of the sender, the technical glitch will not prejudice compliance with the law provided it is rectified within a reasonable

---

104. *Id.* § 1037(a)(2).

105. *Id.* § 1037(a)(3).

106. *Id.* § 1037(a)(4). Spammers often use stolen identities to disguise the origin of spam. They would use these identities to sign up for e-mail accounts, and forge e-mail headers to disguise the origin of the mails, and then send millions of unsolicited commercial electronic mails. *See, e.g.*, *Buffalo Spammer Hit with Arrest and $16.4 Million Judgment*, COMPUTER & INTERNET LAW. (Aspen Publishers, New York, NY), July 2003, at 35 [hereinafter *Buffalo Spammer*].

107. 18 U.S.C.A. § 1037(a)(5).

108. *Id.* § 1037(b)(1)(A)-(B).

109. 15 U.S.C.A. § 7704(a)(1)(A)-(C) (Supp. VI 2004).

110. *Id.* § 7704(a)(2).

111. *Id.* § 7704(a)(3).

112. *Id.* § 7704(a)(3)(A)(i).

time.[113] Following the objection of a recipient of an unsolicited commercial electronic message, the sender is prohibited from initiating future transmission of any unsolicited electronic mail message to the recipient.[114] However, subsequent affirmative consent would override the earlier objection.[115]

In April 2004, federal authorities instituted the first criminal lawsuits under the CAN-SPAM Act in *FTC v. Phoenix Avatar LLC*,[116] and *United States v. Lin*.[117] The FTC charged Phoenix Avatar LLC and its Detroit-based agents for allegedly flooding the Internet with close to half a million e-mail messages.[118] In *Lin*, court papers showed that the defendants allegedly used falsehood and deception to hide the origin of their spam messages, and obscured their identities by using innocent third-party e-mail addresses.[119] They also hawked fraudulent weight-loss patches from which they raked in about $100,000 monthly from product sales.[120]

Significantly, the CAN-SPAM Act requires the labeling of sexually oriented e-mails[121] and a clear and conspicuous identification of an unsolicited commercial electronic message as an advertisement or solicitation.[122] Moreover, it requires a clear and conspicuous notice that the recipient could opt-out of the future receipt of unsolicited commercial electronic messages;[123] and a valid physical address of the sender.[124] The following paragraphs will analyze the extent to which the CAN-SPAM Act has balanced the conflicting rights of spam senders and receivers, the prospects for the Act's success, and the potential for conflicts with certain civil liberties as guaranteed by the United States Constitution.

---

113. *Id.* § 7704(a)(3)(C).
114. *See id.* § 7704(a)(4)(A).
115. *See id.* § 7704(a)(4)(B).
116. No. 04 C 2897, 2004 WL 1746698, at *1 (N.D. Ill. July 30, 2004).
117. No. 04-80383 (E.D. Mich. filed Apr. 29, 2004).
118. *See Feds Charge Four Under New Anti-Spam Law*, ANDREWS COMPUTER & INTERNET LITIG. REP. (Andrews Publications, Wayne, PA), May 18, 2004, at 9.
119. *Id.*
120. *Id.*
121. 15 U.S.C.A. § 7704(d) (Supp. VI 2004).
122. *Id.* § 7704(a)(5)(A)(i). This notice would not be necessary if the recipient had given prior affirmative consent that they were willing to receive unsolicited electronic commercial messages. *Id.* § 7704(a)(5)(B).
123. *Id.* § 7704(a)(5)(A)(ii).
124. *Id.* § 7704(a)(5)(A)(iii).

V. THE CAN-SPAM ACT: CHALLENGES AND PROSPECTS FOR SUCCESS

Spam regulation in the United States has raised some constitutional issues. They include: the extraterritorial effects of states' spam laws on the Commerce Clause, the validity of the advertising labeling requirement vis-à-vis the First Amendment, and the burden of accurate header information vis-à-vis the right to anonymity. The following paragraphs will examine these issues *in seriatim* through the case law prism, and then discuss the challenges and prospects for success of the CAN-SPAM Act and states' spam laws in the United States.

A. The Dormant Commerce Clause and State Spam Laws

The first constitutional issue to be discussed is the future of states spam laws vis-à-vis the Commerce Clause. As noted above, states can still enforce their spam laws because the CAN-SPAM Act does not completely override states' spam laws. It will operate concurrently and will not preempt state spam laws that prohibit false and deceptive commercial e-mail messages.[125] However, a state attorney general's power to prosecute a defendant for transmitting false or deceptive commercial e-mail messages is automatically put in abeyance if the FTC or other federal agency decides to file a civil lawsuit against the defendant pursuant to the relevant provisions of the CAN-SPAM Act.[126]

Invariably, commercial e-mail messages relate to commerce. It is therefore inevitable that issues would be raised about the propriety of state spam laws in the context of the Commerce Clause of the United States Constitution. Article 1, Section 8, Clause 3 of the Constitution empowers Congress "[t]o regulate Commerce with foreign Nations, and among the several States, and with the Indian Tribes."[127] In *Healy v. The Beer Institute*, the Supreme Court held: "This affirmative grant of authority to Congress also encompasses an implicit or 'dormant' limitation on the authority of the States to enact legislation affecting interstate commerce."[128] The Commerce Clause is the basis for decades' worth of jurisprudence that prohibits states from regulating in ways that

---

125. *See supra* notes 95-98 and accompanying text.

126. 15 U.S.C.A. § 7706(f)(8).

127. U.S. CONST. art. 1, § 8, cl. 3.

128. 491 U.S. 324, 326 n.1 (1989). In *Healy*, the Supreme Court struck down provisions of a Connecticut statute that required out-of-state shippers of beer to affirm that their posted prices for products sold to Connecticut wholesalers were no higher than the prices at which those products were sold in States bordering Connecticut. The *Healy* Court found that Connecticut's price affirmation statute violated the dormant Commerce Clause because it discriminated against brewers and shippers of beer engaged in interstate commerce, and directly controlled commerce occurring wholly outside the state. *Id.* at 491.

hamper interstate commerce,[129] even in the absence of Congressional action.[130] It has been applied in various commercial settings by the Supreme Court with varied outcomes (occasioned largely by the peculiar facts of each case) that either prohibited the state legislation in question as unconstitutional, or that absolved it of any contravention of the Commerce Clause.[131]

In recent times, litigants have invoked the dormant Commerce Clause to combat states' regulations of pornography and spam on the Internet. *Ferguson* was such an example.[132] The plaintiff, an e-mail recipient, sued the defendants for sending him deceptive and misleading unsolicited e-mails in contravention of California law.[133] The defendants challenged the lawsuit, on grounds that the statute in question violated

---

129. The Supreme Court has invoked the dormant Commerce Clause to strike down state legislation that was perceived as anticompetitive, discriminatory, and prejudicial to the interstate free flow of goods and services. The dormant Commerce Clause also generally stands for the proposition that states cannot regulate commerce in certain ways, but the states and Congress retain concurrent power to regulate commerce in many other ways. This is the usual interpretation in the long line of cases by the Supreme Court in its decisions regarding the Commerce Clause. One of the early cases was *Cooley v. Board of Wardens*, 53 U.S. 299 (1851). The main issue in the case was whether an 1803 Pennsylvania law that required that all ships entering or leaving the Port of Pennsylvania to hire a local pilot violated the Commerce Clause of the Constitution. Justice Curtis, who wrote the majority opinion, found that the Commerce Clause of the constitution was not violated. The Court held:

> But, having previously stated that, in this instance, the law complained of does not pass the appropriate line which limits laws for the regulation of pilots and pilotage, the suggestion, that this law levies a duty on tonnage or on imports or exports is not admissible; and, if so, it also follows that this law is not repugnant to the first clause of the eighth section of the first article of the Constitution, which declares that all duties, imposts, and excises shall be uniform throughout the United States; for, if it is not to be deemed a law levying a duty, impost, or excise, the want of uniformity throughout the United States is not objectionable. Indeed the necessity of conforming regulations of pilotage to the local peculiarities of each port, and the consequent impossibility of having its charges uniform throughout the United States, would be sufficient of itself to prove that they could not have been intended to be embraced within this clause of the Constitution; for it cannot be supposed uniformity was required when it must have been known to be impracticable.

Id. at 314.

130. *See* CTS Corp. v. Dynamics Corp. of Am., 481 U.S. 69, 87 (1987).

131. For some of the early cases on Dormant Commerce Clause vis-à-vis state legislations, see *Maine v. Taylor*, 477 U.S. 131 (1986); *Brown-Forman Distillers Corp. v. New York State Liquor Authority*, 476 U.S. 573 (1986); *Hughes v. Oklahoma*, 441 U.S. 322 (1979); *City of Philadelphia v. New Jersey*, 437 U.S. 617 (1978); *Hunt v. Washington Apple Advertising Commission*, 432 U.S. 333 (1977); *Dean Milk Co. v. City of Madison*, 340 U.S. 349 (1951); *H.P. Hood & Sons, Inc. v. Du Mond*, 336 U.S. 525 (1949); *Edwards v. California*, 314 U.S. 160 (1941); *Baldwin v. G.A. F. Seelig Inc.*, 294 U.S. 511 (1935).

132. 115 Cal. Rptr. 2d 258 (Ct. App. 2002).

133. *See* CAL. BUS. & PROF. CODE § 17538.4 (West 2004).

the dormant Commerce Clause of the United States Constitution.[134] The court found that section 17538.4 of the California Business and Professions Code did not discriminate against or directly regulate or control interstate commerce. Consequently, the section did not violate the Commerce Clause, because it served a legitimate local public interest. In dismissing the respondent's argument that the California law had an impermissible extraterritorial reach, the court noted inter alia that "to the extent that section 17538.4 requires truthfulness in advertising, it does not burden interstate commerce at all, but actually 'facilitates it by eliminating fraud and deception.'"[135] The court distinguished *American Libraries Ass'n v. Pataki*[136] in arriving at its decision. It found that unlike the New York statute in *American Libraries*, the California statute "does not regulate the Internet or Internet use per se. It regulates individuals and entities who (1) do business in California, (2) utilize equipment located in California and (3) send UCE to California residents. The equipment used by electronic-mail service providers does have a geographic location. E-mail recipients are people or businesses who function in the real world and have a geographic residence."[137]

Although this paragraph is focused on Commerce Clause effects on states' spam laws, a brief review of the United States District Court for the Southern District of New York's decision in *American Libraries* on New York's Internet pornographic legislation is appropriate due to its central significance, and the comparative lessons it holds for the discourse on interstate cyberspace spam governance. The plaintiffs and other organizations that used the Internet to communicate challenged the constitutionality of a New York statute that criminalized the use of a computer to disseminate obscene or indecent materials to minors.[138] The

---

134. U.S. CONST. art. 1, § 8, cl. 3.

135. *Ferguson*, 115 Cal. Rptr. 2d at 268 (quoting State v. Heckel, 24 P.3d 404, 411 (Wash. 2001)).

136. 969 F. Supp. 160 (S.D.N.Y 1997).

137. *Ferguson*, 115 Cal. Rptr. 2d at 265.

138. *See* N.Y. PENAL LAW § 235.21(3) (McKinney 1997). It provides as follows:

> A person is guilty of disseminating indecent material to minors in the second degree when:
>
> 1. With knowledge of its character and content, he sells or loans to a minor for monetary consideration:
>
> (a) Any picture, photograph, drawing, sculpture, motion picture film, or similar visual representation or image of a person or portion of the human body which depicts nudity, sexual conduct or sado-masochistic abuse and which is harmful to minors; or
>
> (b) Any book, pamphlet, magazine, printed matter however reproduced, or sound recording which contains any matter enumerated in paragraph (a) hereof, or explicit or detailed verbal descriptions or narrative accounts of

grounds of the challenge were alleged violations of the First Amendment and the Commerce Clause. On a motion for a preliminary injunction to bar the governor and Attorney General of New York from enforcing the statute, the district court judge found that the Act clearly applied to interstate and intrastate communications,[139] and that the type of communications involved constituted commerce.[140] The court further noted that the Act potentially had overreaching effects on other states due to the Internet's inherent ubiquity. This, according to the court, could lead to the criminalization in New York of conduct that could be legal in other states.[141] The court reasoned that this could

> subordinate the user's home state's policy—perhaps favoring freedom of expression over a more protective stance—to New York's local concerns.

> sexual excitement, sexual conduct or sado-masochistic abuse, and which, taken as a whole, is harmful to minors; or
>
> 2. Knowing the character or content of a motion picture, show or other presentation which, in whole or in part, depicts nudity, sexual conduct or sado-masochistic abuse, and which is harmful to minors, he:
>
> (a) exhibits such motion picture, show or other presentation to a minor for monetary consideration; or
>
> (b) sells to a minor an admission ticket or pass to premises whereon there is exhibited or to be exhibited such motion picture, show or other presentation; or
>
> (c) admits a minor for a monetary consideration to premises whereon is exhibited or to be exhibited such motion picture or show or other presentation; or
>
> 3. Knowing the character and content of communication which, in whole or in part, depicts actual or simulated nudity, sexual conduct or sado-masochistic abuse, and which is harmful to minors, he intentionally uses any computer communication system allowing the input, output, examination or transfer of computer data or computer programs from one computer to another, to initiate or engage in such communication with a person who is a minor.
>
> Disseminating indecent materials to minors is a class E felony.

Id.

139. *Am. Libraries*, 969 F. Supp. at 168.

140. In linking the Act to commerce, the court found:

> Commercial use of the Internet, moreover, is a growing phenomenon. In addition, many of those users who are communicating for private, noncommercial purposes are nonetheless participants in interstate commerce by virtue of their Internet consumption. Many users obtain access to the Internet by means of an on-line service provider, such as America Online, which charges a fee for its services. . . . The inescapable conclusion is that the Internet represents an instrument of interstate commerce, albeit an innovative one; the novelty of the technology should not obscure the fact that regulation of the Internet impels traditional Commerce Clause considerations. . . . The . . . scrutiny of the Act under the Commerce Clause is entirely appropriate. . . . [T]he Act cannot survive such scrutiny, because it places an undue burden on interstate traffic, whether that traffic be in goods, services, or ideas.

Id. at 173 (internal citations omitted).

141. *Id.* at 170.

> New York has deliberately imposed its legislation on the Internet and, by doing so, projected its law into other states whose citizens use the Net. This encroachment upon the authority which the constitution specifically confers upon the federal government and upon the sovereignty of New York's sister states is per se violative of the Commerce Clause.[142]

The court's finding was predicated on the Internet's ubiquity, which, according to the court,

> is wholly insensitive to geographic distinctions. In almost every case, users of the Internet neither know nor care about the physical location of the Internet resources that they access. Internet protocols were designed to ignore rather than document geographic location; while computers on the network do have "addresses," they are logical addresses on the network rather than geographic addresses in real space. The majority of Internet addresses contain no geographic clues and, even where an Internet address provides such a clue, it may be misleading. . . . Moreover, no aspect of the Internet can feasibly be closed off to users from another state. An Internet user who posts a Web page cannot prevent New Yorkers or Oklahomans or Iowans from accessing that page and will not even know from what state visitors to that site hail. Nor can a participant in a room prevent other participants from a particular state from joining the conversation. Someone who uses a mail exploder is similarly unaware of the precise contours of the mailing list that will ultimately determine the recipients of his or her message, because users can add or remove their names from a mailing list automatically. Thus, a person could choose a list believed not to include any New Yorkers, but an after-added New Yorker would still receive the message.[143]

American Libraries was a significant victory for First Amendment and free speech advocates. It underscored the inherent extraterritoriality effects as a potential obstacle to the success of the disparate states spam laws. This illustrates the benefits of a federal spam law. Whatever reservations one might have about the CAN-SPAM Act's preemption of state spam laws, it is beyond doubt that the CAN-SPAM Act's homogeneity proffers a solution to the constitutional quagmire that the Commerce Clause posed to the disparate state laws.

For sure, cases involving the Commerce Clause have historically had varied outcomes.[144] The Supreme Court has had occasion to strike

---

142. *Id.* at 177 (internal citations omitted).

143. *Id.* at 170 (internal citations omitted).

144. *Compare* Kraft v. Jacka, 872 F.2d 862, 869 (9th Cir. 1989) (holding that a violation of the Commerce Clause does not deprive an individual of a constitutional right under 42 U.S.C. § 1983) *and* J & J Anderson, Inc. v. Town of Erie, 767 F.2d 1469, 1476-77 (10th Cir. 1985) (same) *with* Consol. Freightways Corp. v. Kassel, 730 F.2d 1139, 1144 (8th Cir. 1984) (holding that the Commerce Clause serves to allocate power rather than secure rights under 42 U.S.C. § 1983).

down or uphold the constitutionality of such legislations in the past, with decisions greatly influenced by the peculiar nature of the state laws in question.[145] In other words, state statutes had historically fallen or survived on the basis of the Supreme Court's perception of their overreaching effects on sister states' commerce, against the background of the Commerce Clause.[146] Since state spam laws also differ in material particulars,[147] it is inevitable that their interpretation would induce disparate decisions by state courts vis-à-vis the Commerce Clause.[148] This would hamstring their effectiveness in spam control, a point that underscores the imperatives for the CAN-SPAM Act's preemption of state spam laws. Although the Washington Supreme Court asserted personal jurisdiction over a spammer from Oregon and declared that Washington's Consumer Protection Act was constitutional vis-à-vis the Commerce Clause (in *State v. Heckel*, as noted earlier in this Article),[149] there was no guarantee that the United States Supreme Court would share a similar view if it were to interpret the constitutionality of Washington's Consumer Protection Act in light of the Commerce Clause. After all, it was a decision of the Washington Supreme Court on the constitutionality of the state of Washington's statute. This is not to suggest however that *Heckel* is bad law or wrongly decided on the facts. Rather, the argument borrows from the familiar trends in the antecedence of the Commerce Clause and state statutes. The latter are historically tendentious; and it is likely, especially in borderline cases, that the Supreme Court would rather embrace the Commerce Clause than a state spam law that exudes the slightest evidence of protectionism or any extraterritoriality effects that could appear to overreach or hinder interstate commerce. The imperatives of federal paradigms, which require balancing the varied interests of the constituent states,[150] make

---

145. *See Am. Libraries*, 969 F. Supp. at 168.

146. *See* Golden State Transit Corp. v. City of Los Angeles, 493 U.S. 103, 110-11 (1989) (discussing the Supremacy Clause and the preemption of state laws in the context of the National Labor Relations Act).

147. For instance, it is said that the state of Virginia has the toughest antispam legislation in the United States with its Virginia Computer Crimes Act, which was signed into law by the Governor on April 29, 2003. The Virginia law raised the penalty to a felony for high-volume unsolicited bulk e-mail. *See Buffalo Spammer*, *supra* note 106, at 34-35.

148. *See* State v. Heckel, 24 P.3d 404, 411-12 (Wash. 2001).

149. *See supra* note 91 and accompanying text.

150. The Supreme Court stated how it would be guided in maintaining a balance between a state statute and the Commerce Clause in *Pike v. Bruce Church, Inc.*, 397 U.S. 137 (1970), as follows:

> Where the statute regulates evenhandedly 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

such an outcome highly inevitable and assured; even where such legislation was characteristically motivated by legitimate local public interests.[151] The CAN-SPAM Act's preeminence over state spam laws can effectively foreclose possible clashes between the disparate states spam laws and the Commerce Clause. The Act transcends the constitutional impasse posed by the Commerce Clause to state spam laws. Its homogeneity vis-à-vis state spam laws offers a comparatively better front in the fight against spam.

B. Advertisement Labeling and the First Amendment

Section 5(a)(5)(A)(i) of the CAN-SPAM Act makes it unlawful to transmit a commercial electronic message to a protected computer without a "clear and conspicuous identification that the message is an advertisement or solicitation."[152] Similarly, section 5(d)(1) requires the mandatory placement of warning labels on sexually oriented unsolicited electronic mails.[153] This mandatory labeling provision obviously empowers ISPs and consumers to easily identify and effectively filter out unsolicited commercial and sexually oriented electronic messages. However, observers have identified two major problems posed by the labeling provisions.[154] First, the labeling provision could not be enforced against e-mails that emanate from outside of the United States.[155]

> benefits. If a legitimate local purpose is found, then the question becomes one of degree. And the extent of the burden that will be tolerated will of course depend on the nature of the local interest involved, and on whether it could be promoted as well with a lesser impact on interstate activities.

Id. at 143 (internal citations omitted).

151. Most state legislations that have had to contend with the Commerce Clause almost always had legitimate local public interests to protect. This was even true of the statute in *Cooley*. An 1803 Pennsylvanian statute had sought

> to meet the most usual cases *quae frequentius accidunt*; they rest upon the propriety of securing lives and property exposed to the perils of a dangerous navigation, by taking on board a person peculiarly skilled to encounter or avoid them; upon the policy of discouraging the commanders of vessels from refusing to receive such persons on board at the proper times and places; and upon the expediency, and even intrinsic justice, of not suffering those who have incurred labor, and expense, and danger, to place themselves in a position to render important service generally necessary, to go unrewarded, because the master of a particular vessel either rashly refuses their proffered assistance, or, contrary to the general experience, does not need it.

Cooley v. Bd. of Wardens of Phila., 53 U.S. 299, 312 (1851).

152. 15 U.S.C.A. § 7704(a)(5)(A)(i) (Supp. VI 2004).

153. *Id.* § 7704(d)(1).

154. *See* Berman & Bruening, *supra* note 11; CENTER FOR DEMOCRACY AND TECHNOLOGY, NOTICE OF PROPOSED RULE MAKING: PROPOSED MARK FOR SEXUALLY ORIENTED SPAM, *at* http://www.cdt.org/speech/spam/20040217cdt.shtml (Feb. 17, 2004).

155. *See* Center for Democracy and Technology, *supra* note 154.

Second, it does no more than institutionalize "forced speech," and therefore contravenes the First Amendment.[156] These are, no doubt, serious legal huddles to the realization of advertisement labeling objectives of the CAN-SPAM Act. The two problems and how the U.S. courts might approach them are addressed in the following paragraphs.

1. Enforcing Compliance with the Labeling Provisions by Senders of Unsolicited Commercial Electronic Messages from Outside of the United States

The first legal problem involves transnational enforcement of national spam laws. Congress was conscious of this as a possible major obstacle and it is by no means a new problem.[157] This Part will examine and draw analogies from comparative international cyberspace jurisdictional disputes in recent times, and what lessons could be learned in the quest for transnational enforcement of spam laws.

As noted earlier in this Article, Christopher Reed, an advocate of the transposition of traditional law on cyberspace, suggested the application of the localization principle to resolving jurisdictional problems in cyberspace.[158] This involves ascertaining where a human actor was situated when the relevant act was performed.[159] Thus, courts, either at the place where digital information is uploaded or downloaded, could assume jurisdiction or apply their rules over disputes.[160] This principle underscores the logic behind the Australian case of *Gutnick v. Dow Jones & Co.*,[161] where the Supreme Court of Victoria assumed jurisdiction over a U.S. corporation in a libel suit filed by a resident of Victoria.[162] The

156. Berman & Bruening, *supra* note 11.

157. The United States Congress noted that it would be necessary to pursue cooperative efforts with other countries for a successful regulation of spam. *See* 15 U.S.C.A. § 7701(a)(12).

158. *See* REED, *supra* note 84, at 188.

159. *Id.*

160. This proposition, albeit imperfect, appears as the most feasible solution to cyberspace jurisdictional problems. Jack Goldsmith echoed Christopher Reed's support for the principle of localization in the following excerpts: A transaction "can legitimately be regulated by the jurisdictions where significant events of the transactions are felt, and the jurisdictions where the parties burdened by the regulation are from." *See* Goldsmith, *supra* note 68, at 1208.

161. This case was unreported by the Supreme Court of Victoria. *See* [2001] VSC 305, 2001 WL 966287 (V.S.C. Aug. 28, 2001).

162. *Id.* ¶ 79. The plaintiff, who resided and carried on a business in the state of Victoria in Australia, alleged that he had been defamed by the publication in Victoria of material which had been downloaded there from the World Wide Web by subscribers to a business news service conducted by the defendant. The alleged defamatory material related to the plaintiff's probity as a businessman. The defendant had an editorial office in New York where material for the service was prepared. The material was then transferred to computers operated by the defendant in New Jersey from which it was made available (by downloading) to subscribers to the news service by computers which had access to the Internet. Subscribers might be anywhere that access was

alleged defamatory statement had been uploaded on the World Wide Web by the defendant in New York. On appeal, the Victoria Supreme Court decision was upheld a year later by the High Court of Australia in *Dow Jones & Co. v. Gutnick*.[163] In the comparative case of *Playboy Enterprises, Inc. v. Chuckleberry Publishing, Inc.*,[164] a district court judge enjoined the defendants from accepting further subscriptions from customers in the United States, for their Italian PLAYMEN magazine, which was published on the World Wide Web in Italy.[165] The court found that making the magazine available to subscribers in the United States, would violate a subsisting United States injunctive order of June 26, 1981, which enjoined the use of PLAYMEN as a mark in the United States, for its infringement of the Playboy trademark.[166]

The underlying principles in *Gutnick* and *Playboy* could by extrapolation be applied in enforcing compliance with the labeling requirement in particular, and other provisions of the CAN-SPAM Act in general, to spam that originates from outside of the United States. It should be noted, however, that the application of local rules and the assumption of jurisdiction by local courts over transnational disputes via the localization principle is by no means free of conflict of laws problems. These stem mainly from the differing substantive and procedural laws from country to country. For instance, a criminalized behavior in country A could be legal in country B. National spam laws also differ in material particulars. For instance, U.K. spam law, like most in Europe, operates an "opt-in" consent-based spam traffic scheme, in contrast to the U.S. "opt-out" mechanism. Additionally, while Europe's E-Privacy Directive empowers aggrieved individuals to file civil lawsuits against spammers who violate its provisions as implemented by member states, the CAN-SPAM Act has no corresponding provision.[167] This raises a specter of differing judicial pronouncements on culpabilities,

---

available to the Internet. There were more than 500,000 subscribers to the news service of whom approximately 1700 were in Australia. *Id.* ¶¶ 1-2. It was held that because the plaintiff's claim was confined to damage allegedly caused to his reputation in Victoria as a consequence of a publication in that State, substantive issues arising in the action would be determined by the law of Victoria. Accordingly, there was no reason to conclude that Victoria was an inappropriate forum. *Id.* ¶ 79.

163. *See* (2002) 210 CLR 575.

164. 939 F. Supp. 1032 (S.D.N.Y. 1996).

165. *Id.* at 1033-34.

166. *Id.* at 1042.

167. Note that some state spam laws, including Idaho and Nevada, permit civil lawsuits by recipients of unsolicited e-mails against spammers. *See* IDAHO CODE §§ 48-60E (Michie 2000); NEV. REV. STAT. ANN. 41.730-35 (Michie 2002). The usefulness of such provisions, however, is in doubt because they are arguably open to the CAN-SPAM Act's preemption.

liabilities, and damages that are a sure fillip for forum shopping by litigants.[168] This dilemma was amply demonstrated in *Gutnick*, where the Victoria Supreme Court noted that the plaintiff had a relatively better prospect for success in his libel suit against the defendant in Australia than in the United States where his claims might not withstand the scrutiny of the First Amendment.[169]

Furthermore, central to the success of the localization principle is the recognition and enforcement of foreign judgments relating to spam. In the European Union, the Brussels Convention allows for free recognition and enforcement of judgments among member states.[170] In the United States, however, the legal processes for recognition and enforcement of transnational judgments are less certain.[171] A major obstacle to the enforcement of foreign judgments in the United States is that, unlike interstate judgments, foreign judgments are not covered by the Full Faith and Credit Clause.[172] Moreover, recognition and enforcement of a foreign judgment could be declined on due process grounds of unreasonable jurisdiction and defective procedure.[173]

The conundrum of recognition and enforcement of foreign judgments in the United States is epitomized by the recent French judgment in the *Yahoo!* case. Because of the central significance of

---

168. *See* Susanne Fruhstorfer & Felix Klement, *General Grounds on Which Courts Will Accept Jurisdiction*, *in* FORUM SHOPPING 1 (J.H. Barton Van Lynden ed., 1998).

169. [2001] VSC 305, 2001 WL 966287, ¶ 73 (V.S.C. Aug. 28, 2001).

170. *See* Council Regulation 44/2001 on Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial Matters, arts. 5, 16, 2001 O.J. (L 12) 1, 4, 7 [hereinafter Brussels Regulation]. The Brussels Regulation is based on the Brussels and Lugano Conventions. *See* Brussels Convention, *supra* note 88; Lugano Convention on Jurisdiction and Enforcement of Judgments on Civil and Commercial Matters, Sept. 16, 1988, 28 I.L.M. 620. The Brussels Convention contains provisions that are similar to the Full Faith Clause of the United States Constitution. Pursuant to section 3 of article 5 of the Brussels Convention, a resident of a member state may be sued in the court of another member state "in matters of tort, delict, or quasidelict, in the courts for the place in which the harmful effect occurred." Article 26 provides further that: "[a] judgment given in a Contracting State shall be recognized in the other Contracting States without any special procedure being required." Article 27, however, allows a Contracting State to refuse recognizing such a judgment if it contravenes their public policy, if the defendant was not properly served and thereby defaulted, or if the judgment is contrary to a previous judgment involving the same parties delivered in the Contracting State in which judgment is sought.

171. There is no guarantee that U.S. judgments would be enforced overseas because the United States is not a party to any multinational convention such as the Brussels Convention on transnational enforcement of foreign judgments. Furthermore, foreign judgments are not centrally enforced in the United States as each state applies its own rules barring federal preemption. *See* Julie E. Dowler, *Forging Finality: Searching for a Solution to the International Double-Suit Dilemma*, 4 DUKE J. COMP. & INT'L L. 363, 390-91 (1994).

172. U.S. CONST. art. 4, § 1, cl. 1.

173. *Id.* amend XIV, § 1.

foreign judgment enforcement to transnational enforcement of spam laws, the *Yahoo!* case should be discussed in detail. A French court found Yahoo! liable for infringing section R645-1 of the French Criminal Code, which prohibits exhibition of Nazi propaganda and artifacts for sale in *Ligue Contre le Racisme et L'Antisémitisme v. Yahoo! Inc.*[174] The United States District Court for the Northern District of California, however, in *Yahoo!, Inc. v. La Ligue Contre le Racisme et l'Antisémitisme*,[175] on the same facts held that the French order was in violation of the freedom of expression provision in the First Amendment.[176] The district court judge hypothesized that if a

> party were physically present in France engaging in expression that was illegal in France but legal in the United States, it is unlikely that a United States court would or could question the applicability of French law to that party's conduct. However, an entirely different case would be presented if

---

174. *See* Interim Order, T.G.I. Paris, Nov. 20, 2000, No. RG:00/05308 (detailing ways in which Yahoo! Inc., could block access from France to sites auctioning Nazi memorabilia). Yahoo! challenged the jurisdiction of a French court, when it was ordered to implement screening technology to block individuals located within French territory from accessing auctions involving Nazi memorabilia. Although the French subsidiaries of Yahoo! did not allow such postings on their auction sites, Yahoo's U.S. site allowed such postings, fearing that any restrictions would impinge the First Amendment. Yahoo! argued unsuccessfully that the U.S. site's services were designed and intended for Internet users in the United States. It argued further that its servers were located in U.S. territory; and that prohibiting the auction site in the United States would contravene the First Amendment, which guaranteed freedom of expression. The court dismissed these arguments, and affirmed that French courts have jurisdiction over Yahoo! for activities on its general auction site that are directed to a French audience. The court relied on evidence that Yahoo! responded to visitors to its auction site from computers located in France by posting advertisement banners in French. Additionally, the court noted Yahoo's control of the delivery of objects purchased in its auctions. It also found that Yahoo! was able to prohibit auctions in certain objects such as "human organs, drugs, works or objects related to pedophilia, cigarettes or live animals." While relying on these findings, the court dismissed Yahoo's argument that it was impossible to comply with a court injunction of May 22, 2000, and ordered filtering access to the auction sites of Nazi objects. Because any French citizen is able to access these materials on Yahoo.com directly or through a link on Yahoo.fr, the French court concluded that the Yahoo.com auction site violates section R645-1 of the French Code pénal, which prohibits exhibition of Nazi propaganda and artifacts for sale.

175. *See* 169 F. Supp. 2d 1181 (N.D. Cal. 2001).

176. *See id.* at 1193. The district court held:

> Moreover, the French order requires Yahoo! not only to render it impossible for French citizens to access the proscribed content but also to interpret an impermissibly overbroad and vague definition of the content that is proscribed. . . . In light of the Court's conclusion that enforcement of the French order by a United States court would be inconsistent with the First Amendment, the factual question of whether Yahoo! possesses the technology to comply with the order is immaterial. Even assuming for purposes of the present motion that Yahoo! does possess such technology, compliance still would involve an impermissible restriction on speech. Accordingly, Defendants' motion pursuant to Rule 56(f) motion will be denied.

Id. at 1193-94.

> the French court ordered the party not to engage in the same expression in the United States on the basis that French citizens (along with anyone else in the world with the means to do so) later could read, hear or see it. While the advent of the Internet effectively has removed the physical and temporal elements of this hypothetical, the legal analysis is the same.[177]

However, the district court judgment was reversed by the United States Court of Appeals for the Ninth Circuit in *Yahoo!, Inc. v. La Ligue Contre le Racisme et l'Antisémitisme*.[178] The court of appeals found that the district court wrongly assumed personal jurisdiction in the case below.[179] In arriving at their decision, the court of appeals drew heavily on the three conditions of "minimum contacts," "fairplay," and "substantial justice,"[180] that the Supreme Court had held as prerequisites to a finding of personal jurisdiction in *International Shoe Co. v. Washington*,[181] as elaborated on by the Court in *Calder v. Jones*.[182] The court of appeals further reiterated their view in the earlier case of *Bancroft & Masters, Inc. v. Augusta National Inc.*,[183] where they interpreted *Calder*, to the effect "that the case [*Calder*] cannot stand for the broad proposition that a foreign act with foreseeable effects in the forum state always gives rise to specific jurisdiction."[184] The court of appeals had further held in *Bancroft* while interpreting *Calder* that, besides the effects doctrine, the foreign wrongful act must be expressly aimed at the forum state.[185] However, in the *Yahoo!* case, the court of appeals found that La Ligue Contre le Racisme et l'Antisémitisme's litigation against Yahoo! did not amount to "express aiming," as it did not qualify as wrongful conduct targeted at Yahoo!.[186] While discussing the validity of La Ligue Contre le et l'Antisémitisme's litigation against Yahoo!, the court of appeals found as follows:

> LICRA and UEJF took action to enforce their legal rights under French law. Yahoo! makes no allegation that could lead a court to conclude that there was anything wrongful in the organizations' conduct. As a result, the District Court did not properly exercise personal jurisdiction over LICRA and UEJF. Because the District Court had no personal jurisdiction over the French parties, we do not review whether Yahoo!'s action for declaratory

177. *Id.* at 1194.
178. 379 F.3d 1120 (9th Cir. 2004).
179. *Id.* at 1125.
180. *Id.* at 1123.
181. 326 U.S. 310 (1945).
182. 465 U.S 783 (1984).
183. 223 F.3d. 1082, 1087 (9th Cir. 2000).
184. *Yahoo!*, 379 F.3d at 1124 (quoting *Bancroft & Masters*, 223 F.3d at 1087).
185. *See Bancroft & Masters*, 223 F.3d at 1087.
186. *See Yahoo!*, 379 F.3d at 1125.

> relief was ripe for adjudication or whether the District Court properly refused to abstain from hearing the case.[187]

Although the court of appeals declined to review whether the declaratory relief was ripe for adjudication, the court also observed that U.S. courts could assume jurisdiction and hear the First Amendment claim, if the French associations had sought the assistance of a U.S. district court to enforce the French judgment.[188] It was inevitable that the French associations would have resorted to a U.S. district court to enforce its judgment, had they not been preempted by Yahoo!'s litigation. However, whether the French judgment would have passed First Amendment muster in the circumstances remains an open question, given the wide reach of the free speech ambit in the United States.

The court of appeals has ordered the *Yahoo!* case to be reheard en banc.[189] While the world awaits the decision of the en banc court, it is beyond doubt that the French decision in the *Yahoo!* case is still open to First Amendment scrutiny. This is an obvious pitfall to transnational enforcement of spam laws, as it is for other aspects of Internet-related disputes.[190] However, despite the conflict of laws obstacles, the localization principle is the most practical solution to the jurisdictional problems of choice of court, law, and enforcement in transnational spam governance.[191] For instance, it would allow U.S. courts to enforce compliance with the labeling requirements of sections 5(A)(i) and 5(d)(1) as well as other provisions of the CAN-SPAM Act concerning unsolicited commercial electronic messages sent from outside of the United States. Conversely, it would allow other countries to assume jurisdiction on spam sent from the United States, which did not comply with local rules. The validity of such judgments in the United States is of course subject to the Due Process Clause as epitomized by *Yahoo!*.[192]

2. Would the First Amendment Block Advertising and Sexually Oriented Labeling Provisions?

The First Amendment provides that: "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise

---

187. *Id.* at 1126-27.

188. *Id.* at 1123.

189. *See* Yahoo! Inc. v. La Ligue Contre le Racisme et l'Antisémitisme, 399 F.3d 1010 (9th Cir. 2005).

190. *See* Paul Schiff Berman, *The Globalization of Jurisdiction*, 151 U. PENN. L. REV. 311, 342 (2002).

191. *See* REED, *supra* note 84, at 188.

192. 169 F. Supp. 2d at 1187-93.

thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances."[193] Critics of the CAN-SPAM Act have charged that both sections 5(a)(5)(A)(i) and 5(d)(1), which respectively require a clear and conspicuous labeling of unsolicited commercial electronic messages as advertisements, and labeling of sexually oriented electronic messages,[194] are no more than a legal validation of "forced speech," and, *a fortiori*, vulnerable to the First Amendment which protects the sanctity of freedom of expression.[195] This argument is predicated on the proposition that the

> rule would unduly burden either entities selling sexually oriented material through email messages or consumers who were interested in purchasing sexually oriented material offered to them through email messages. Precisely because the label is intended to interface with ISP filters; the rule would burden senders of lawful, sexually oriented material.[196]

How might the Supreme Court construe the CAN-SPAM Act's labeling requirements vis-à-vis the First Amendment? The Supreme Court recognizes the Internet as a unique medium of communication.[197] The Supreme Court also acknowledges the differences in the characteristics of communication media[198] and has historically applied medium-specific rules in ascertaining whether a regulatory provision violates the First Amendment.[199] With the decisions in *Reno*, and *Ashcroft*, it is beyond doubt that the Supreme Court will not allow suppression of free speech on the Internet.[200] Taking a cue from

---

193. U.S. CONST. amend. I.

194. 15 U.S.C.A. §§ 7704(a)(5)(A)(i), (d)(1) (Supp. VI 2004). On April 19, 2004, the FTC adopted a final rule on labeling of sexually explicit electronic mails. *See* Label for Email Messages Containing Sexually Oriented Material, 69 Fed. Reg. 21,024 (Apr. 19, 2004).

195. *See* Jan H. Samoriski, *Unsolicited Commercial E-mail, the Internet and the First Amendment: Another Free Speech Showdown in Cyberspace?*, 43 J. BROAD. & ELEC. MEDIA 670 (1999). The author argues that content-based government regulation is unconstitutional. He recommends a recourse to filtering technology which he describes as a "First Amendment friendly solution." *Id.* at 682; *see also* Global Internet Liberty Campaign, *"Regardless of Frontiers": Protecting the Human Right to Freedom of Expression on the Global Internet*, *at* http://www.cdt.org/gilc/report.html (last visited July 27, 2004); R. Jonas Geissler, *Whether 'Anti-Spam' Laws Violate The First Amendment*, 2001 J. ONLINE L. art. 8, ¶¶ 35-37 (2001), *at* www.wm.edu/law/publications/jol/articles/geissler.shtml.

196. *See* Center for Democracy and Technology, *supra* note 154.

197. *See* Reno v. ACLU, 521 U.S. 844, 850 (1997).

198. *See* Red Lion Broad. Co. v. FCC, 395 U.S. 367, 386-87 (1969).

199. *See* RAYMOND S.R. KU ET AL., CYBERSPACE LAW: CASES AND MATERIALS 138 (2002).

200. 124 S. Ct. 2783 (2004). Justice Kennedy, while delivering the Court's opinion held:

> The imperative of according respect to the Congress, however, does not permit us to depart from well-established First Amendment principles. Instead, we must hold the Government to its constitutional burden of proof.

Ashcroft,[201] the Supreme Court, faced with the constitutional validity of the advertisement labeling provision of the CAN-SPAM Act, might inquire into whether there was a less restrictive or less burdensome way (other than the labeling provision) that Congress could have achieved its objective of empowering ISPs and electronic mail recipients to control unsolicited commercial electronic messages and sexually oriented messages.

Furthermore, the Supreme Court decision in *Rowan v. United States Post Office Department*[202] offers another insight into how the Court might handle the CAN-SPAM Act's labeling provisions. The Court in *Rowan* held that the First Amendment did not forbid federal legislation that allowed addressees to remove themselves from mailing lists and stop all future mailings. The Court stated that the "mailer's right to communicate must stop at the mailbox of an unreceptive addressee. . . . To hold less would be to license a form of trespass."[203] This affirms addressees' general right to accept or reject unsolicited mails. In this context, the free speech right is not a one-way affair. By extrapolation, it arguably covers an addressee's right to require labeling of certain unsolicited mails. It should make no difference that e-mail recipients are assisted by Congress's mandated statutory conditions. The essence of the labeling provisions is to ensure that unsolicited commercial electronic messages are tagged as advertisements, and that sexually oriented messages should be identified as such. Although compliance with the labeling provision by senders of such messages technically empowers ISPs and targeted addressees to identify and filter out or block such messages, such empowerment arguably falls within the remit of the *Rowan* decision.

> Content-based prohibitions, enforced by severe criminal penalties, have the constant potential to be a repressive force in the lives and thoughts of a free people. To guard against that threat the Constitution demands that content-based restrictions on speech be presumed invalid . . . and that the Government bear the burden of showing their constitutionality. This is true even when Congress twice has attempted to find a constitutional means to restrict, and punish, the speech in question.

124 S. Ct. 2783, 2788 (2004) (Stevens, J., concurring) (citations omitted).

201. Justice Stevens further observed: "In view of the gravity of the burdens COPA imposes on Web speech, the possibility that Congress might have accomplished the goal of protecting children from harmful materials by other, less drastic means is a matter to be considered with special care." *Id.* at 2797 (Stevens, J., concurring).

202. 397 U.S. 728, 736 (1970).

203. In the context of spam regulation, however, the *Rowan* legislation was more analogous to the "opt-out" spam traffic provision than the labeling provisions of the CAN-SPAM Act. Nevertheless, the underlying principle is relevant to ascertaining how the Supreme Court might view the latter in light of the First Amendment. This is more so because of the labeling provisions' comparatively milder disposition than CAN-SPAM Act's "opt-out" option and the federal postal legislation in the *Rowan* case. *Id.* at 728.

Indeed, a creative construct of the First Amendment could validate the rights of recipients of unsolicited commercial e-mails to choose what type of information to allow into their inboxes. In other words, if the First Amendment guarantees freedom of speech to senders of unsolicited commercial and sexually oriented e-mails, there should be a corresponding freedom for recipients of unsolicited e-mails to elect or choose what kinds of mail (i.e., speech) to allow or bar from clogging their inboxes. This proposition is not new, and has in fact been endorsed by the Supreme Court, albeit in nonspam cases.[204]

Furthermore, it has been argued that "the right to receive speech, while constitutionally derivative of the right to produce it, is distinct and possesses independent legal force."[205] In *Virginia State Board of Pharmacy*, the Supreme Court held that "freedom of speech 'necessarily protects the right to receive.'"[206] The Supreme Court held further: "Freedom of speech presupposes a willing speaker. But where a speaker exists . . . the protection afforded is to the communication, to its source and to its recipients both."[207] Viewed from the foregoing perspectives, it is correct to argue that the CAN-SPAM Act's labeling provision only seeks to maintain an even balance between the competing First Amendment rights to free speech of the senders and recipients of unsolicited commercial or sexually oriented e-mails.

Furthermore, while one could only speculate on how the Supreme Court might apprize the CAN-SPAM Act's labeling provision vis-à-vis the First Amendment, the United States District Court for the Southern

---

204. *See* Va. State Bd. of Pharmacy v. Va. Citizens Consumer Council, Inc., 425 U.S. 748, 757 (1976). Lawrence Lessig aptly captures the free speech enigma in his proposition:

> The right to free speech is not the right to speak for free. It is not the right to free access to television, or the right that people not hate you for what you have to say. Strictly speaking-legally speaking-the right to free speech in the United States means the right to be free from punishment by the government in retaliation for at least some (probably most) speech. You cannot be jailed for criticizing the president, though you can be jailed for threatening him; you cannot be fined for promoting segregation, though you can be stopped from speaking with an FM transmitter. Speech in the United States is protected-in a complex, and at times convoluted, way-but its constitutional protection is a protection against the government. . . . Nevertheless, a constitutional account of free speech that thought only of government would be radically incomplete. . . . More than government constrains speech, and more than government protects free speech. A complete account of this-and any-right must consider the full range of burdens and protections.

LESSIG, *supra* note 67, at 164.

205. *See* Dana R. Wagner, Note, *The First Amendment and The Right to Hear:* Rofsky v. Allen, 108 YALE L.J. 669, 673 (1998) (citations omitted).

206. *See Va. State Bd.*, 425 U.S. at 757 (quoting Kleindienst v. Manel, 408 U.S. 753, 762-63 (1974)).

207. Wagner, *supra* note 205, at 669.

District of Ohio in the *CompuServe*[208] decision provided a more direct clue and insight into how the Supreme Court might handle the labeling provision of the CAN-SPAM Act.[209] The district court held that an electronic mail advertising company did not have a free speech right to send unsolicited commercial e-mail to subscribers of a commercial online computer service. The decision was partly predicated on the grounds that Cyber Promotions, the sender of unsolicited e-mails, had adequate alternative means of communication available to it. This is better illustrated in the court's words:

> Defendants in the present action have adequate alternative means of communication available to them. Not only are they free to send e-mail advertisements to those on the Internet who do not use CompuServe accounts, but they can communicate to CompuServe subscribers as well through online bulletin boards, web page advertisements, or facsimile transmissions, as well as through more conventional means such as the U.S. mail or telemarketing. Defendants' contention, referring to the low cost of the electronic mail medium, that there are no *adequate* alternative means of communication is unpersuasive. There is no constitutional requirement that the incremental cost of sending massive quantities of unsolicited advertisements must be borne by the recipients.[210]

In the context of *CompuServe*, senders of unsolicited commercial e-mails who dislike the labeling requirements should not have the free speech right to send unsolicited commercial e-mails since they most certainly have adequate alternative means of communicating their messages to their targeted audiences.[211] If there were no free speech right to send unsolicited commercial e-mails, or unsolicited sexually oriented e-mails, then arguably, no free speech right was threatened by the CAN-SPAM Act's labeling provision. Viewed from this perspective, it is arguable that the labeling provision does not validate "forced speech," and therefore does not violate the First Amendment. This proposition is

---

208. 962 F. Supp. 1015 (S.D. Ohio 1997). The Southern District of Ohio had indeed taken the same stance as the United States District Court for the Eastern District of Pennsylvania, in *Cyber Promotions, Inc. v. American Online, Inc.*, 948 F. Supp. 456 (E.D. Pa. 1996). One of the issues for determination in that case was whether Cyber Promotions had the First Amendment right to send unobstructed e-mail to AOL subscribers. The court held that Cyber Promotions had no such right and that AOL was not exercising powers that are traditionally the exclusive prerogative of the state, i.e., AOL was not operating as an "essential facility." *Id.* at 464-65.

209. This is not however suggesting that the Supreme Court is bound to share the district court's view. Such a proposition is an obviously sacrilegious attack on hallowed normative judicial precedence.

210. *CompuServe*, 962 F. Supp. at 1026.

211. Arguably, there are other media of advertisements such as radio, television, and newspapers.

reinforced by the fact that the labeling requirement is not a blanket ban on unsolicited commercial electronic messages or on unsolicited sexually oriented messages.[212] It merely stipulates the conditions for transmitting unsolicited commercial e-mail messages that both impose extra economic burdens and intrude on recipients' privacy.

C. The CAN-SPAM Act's Accurate Header Provision and the Right to Anonymity

Section 5(a)(1) of the CAN-SPAM Act prohibits the transmission of unsolicited commercial electronic messages whose header information is materially false or materially misleading.[213] The Act also elaborates on the types of header information that would be classified as such.[214] Furthermore, the Act in section 3(8) defines "header information" 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."[215] The above provision has the inevitable effect of revealing the online identity of the sender of unsolicited commercial e-mails. This has generated concerns among civil rights advocates that the provision endangers anonymity and anonymous communications on the Internet.[216] The pertinent question is whether U.S. courts would hold the CAN-SPAM Act's accurate header information provision in violation of the First Amendment. This question will be answered in the context of the right to anonymous communication.

---

212. The Supreme Court has historically not applied the First Amendment provisions in absolute terms. In *Breard v. City of Alexandria*, 341 U.S. 622 (1951), the Court held that "[t]he First and Fourteenth Amendments have never been treated as absolutes. Freedom of speech or press does not mean that one can talk or distribute where, when and how one chooses." *Id.* at 642 (citations omitted).

213. 15 U.S.C.A. § 7704(a)(1) (Supp. VI 2004). A recent report by the Federal Trade Commission showed that 22% of spam analyzed contained false information in the subject line; 42% contained misleading subject lines which misrepresented that the sender had a business or personal relationship with the recipients; 44% of spam contained false information in the form of subject lines; 40% of all spam showed false messages; ninety percent of investment and business opportunities contained key likely false claims; and 66% of spam contained falsehood from lines, subject lines, or message text. *See* MARKETING DIVISION, FED. TRADE COMM'N, FALSE CLAIM IN SPAM 30, *available at* http://www.ftc.gov/opa/2003/04/spamrpt.htm (Apr. 29, 2003).

214. 15 U.S.C.A. § 7704(a)(1)(A)-(C).

215. *Id.* § 7702(8).

216. *See* Letter from ACLU to the Senate Urging Opposition to the CAN-SPAM Act, *at* http://www.aclu.org/FreeSpeech/FreeSpeech.cfm?ID=13258 (July 30, 2003).

U.S. courts recognize a general constitutional right to speak anonymously.[217] In *McIntyre v. Ohio Elections Commission*,[218] the Supreme Court identified and supported anonymity as an integral element of freedom of speech under the First Amendment:

> The decision in favor of anonymity may be motivated by fear of economic or official retaliation, by concern about social ostracism, or merely by a desire to preserve as much of one's privacy as possible. Whatever the motivation may be, at least in the field of literary endeavor, the interest in having anonymous works enter the marketplace of ideas unquestionably outweighs any public interest in requiring disclosure as a condition of entry. Accordingly, an author's decision to remain anonymous, like other decisions concerning omissions or additions to the content of a publication, is an aspect of the freedom of speech protected by the First Amendment.[219]

As a medium of communication, the Web has come under judicial spotlight in the determination of the nature, degree, and scope of anonymity allowable.[220] Anne Wells Branscomb proposes that true anonymity on the Web "means that no one could trace the source of an electronic message."[221] Branscomb argues further that the First Amendment forbids the prohibition of true anonymity to the extent that governmental interference with anonymous messages is outlawed.[222] Anonymity on the Internet confers certain advantages. While conceding its vulnerability to abuse, Raymond S.R. Ku and his coauthors opine that anonymity in cyberspace through the use of aliases and pseudonyms may help to eliminate discrimination against women and minorities.[223]

---

217. *See* ACLU v. Miller, 977 F. Supp. 1228, 1232 (N.D. Ga. 1997). Internet users challenged the constitutionality of a state criminal statute, which prohibited Internet transmissions that falsely identify the sender or that use trade names or logos which would falsely state or imply that the sender was legally authorized to use them. The district court held that the users had standing to bring the action and that the users were substantially likely to succeed on their claims that the statute was unconstitutionally overbroad and vague. *Id.* at 1235. The court held further that

> the statute's prohibition of internet transmissions which "falsely identify" the sender constitutes a presumptively invalid content-based restriction. . . . The state may impose content-based restrictions only to promote a "compelling state interest" and only through use of "the least restrictive means to further the articulated interest." Thus, in order to overcome the presumption of invalidity, defendants must demonstrate that the statute furthers a compelling state interest and is narrowly tailored to achieve it.

Id. at 1232 (citations omitted).

218. 514 U.S. 334 (1995).

219. *Id.* at 341-42.

220. *See Miller*, 977 F. Supp. at 1232.

221. *See* Anne Wells Branscomb, *Anonymity, Autonomy, and Accountability: Challenges to the First Amendment in Cyberspace*, 104 YALE L.J. 1639, 1641 (1995).

222. *Id.* at 1641-42.

223. *See* KU ET AL., *supra* note 199, at 196.

However, true anonymity has serious implications for the cyber community due to its vulnerability to abuse.[224] In the context of unsolicited e-mails, true anonymity would encourage the transmission of information whose header is materially misleading or deceptive. For instance, sexually oriented material might come with header information that gives the appearance of an advertisement, pitching a household product or an insurance policy.[225] Consequently, recipients' autonomy or right to control their electronic environment is compromised,[226] with no one held accountable or responsible due to unfettered anonymity.[227] In *Miller*, the United States District Court for the Northern District of Georgia accepted the state statute's primary aim of fraud prohibition as a compelling state interest which could override anonymity on the Web.[228] However, the court declared the statute unconstitutional because

> the statute is not narrowly tailored to achieve that end and instead sweeps innocent, protected speech within its scope. Specifically, by its plain language the criminal prohibition applies regardless of whether a speaker has any intent to deceive or whether deception actually occurs. Therefore, it could apply to a wide range of transmissions which "falsely identify" the sender, but are not "fraudulent" within the specific meaning of the criminal code.[229]

---

224. Branscomb argues that individuals would have different objectives for wanting to remain anonymous in cyberspace. While anonymity is game and fun for some computer users, it provides a refuge for antisocial behavior and an escape route for assumption of responsibility for computer misuse. *See* Branscomb, *supra* note 221, at 1642.

225. *See* FTC v. Westby, No. 03 C 2540, 2004 WL 1175047 (N.D. Ill. May 6, 2004) (settlement). A complaint was filed against the defendants in the United States District Court for the Northern District of Illinois in April 2003. The FTC alleged that the defendants used misleading headlines to draw recipients to a sexually explicit Web site. According to the complaints, the defendants sent spam with subject lines such as "Did you hear the news?" and "New Movie info" that disguised the contents of the e-mail. When messages were opened by recipients, they were treated to sexually explicit solicitations to visit the site. The case was settled out of court on May 6, 2004, after the defendants paid $112,500, which represented their "ill-gotten gains" they allegedly made from the spam. *Id.* at *3-*4; *see FTC Settles with Adult Web Site Spammers*, ANDREWS COMPUTER & INTERNET LITIG. REP. (Andrews Publications, Wayne, PA), May 18, 2004, at 10.

226. Branscomb describes autonomy as "the right to exert some modicum of control over one's electronic environment." Branscomb, *supra* note 221, at 1644. On the interface between autonomy and free speech, she argues that "[c]ontrol over information may appear to be the flip side of freedom of speech; that is, the freedom not to speak. This freedom not to speak simply protects the right not to have information disclosed without consent or in a manner that may be contrary to one's interests. This has become a matter of considerable concern." *Id.*

227. *See id.* at 1645 (describing the complex interface of anonymity, autonomy, and accountability).

228. 977 F. Supp. 1228, 1231-32 (N.D. Ga. 1997).

229. *Id.* at 1232.

It could be surmised from *Miller* that the anonymity right is not absolute, but could be constrained by fraud-prevention or other public interest-oriented legislations, provided such legislations are narrowly designed to achieve that aim without trampling on innocent protected speech. Undoubtedly, the primary aim of section 5(a)(1) of the CAN-SPAM Act is the prohibition of fraudulently misleading header information in unsolicited commercial e-mails. This, without doubt, is a compelling public interest. Moreover, the section does not apply to all forms of e-mails, but only unsolicited commercial e-mails. The provision is therefore narrowly defined, and would not affect noncommercial unsolicited electronic messages. Thus, it will not affect the free speech right of the generality of Internet users who send unsolicited noncommercial electronic messages daily. Viewed from this perspective, section 5(a)(1) of the CAN-SPAM Act arguably passes First Amendment muster.

Furthermore, to ascertain how U.S. courts might construe the accurate header information provision in section 5(a)(1) of the CAN-SPAM Act, it is apt to analyze comparative, albeit nonspam statutes regulating anonymity in communication. In *Talley v. California*,[230] the petitioner was prosecuted for violating a city ordinance which prohibited the distribution of anonymous handbills in any place under any circumstances. The petitioner distributed certain handbills which urged readers to boycott certain businesses who sold goods manufactured by companies who discriminated on the basis of race in their employment opportunities. In dismissing the California ordinance as violative of the Fourteenth and First Amendments, Justice Black wrote:

> There can be no doubt that such an identification requirement would tend to restrict freedom to distribute information and thereby freedom of expression. "Liberty of circulating is as essential to that freedom as liberty of publishing; indeed, without the circulation, the publication would be of little value." Anonymous pamphlets, leaflets, brochures and even books have played an important role in the progress of mankind. Persecuted groups and sects from time to time throughout history have been able to criticize oppressive practices and laws either anonymously or not at all.[231]

---

230. 362 U.S. 60 (1960). For discussion on cases dealing with the right to remain anonymous, see *McVeigh v. Cohen*, 983 F. Supp. 215 (D.D.C 1998); *Columbia Ins. Co. v. seescandy.com*, 51 U.S.P.Q.2d 1130 (N.D. Cal. 1999); *Doe v. 2TheMart.Com Inc.*, 140 F. Supp. 2d 1088 (W.D. Wash. 2001).

231. *Talley*, 362 U.S. at 64 (quoting Covell v. City of Griffin, 352 U.S. 444, 452 (1938)).

Referring to its previous decisions in *Bates v. City of Little Rock*,[232] and *NAACP v. Alabama*,[233] the Supreme Court in *Talley* further held:

> We have recently had occasion to hold in two cases that there are times and circumstances when States may not compel members of groups engaged in the dissemination of ideas to be publicly identified. The reason for those holdings was that identification and fear of reprisal might deter perfectly peaceful discussions of public matters of importance. This broad Los Angeles ordinance is subject to the same infirmity. We hold that it, like the Griffin, Georgia, ordinance, is void on its face.[234]

Although the *Talley* decision trumped the California ordinance which constrained the petitioner's right to anonymous communication as guaranteed by the First and Fourteenth Amendments, the restrictive California ordinance and section 5(a)(1) of the CAN-SPAM Act which requires accurate header information for transmitted electronic messages are in no way comparable. Section 28.06 of Municipal Ordinance No. 77,000 of the City of Los Angeles, struck down by the *Talley* Court, provided:

> No person shall distribute any hand-bill in any place under any circumstances, which does not have printed on the cover, or the face thereof, the name and address of the following:
> (a) The person who printed, wrote, compiled or manufactured the same.
> (b) The person who caused the same to be distributed; provided, however, that in the case of a fictitious person or club, in addition to such fictitious name, the true names and addresses of the owners, managers or agents of the person sponsoring said hand-bill shall also appear thereon.[235]

On the contrary, the type of speech sought to be regulated by section 5(a)(1) of the CAN-SPAM Act, is essentially nonpolitical, commercial advertisements that are targeted at prospective customers.[236] Senders of such unsolicited commercial messages are merely required to truthfully and accurately head information on their unsolicited electronic messages. Although the provision has the effect of revealing the true identities of

---

232. 361 U.S. 516 (1960).
233. 357 U.S. 449, 462 (1958).
234. *Talley*, 362 U.S. at 65.
235. LOS ANGLES COUNTY, CAL., MUN. ORDINANCE No. 77,000, § 28.06.
236. Good examples of noncommercial unsolicited electronic messages are those sent by a disgruntled ex-employee in *Intel Corp. v. Hamidi*, 71 P.3d 296 (Cal. 2003). *But see* Peter A Steinmeyer, *California Spamming: Opening the E-mail Spigot*, NAT'L L.J., July 28, 2003, at 34 (criticizing the judgment).

senders, the consequence is purely circumstantial,[237] and (unlike *Talley*) could hardly induce a "fear of reprisal" that "might deter perfectly peaceful discussions of public matters of importance."[238] The worst that could happen to such a message is its increased visibility and vulnerability to filtering technology. This makes it easier for ISPs and recipients to delete the message, a right that is arguably cognizable under the First Amendment.[239]

D. The CAN-SPAM Act: Summary of Analysis and Conclusion

This Part examines the challenges facing the CAN-SPAM Act, as well as the prospects for its success. The major challenges are the possible infraction of the First and Fourteenth Amendments by the labeling and accurate header information provisions. Critics have charged that the provisions respectively validate "forced speech" and destroy the First and Fourteenth Amendment rights to anonymous communication. The Article evaluates these charges through the case law prism. It argues that the provisions are justifiable for maintaining an even balance between the conflicting rights of senders of unsolicited commercial electronic messages and their targeted recipients. The theory

---

237. The essence of section 5(a)(1) of the CAN-SPAM Act, 15 U.S.C.A. § 7704(a)(1) (Supp. VI 2004), is to prevent materially misleading or deceptive headers of unsolicited e-mails. The goal is to protect the interest of e-mail recipients. It empowers them to choose whether to read or delete the messages. It does not matter that compliance with the provision would facilitate the weeding out or filtering out of certain unsolicited messages by ISPs and e-mail recipients.

238. *Talley*, 362 U.S. at 65.

239. As in *Talley*, the Supreme Court has historically sanctioned statutes that impinged on the First Amendment right to anonymity in political speech dissemination. McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 357 (1995). A pamphleteer challenged a fine imposed by the Ohio Elections Commission for distributing anonymous leaflets opposing a proposed school tax levy. *Id.* at 336-37. Ohio Revised Code Annotated section 3599.09(A) (West 1988) provided:

> No person shall write, print, post, or distribute, or cause to be written, printed, posted, or distributed, a notice, placard, dodger, advertisement, sample ballot, or any other form of general publication which is designed to promote the nomination or election or defeat of a candidate, or to promote the adoption or defeat of any issue, or to influence the voters in any election, or make an expenditure for the purpose of financing political communications through newspapers, magazines, outdoor advertising facilities, direct mailings, or other similar types of general public political advertising, or through flyers, handbills, or other nonperiodical printed matter, unless there appears on such form of publication in a conspicuous place or is contained within said statement the name and residence or business address of the chairman, treasurer, or secretary of the organization issuing the same, or the person who issues, makes, or is responsible therefor.

The issue for determination was whether the Ohio statute was a "law . . . abridging the freedom of speech" within the meaning of the First Amendment." *McIntyre*, 514 U.S. at 336. The Supreme Court held that the prohibition violated the First Amendment. *Id.* at 357.

is advanced that a sender of unsolicited commercial electronic messages has no more claim to the First Amendment free speech protection than a recipient of unsolicited commercial electronic messages has in stipulating conditions for receiving such messages. Thus, this Article argues that U.S. courts will most likely absolve the CAN-SPAM Act of any free speech infraction.

This Article also notes the merits inherent in the CAN-SPAM Act's preemption of state spam laws. This Article finds merit in Congress's fears that the disparate state spam laws could engender confusion among law-abiding citizens. It argues that federal preemption of state spam laws would facilitate a unified front, and a better coordinated fight against spam. Most importantly, preemption would obviate the inevitable clash of states' spam laws with the Commerce Clause of the United States Constitution, as states reach out to prosecute interstate spam regulation violations.

The Article also notes that transnational enforcement of spam regulation is a major obstacle to the success of the CAN-SPAM Act. In the absence of an international convention on jurisdiction and foreign judgments enforcement of Internet-related disputes, the United States would have to hope for mutual reciprocity in transnational spam enforcement. It is noted that this would not be easy, because states, and not the federal government, are in charge of local enforcement of foreign judgments in the United States. The hurdle to enforcement of foreign judgments in the United States is further layered by the due process compliance rule of the Fourteenth Amendment. This point is well illustrated by the *Yahoo!* case. No foreign country would enforce U.S. courts' judgments relating to the CAN-SPAM Act, if there were no assurance of reciprocity from U.S. courts. The best solution might be to revive discussions on the proposed Hague Convention on International Jurisdiction and Foreign Judgments in Civil and Commercial Matters.[240]

This Article acknowledges that the CAN-SPAM Act is not perfect. A major weakness is that individuals are not allowed to pursue civil

---

240. Preliminary Draft Convention on Jurisdiction and Foreign Judgments in Civil and Commercial Matters, *at* http://www.hcch.net/upload/wop/jdgon_drafte.pdf (Oct. 30, 1999). A Diplomatic Conference was held at the Hague in 2001 to consider a proposed "Hague Convention." The aim was to internationalize the principles in the Brussels Convention. *See* Special Commission on Jurisdiction and Enforcement of Foreign Judgments in Civil and Commercial Matters, *at* http://europa.eu.int/comm/justice_home/news/consulting_public/gp_15112004/doc_travail_en.pdf (Apr. 27, 2004); Peter D. Trooboff, *Choice-of-Court Clauses*, NAT'L L.J., Jan. 19, 2004, col. 1; Benjamin C. Elacqua, *The Hague Runs into B2B: Why Restructuring the Hague Convention of Foreign Judgments in Civil and Commercial Matters to Deal with B2B is Long Overdue*, 3 J. HIGH TECH. L. 93 (2004).

lawsuits for alleged violation of the Act's provisions. Furthermore, the Act adopts an "opt-out" rule for spam traffic. This is generally perceived as more lax than the "opt-in" consent-based rule, which some state spam laws favor. An appraisal of the Act's weaknesses should however be made in light of the imperatives for unencumbered e-commerce transactions. Besides, there are the First and Fourteenth Amendment constitutional quagmires, which have successfully scuttled Congress's previous attempts at Internet regulation. A stronger antispam legislation than the CAN-SPAM Act could equally end up in the clutches of the First Amendment.

VI. ANTISPAM REGULATION IN THE EUROPEAN UNION

In the European Union,[241] and the European Free Trade Association (EFTA),[242] (which make up the European Economic Area) spam is directly regulated by the Electronic Personal Data and Privacy Directive 2002/58/EC (E-Privacy Directive).[243] The directive covers all public electronic communications, and not just the Internet and computers. However, antispam provisions that are similar to the key provisions in the E-Privacy Directive can be found scattered in previous directives generally regulating electronic commerce.[244] The analysis of the EU antispam regulation will be focused on the E-Privacy Directive, and its implementation in selected member states.

---

241. The European Union comprises 25 member countries: Austria, Belgium, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden, and the United Kingdom.

242. The EFTA members are Iceland, Liechtenstein, Norway and Switzerland. The EFTA Convention established a free trade area among its member states in 1960. *See* European Free Trade Ass'n, *at* http://www.efta.int (last visited Mar. 15, 2005).

243. *See* E-Privacy Directive, *supra* note 9, art. 1. The E-Privacy Directive seeks to harmonize

> the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the electronic communication sector and to ensure free movement of such data and electronic communication equipment and services in the Community.

Id. art. 1(1).

244. *See* Council Directive 2000/31/EC of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market, art. 6, 2000 O.J. (L 178) 1. Article 6(a) of this directive requires that "commercial communications" be clearly identified as such. *See also* Council Directive 84/450, 1984 O.J. (L 250) 17 (concerning misleading advertising); Council Directive 95/46 on the Protection of Individuals with Regards to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31; Council Directive 97/7 on the Protection of Consumers in Respect of Distance Contracts, 1997 O.J. (L 144) 19.

The first key provision of the E-Privacy Directive is the requirement of prior consent of subscribers before transmission of unsolicited commercial e-mails for direct marketing.[245] This is otherwise known as "opt-in" consent-based e-mail traffic control, as distinct from the "opt-out" nonconsensual approach adopted by the CAN-SPAM Act. During negotiations of the E-Privacy Directive, Luxembourg was opposed to the opt-in strategy on grounds that it was "inappropriate,"[246] "disproportional,"[247] and "pointless."[248] Nevertheless, most member countries have implemented the opt-in policy and the provisions of the E-Privacy Directive.[249]

One of the rationales for the opt-in policy was to safeguard the privacy of Internet subscribers, a key policy of the European electronic commerce governance.[250] However, whether or not the opt-in policy would survive the European Court of Justice (ECJ) would invariably depend on whether or not the Court perceives it as a restriction on advertising rules. In *KO v. Gourmet International Products AB*,[251] the ECJ held that a prohibition of all advertising directed at consumers (such as advertisements in the press, on the radio, and on television, the direct mailing of unsolicited material, or the placing of posters on the public highway) of alcoholic beverages, the consumption of which is linked to traditional social practices and to local habits and customs, is liable to impede access to the market by products from other member states more than it impedes access by domestic products, with which consumers are

245. *See* E-Privacy Directive, *supra* note 9, art. 13(1).

246. The inappropriateness claim was based on the argument that the opt-in proposal exceeded the objective of the E-Privacy Directive, while the opt-out provided the minimum requirement which member states could change to opt-in, if they wished. *See* Statement by the Luxembourg Delegation on Article 13(1), *available at* http://www.euro.cauce.org/en/countries/c_lu.html (last visited Feb. 20, 2005).

247. The charge of the opt-in policy's disproportionality was premised on the claim that it was too overbearing, and could prevent young businesses who could not afford other media of advertising, from getting to their potential customers. *Id.*

248. The reason adduced for this charge was that an opt-in policy would never stem the tide of spam that originates from foreign countries, but would rather unduly penalize European businesses. *Id.*

249. For instance, Spain's article 21(1) of the Law on the Information Society and Electronic Commerce (L.O. 2002, 34), incorporated the opt-in policy. It provides: "The distribution of promotional or advertising communications by electronic mail or equivalent electronic means, is forbidden if they have not been solicited before or if they have not been explicitly authorized by the recipient." *Id.* Regulation 22(2) of the United Kingdom Privacy and Electronic Communications (EC Directive) Regulations, SI 2003/2426, provides that unsolicited electronic communications shall not be sent without the previous consent of recipients. *See supra* note 17 and accompanying text.

250. *See* Spam Communication, *supra* note 12.

251. Case C-405/98, 2001 E.C.R. I-1795 (2001).

instantly more familiar. The Court further held, however, that such a restriction could be justified on grounds of public health protection. It remains to be seen whether European courts would uphold the opt-in spam policy on privacy grounds, in the face of a possible advertisement restrictions challenge.

The second key provision of the E-Privacy Directive allows businesses to use customers' electronic contact details, acquired in the course of commercial transactions for future direct marketing of similar products or services.[252] However, customers must be given an opportunity to object free of charge to such use of their electronic contact details.[253] This provision does not arguably detract from the opt-in policy since customers' prior consent is crucial for its implementation. The Directive seems at pains to maintain an even balance between customers' privacy rights and businesses' legitimate advertising. This is the greatest challenge to all forms of antispam measures.[254]

The third key provision of the Directive is its prohibition of disguising or concealment of the identity of the sender of unsolicited e-mail messages, or the sending of an unsolicited electronic mail without a valid return address of the sender's e-mail for the purpose of direct marketing.[255] This is *in pari materia* with the labeling and accurate header provisions in section 5 of the United States' CAN-SPAM Act, and could raise similar anonymity and free speech issues in Europe.

Europe has long recognized e-commerce's high propensity for intruding directly or indirectly on privacy.[256] Specifically, articles 8(1)

---

252. *See* E-Privacy Directive, *supra* note 9, art. 13(2).

253. *See id.*

254. It is always important to maintain an even regulatory balance between the conflicting interests of all Internet users if electronic commerce were to achieve its potentials. For example, the European Parliament and the European Council have repeatedly stated their commitment towards the development of e-commerce. This is reflected in Directive 2000/31/EC, which states:

> The development of electronic commerce within the information society offers significant employment opportunities in the Community, particularly in small and medium-sized enterprises, and will stimulate economic growth and investment in innovation by European companies, and can also enhance the competitiveness of European industry, provided that everyone has access to the Internet.

Directive 2001/31/EC of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market, ¶ 1, 2000 O.J. (L 178) 1.

255. E-Privacy Directive, *supra* note 9, art. 13(4).

256. *See* Henrik W.K. Kaspersen, *Data Protection and E-commerce*, *in* ARNO R. LODDER & HENRICK W.K. KASPERSEN, EDIRECTIVES: GUIDE TO EUROPEAN UNION LAW ON E-COMMERCE 119-45 (2002).

and (2) of the European Convention on Human Rights[257] guarantee the right to privacy and family life. According to Henrik W.K. Kaspersen, respect for private life has been established as a human right in a number of the European Court of Human Rights decisions in Strasbourg.[258] For instance, in *Perry v. United Kingdom*,[259] the European Court of Human Rights defined "private life" broadly as follows:

> "Private life" is a broad term not susceptible to exhaustive definition. Aspects such as gender identification, name, sexual orientation and sexual life are important elements of the personal sphere protected by Art.8. The Article also protects a right to identity and personal development, and the right to establish and develop relationships with other human beings and the outside world and it may include activities of a professional or business nature. There is, therefore, a zone of interaction of a person with others, even in a public context, which may fall within the scope of "private life."[260]

It would be interesting to know how national courts and the European Court of Human Rights would interpret the Directive's accurate header provision. Would courts in Europe justify the accurate header and labeling provisions on the imperatives of the sanctity of privacy and family life as guaranteed by article 8 of the European Convention on Human Rights?[261] Or would they hold that the provisions are prior restraints on free speech, and therefore in violation of article 10 of the European Convention on Human Rights?[262] In *Gaweda v.*

---

257. Nov. 4, 1950, art. 8, Eur. T.S. No. 005. Article 8(1) provides: "Everyone has the right to respect for his private and family life, his home and his correspondence." Article 8(2) provides:

> There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

258. *See* Kaspersen, *supra* note 256, at 119.

259. 39 Eur. H.R. Rep. 76 (2004).

260. *Id.* at 85 (citation omitted).

261. Other comparative international human rights provisions on the sanctity of privacy and family life, to which the European Union is signatory are article 12 of the Universal Declaration of Human Rights and article 17 of the International Convention on Civil and Political Rights. *See* Kaspersen, *supra* note 256, at 119.

262. Nov. 4, 1950, art. 10, Eur. T.S. No. 005. Article 10(1) of the Convention provides: "Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises." *Id.* This right is however subject to the limitations under article 10(2) of the Convention, which provides:

> The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by

Poland,[263] the European Court of Human Rights, while interpreting article 10 of the Human Rights Convention on Freedom of Expression, held:

> Subject to Art.10(2), freedom of expression is applicable not only to "information" or "ideas" that are favorably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb. Such are the demands of that pluralism, tolerance and broadmindedness without which there is no "democratic society."[264]

The greatest challenge here for European courts is to maintain a balance between competing privacy and free speech rights. The fate of article 13(4)(d) of the E-Privacy Directive on accurate header and labeling of unsolicited electronic messages for direct marketing purposes, would depend on where the balance tilts.

Significantly, article 15(2) of the E-Privacy Directive incorporates article 22 of the Data Protection Directive,[265] which allows individuals in member countries to sue for an alleged breach of any of the provisions of national antispam legislations. This is a marked difference from the CAN-SPAM Act, where there is no express statutory right to file a civil suit for an alleged infringement of any of its provisions.[266] However, it remains to be seen whether a U.S. subscriber or a recipient of unsolicited electronic messages (apart from ISPs) could take advantage of the U.S.

> law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

Id. For instance, in a Report Commissioned by UNESCO, the right of communication was deemed a fundamental human right. The Report also stated that every citizen should have the right to meaningful participation in the information society. *See* Report of the Experts Meeting on Cyberspace Law, *at* http://unesdoc.unesco.org/images/0011/001163/116300e.pdf (Feb. 22, 1999).

263. 39 Eur. H.R. Rep. 90 (2004).

264. *Id.* at 97 (citation omitted). The court held further that "Art. 10 does not in terms prohibit the imposition of prior restraints on publications. However, the dangers inherent in prior restraints are such that they call for the most careful scrutiny." *Id.* at 98 (citation omitted).

265. *See* E-Privacy Directive, *supra* note 9, art. 15(2); Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regards to the Processing of Personal Data and on the Free Movement of Such Data, art. 22, 1995 O.J. (L 281) 31 [hereinafter Data Protection Directive].

266. Apart from the FTC and the Attorneys Generals only the ISPs can sue under the CAN-SPAM Act. Recently, the major ISPs, Yahoo!, Microsoft, and AOL, announced the combined filing of six lawsuits against hundreds of alleged spammers. This was the first major industry lawsuit under the CAN-SPAM Act. *See* Yahoo! Press Release, America Online, Earthlink, Microsoft, and Yahoo! Team up to File First Major Industry Lawsuits Under New Federal Anti-Spam Laws, *at* http://docs.yahoo.com/docs/pr/release1145.html (Mar. 10, 2004).

judgment in *CompuServe*[267] to support a cause of action for trespass to property. Furthermore, article 15(3) of the E-Privacy Directive incorporates article 30(1)(c) of the Data Protection Directive.[268]

This Part analyzed spam regulation in the European Union. The key provisions of opt-in policy and accurate header of information in unsolicited commercial e-mails are noted. The Article posed the question of how the European Court of Justice might interpret the opt-in policy. Would it be perceived as a restraint on advertising in the context of the ECJ decision in *Gourmet International Products AB* because of its possible impediment to access by potential customers to advertisers' goods and services in member states? Or would it be perceived as a legitimate restriction, which is arguably justifiable on grounds of sanctity of privacy? The Article also examined how the European Court of Human Rights might interpret the accurate labeling and header of information in unsolicited commercial messages provisions. Would the court hold the provisions in violations of article 10 of the European Human Rights Convention? As with the United States' CAN-SPAM Act, these are some of the major long-term challenges facing antispam laws in Europe and the United States.

---

267. The *CompuServe* court accepted that the junk-mailer "intentionally intermeddled" with another's property and held that electronic signals generated and sent by computer are sufficiently physically tangible to constitute intermeddling. Occupying the disc space and draining the processing power of the plaintiff's computer equipment, together with the resulting loss of goodwill, was sufficiently injurious to maintain an action for trespass to chattel. *Id.* at 1028; *see also* Michael A. Fisher, *The Right to Spam? Regulating Electronic Junk Mail*, 23 COLUM.-VLA J.L. & ARTS 363, 383-88 (2000). In his remarks on the *CompuServe* case, Fisher opined that the court's concern about the inherent cost-shifting quality of spam was an important factor in its recognition that the public interest is advanced by allowing ISPs to block unsolicited electronic advertisements. *Id.* at 419; *see also* Michael W. Carroll, *Garbage in: Emerging Media and Regulation of Unsolicited Commercial Communications*, 11 BERKELEY TECH. L.J. 233, 259-71 (1996).

268. E-Privacy Directive, *supra* note 9, art. 15(3); Data Protection Directive, *supra* note 265, art. 30(1)(c). Article 30(1)(c) of the Data Protection Directive provides that the Working Party on the Protection of Individuals with Regard to the Processing of Personal Data shall

> advise the Commission on any proposed amendment of this Directive, on any additional or specific measures to safeguard the rights and freedoms of natural persons with regards to the processing of personal data and on any other proposed Community measures affecting such rights and freedoms.

Article 30(6) further provides:

> The Working Party shall draw up an annual report on the situation regarding the protection of natural persons with regard to the processing of personal data in the Community and in third countries, which it shall transmit to the Commission, the European Parliament and the Council. The report shall be made public.

VII. TECHNICAL MEASURES AGAINST SPAM

The inexorable rise in the volume of unsolicited commercial electronic messages and the inherent limitations of regulatory regimes make a technical solution to combating spam imperative. The United States Congress acknowledges in its policy statement that technological measures are crucial to a successful antispam regime.[269] As spam flourishes, so have antispam companies, in a lucrative and thriving content security and antispam software market, which is expected to reach $952 million in 2004.[270]

Antispam software is generally designed to filter out spam using the following methodologies: Black/white list filtering, Integrity Check, Heuristics, Content/keyword filtering, and Reverse DNS lookup.[271] All of the five solutions or just one or two, could be used, depending on the need of the client. A blacklist comprises domain names, mail servers, or specific e-mail accounts that have been listed for identification and blockade by the software solution.[272] The list could be drawn up by the client or by the software vendor to client's specification.[273] The whitelist on the other hand comprises e-mail addresses that are allowed, even if they bear the hallmarks of spam.[274]

A likely effect of spam filtering technology is privacy intrusion. Filtering is facilitated by spam laws' requirement of labeling and accurate information headers on unsolicited commercial electronic messages. The process of filtering out unwanted spam would necessarily involve message profiling, with software solutions on the lookout for words like "ADV" and "Sexually explicit message."[275] It has been argued that this is no more than "message screening," which is intrusive and violative of unsolicited commercial e-mail senders' privacy.[276] From previous

---

269. *See* 15 U.S.C.A. § 7702(12) (Supp. VI 2004).

270. Existing antispam companies include: Plus, MailWasher, ePrompter, Spamex, BVRP USA/Mail Warden, SpamCop, Brightmail. *See* Ryman, *supra* note 40, at 15.

271. *See* Thomas A. Knox, *Technologies to Combat Spam*, *at* http://www.sans.org/rr/papers/index.php?id=1130 (June 16, 2003). Heuristics involves the application of a solution that makes it impossible to fool or trick antispam software by the use of incorrect spellings, or words inversion. *Id.* at 5. Content/keyword filtering involves checking key words or content of messages with a view to determining whether they match spam characteristics or features. *Id.* Reverse DNS lookup allows a server that is receiving e-mails to match up the IP address of the sending server and perform a DNS analysis on that address to see if it matches the header information of the e-mail. *Id.* at 6.

272. *Id.* at 4.

273. *Id.*

274. *Id.* at 5.

275. *See* Ryman, *supra* note 40, at 17; Steven Miller, Note, *Washington's "Spam Killing Statute": Does It Slaughter Privacy in the Process?*, 74 WASH L. REV. 453, 459 (1999).

276. *See* Miller, *supra* note 275, at 476-80.

analyses in this Article, it is clear that the privacy intrusion argument is no less valid for the senders of unsolicited commercial e-mails than the recipients. The crucial challenge for both antispam laws and technologies is how to balance these conflicting interests.

A major downside of the filtering technology is its propensity to filter out nonspam, and sometimes, important messages. Contrary to popular claims by various antispam technology companies, spam filtering has not been 100% successful. The ever-increasing rise in spam volume belies this assertion. It has been correctly pointed out that there is no "silver bullet" solution to spam control.[277] Although spam proliferation could be minimized, it would take the combined efforts of an effective legal regime, self-regulation, and technological solutions to achieve the feat. Spam may have become a permanent feature of our cyberspace.

VIII. CONCLUSIONS

This Article examined the legislative response in the United States and the European Union to spam proliferation, and the prospects for a successful antispam campaign. It is noted that the legal regimes on both sides of the Atlantic try to balance the conflicting interests of spam senders and recipients without much success, and to the displeasure of both antispam and prospam campaigners. With both sides employing privacy and free speech rights to rally their cause, maintaining an even balance between the two conflicting interests is nigh impossible, and remains the greatest challenge to both the CAN-SPAM Act and the E-Privacy Directive. The failure of regulation in this respect is symptomatic of the intractable nature of cyberspace, and the limited effects that regulation could have on netizens.

The Article also examined the prospects for success of spam regulations in the context of free speech rights, marketing rights, and privacy rights. In the United States, the Article noted the vulnerability of state spam laws to the constitutional dormant Commerce Clause, which prohibits states from extra-territorial regulation of commerce in a manner that could prejudice sister states. The Article argued that the Commerce Clause constitutional hurdle is obviated by the federal spam law's preemption of state spam laws, and also provides a homogeneous and arguably better front in the battle against spam.

The Article also analyzed the prospects for the labeling and accurate information header provisions of the United States' CAN-SPAM Act, and

277. *See* Spam Communication, *supra* note 12.

the European Union E-Privacy Directive, vis-à-vis anonymity and freedom of communication rights. It is argued that it was unlikely that the courts in the United States, the European Union, and individual member states would strike the provisions down for free speech infractions. This conclusion was drawn from the common trends in analogous cases from both jurisdictions, which hold there is no absolute free speech right. The right to freely speak is no less important than the right to choose not to listen, which the labeling and accurate information header provisions arguably support. This proposition finds support in the United States Supreme Court decision in *Rowan*.[278] The *Rowan* Court held that "a mailer's right to communicate must stop at the mailbox of an unreceptive addressee."[279]

The Article noted the lack of a definite legal regime for control of transnational spam traffic as a serious derogation from the effectiveness of both the CAN-SPAM Act and the E-Privacy Directive. There is an urgent need for a transnational legal regime for transborder spam control, and a transnational legal structure for enforcement of foreign judgments against transnational spam traffic that violates national laws. International cooperation among all nations is indispensable to effective transnational spam regulation and control.

The Article finally examined the relevance of technological antispam measures. While they play a crucial role in the antispam crusade, they are not 100% effective. Besides, filtering technology often filters out important, nonspam mails. Furthermore, filtering technology suffers from privacy invasion charges. The Article reiterates the theory that neither regulation nor technology alone could tackle the spam phenomenon. It would take the combined efforts of an effective legal regime and cutting-edge antispam technology to rein in the spam epidemic, not only in the United States and Europe, but worldwide.

278. 397 U.S. 728 (1970).
279. *Id.* at 736-37.