PEPPERDINE UNIVERSITY

Pepperdine Law Review

Volume 32 | Issue 4 Article 9

5-15-2005

Is Spam the Rock of Sisyphus?: Whether The Can-Spam Act and Its Global Counterparts Will Delete Your E-mail

Amy G. Marino

Follow this and additional works at: https://digitalcommons.pepperdine.edu/plr

 Part of the Civil Procedure Commons, Computer Law Commons, and the First Amendment Commons

Recommended Citation

Amy G. Marino *Is Spam the Rock of Sisyphus?: Whether The Can-Spam Act and Its Global Counterparts Will Delete Your E-mail*, 32 Pepp. L. Rev. Iss. 4 (2005)
Available at: https://digitalcommons.pepperdine.edu/plr/vol32/iss4/9

This Comment is brought to you for free and open access by the Caruso School of Law at Pepperdine Digital Commons. It has been accepted for inclusion in Pepperdine Law Review by an authorized editor of Pepperdine Digital Commons. For more information, please contact bailey.berry@pepperdine.edu.

Is Spam the Rock of Sisyphus?[1]: Whether The Can-Spam Act and Its Global Counterparts Will Delete Your E-mail

TABLE OF CONTENTS

1. Sisyphus was the mythological Greek character who betrayed the secrets of the gods, and was condemned to push a boulder uphill for eternity. *See* Micha F. Lindemans, *Sisyphus*, Encyclopedia Mythica, *at* http://www.pantheon.org/articles/s/sisyphus.html (last modified Apr. 10, 2001). Each time he reached the top, the boulder would tumble back down to the bottom of the hill. *See id.*

I. INTRODUCTION

Unsolicited commercial electronic mail (UCE), also known as "spam," has far surpassed legitimate electronic mail (e-mail) in online inboxes around the world.[2] Spam accounted for fifty-six per cent of all e-mail in 2003, and is projected to increase to seventy per cent by 2007.[3] This massive influx of spam has contributed to loss of time and money by both businesses and individuals.[4] According to consulting firm Ferris Research, spam will cost global companies more than fifty billion dollars in 2005.[5] Some users spend thirty to sixty minutes a day sorting through spam e-mail and some claim that "it's less aggravating to clean a toilet than to muck around with 'spam.'"[6]

---

2. *See* Michael Zuzel, *Is 'Spam' Overflowing? Just Learn to Live With It*, THE MASTHEAD, http://www.findarticles.com/p/articles/mi_qa3771/is_200301/ai_n9228461 (last visited Mar. 14, 2005). The term "spam" most likely derives from a Monty Python skit in which two diners entered a restaurant, and every item on the menu contained Hormel spam. *See* Joshua A. Marcus, *Commercial Speech On the Internet: Spam and the First Amendment*, 16 CARDOZO ARTS & ENT. L.J. 245, 247 n.14 (1998). The hosts denied the diners requests for a meal without spam, and eventually everyone in the restaurant was singing "spam." *Id.*

3. Zuzel, *supra* note 2.

4. Marcus, *supra* note 2, at 247. Some common spam topics are: pyramid schemes, "Get Rich Quick" schemes, chain letters, pornographic offers, quack health products, and illegally pirated software. *See The Problem*, *at* http://www.cauce.org/about/problem.shtml (last visited Mar. 14, 2005).

5. Richi Jennings, *The Cost of Spam Webinar* (Mar. 5, 2005), *at* http://www.ferris.com/view_content.php?o=Spam+Control&id=719&ferrisresearch_main_PSID=a47d242fe2d992ec3d7e514accd4b7ed (last visited Mar. 24, 2005).

6. Zuzel, *supra* note 2.

In an attempt to minimize its volume, states have enacted anti-spam legislation that ranges from requiring specific labels to be included in e-mail subject lines to prohibiting the sending of unsolicited e-mail altogether.[7] Most recently, California put forward an "opt-in" statute, which requires the explicit consent of the recipient prior to sending any commercial e-mail.[8]

There are, however, some constitutional problems with anti-spam legislation. The dormant Commerce Clause, which applies to all state laws that affect interstate commerce, prevents state legislatures from applying their anti-spam statutes to spammers outside the state.[9] The First Amendment, which guarantees some protections to commercial speech, also plays a large role in the scope of restrictions intended to reduce commercial e-mail.[10]

The federal government became involved in the legislative game by enacting the Can-Spam Act in December 2003.[11] That Act contains a variety of provisions to ensure that senders of e-mail do not falsify their origins and what they are claiming to sell. It also mandates that all commercial e-mail messages contain a legitimate reply address by which recipients can opt-out of future mailings.[12]

Critics have said that the Act has done nothing more than legalize spam, and that it has failed to decrease the amount of spam.[13] Also, as a result of the legislation, more stringent opt-in schemes, like California's, are pre-empted by the less restrictive federal law.[14]

Meanwhile, in European countries, the Directive on Privacy and Electronic Communications promulgates an opt-in provision similar to that of California's pre-empted law.[15] The Directive is currently being transposed into E.U. member countries' laws. Critics remain skeptical about that Directive's effect though, since what constitutes "consent" for purposes of opting-in is relatively low and easy for marketers to circumvent.[16]

As a result of ineffective laws, spam continues to grow and infiltrate our

---

7. *See* David E. Sorkin, *Spam Laws*, *at* http://www.spamlaws.com/state (last visited Mar. 14, 2005).

8. *See, e.g.*, CAL. BUS. & PROF. CODE §§ 17529-.9 (West Supp. 2005).

9. *See* Troy L. Booher & Mark Morris, *A Case for National E-mail Regulation: State UCE Statutes Have Infirmities*, 70 DEF. COUNS. J. 355, 360 (2003).

10. *See infra* Part III.A.1. for a full discussion of the Commercial Speech Doctrine.

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

12. *Id.* § 5(a)(3)(A)(i).

13. *See* David Ho, *Anti-Spam Measures Fail to Foil Rise in Junk E-mail*, PALM BEACH POST, Jan. 27, 2005, at 7D.

14. Controlling the Assault of Non-Solicited Pornography and Marketing Act § 8(b)1.

15. Council Directive 2002/58/EC, 2002 O.J. (L 201) 37 (2002) [hereinafter Dir. 2002/58/EC], *available at* http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf.

16. *See* Danny Lee, *Spam Too Slippery for the Law*, TIMES NEWSPAPERS, LTD., Dec. 16, 2003, at 8.

personal and professional lives. The issue remains whether it will ever be eliminated, or whether the law is simply the hand of Sisyphus, ever pushing the rock of spam uphill, where, when it believes it has reached the top, will simply roll back down with a flood of new issues to invade our inboxes evermore.

In Part II, this comment will take a look at the history of state actions and legislation that have confronted the spam issue. Part III will analyze the constitutional issues that courts have encountered, such as First Amendment rights, personal jurisdiction, and the dormant Commerce Clause. Part IV will include a discussion and constitutional analysis of the recently enacted Can-Spam Act of 2003. In Part V, anti-spam provisions in Europe, such as the Directive on Privacy and Electronic Communications in Europe, will be explored. Finally, in Part VI, a look at self-regulation measures and recently adopted technologies will leave us with the question of whether spam will ever be completely deleted.

II. HISTORY OF ANTI-SPAM ACTIONS AND STATE LEGISLATION

Before there was spam, there was junk mail. Sweepstakes entries and pornographic magazines alike found their way to the private mailboxes of hapless individuals with little power to control what the eyes were to find. That was, until the landmark case of *Rowan v. U.S. Post Office Dep't.*[17] *Rowan* upheld the constitutionality of a section of the Postal Revenue and Federal Salary Act that prohibited "'pandering advertisements in the mails.'"[18] The Court weighed the right to communicate against the right to be "free from sights, sounds, and tangible matter we do not want," and reasoned that a "mailer's right to communicate must stop at the mailbox of an unreceptive addressee."[19] Thus, the recipient was given some power to control what landed in his mailbox.

After junk mail, direct marketers turned to the telephone as another source of attracting business. Calls advertising the next best vacation plan became (and sometimes still are) the source of great frustration for families sitting down to dinner when the phone rang. Businesses also suffered from blocked lines on their facsimiles while they received offer after offer of unnecessary and sometimes fictitious services.[20] Then, the Telephone Consumer Protection Act of 1991 (TCPA) was amended to prohibit unsolicited faxes and prerecorded calls to residential numbers and businesses.[21]

---

17. 397 U.S. 728 (1970).

18. *Id.* at 729. At issue was Title III of the Postal Revenue and Federal Salary Act of 1967, which allowed an individual recipient to require a mailer to "remove his name from its mailing lists and stop all future mailings to the householder." *Id.* The section was a "response to public and congressional concern with use of mail facilities to distribute unsolicited advertisements that recipients found to be offensive because of their lewd and salacious character." *Id.* at 731.

19. *Id.* at 736-37.

20. *See generally* Destination Ventures, Ltd. v. FCC, 46 F.3d 54 (1995).

21. *See* 47 U.S.C. § 227(b)(1)(B)-(C).

A new advertising medium was discovered in 1978 by one Gary Thuerk, a marketing manager for Digital Equipment Corporation, who sent out an ad for "real estate open houses over a network of government and university computers."[22] Although network administrators warned him not to do it again, and the medium went quiet for over a decade, electronic marketing quickly took off again when the Internet became a major tool for mass communication in the early 1990s.[23]

Electronic solicitation took charge when two lawyers in Arizona in 1994 posted a Green Card immigration ad on over six thousand Usenet news groups.[24] By generating around thirty thousand e-mail messages with a mere thirty dollars, the lawyers generated fifty thousand dollars in business.[25] The Internet quickly became a popular medium for advertising, largely due to the low cost of reaching millions of consumers instantaneously, and the assumption that Internet users were typically more educated and financially sound.[26]

Quickly thereafter, spam slammed e-mail inboxes with the potency of the famous meat-replacement in the Monty Python skit.[27] Because e-mail viewers were charged by the minute to read their content, and unlikely to discern ad mail from regular mail, the resulting cost shift from advertisers to consumers became an immediate attraction to marketers and political activists alike.[28]

A. Civil Anti-Spam Actions

1. Trespass to Chattels

Along with the increase of spam came an onslaught of cases under various action headings. Trespass to chattels was a common action due to a number of lawsuits brought by AOL in the Eastern District of Virginia,[29] as

22. Matthew Heller, *Lost In The Cyber-Kudzu; "Legitimate" Internet Marketers Such as L.A.'s Alyx Sachs Have Built an Industry Around the Assumption That You Thoughtfully Evaluate Each Unfamiliar E-Mail Before Hitting the "Delete" Button. You Still Do That, Right?*, L.A. TIMES MAGAZINE, Dec. 12, 2003, at 24. The network was the forerunner of the Internet. *Id.*

23. *Id.*

24. Marcus, *supra* note 2, at 248 (citing Peter H. Lewis, *Advertiser Unfazed By Internet Outrage*, SAN DIEGO UNION & TRIB., Apr. 26, 1994, at 3). Usenet groups are online forums through which users can communicate in real-time on various topics of interest. *See, e.g.*, Google Groups, http:/groups.google.com (last visited Mar. 14, 2005).

25. Marcus, *supra* note 2, at 248.

26. *Id.*

27. *See supra* note 2.

28. Marcus, *supra* note 2, at 249.

29. *See* Am. Online, Inc. v. IMS, 24 F. Supp. 2d 548 (E.D. Va. 1998); Am. Online, Inc., v. LCGM, Inc., 46 F. Supp. 2d 444 (E.D. Va. 1998); America Online, Inc. v. GreatDeals.Net, 49 F. Supp. 2d 851 (E.D. Va. 1999).

well as the notable *CompuServe, Inc. v. Cyber Promotions, Inc.*[30] in the Southern District of Ohio in 1997. In *CompuServe*, the defendants took advantage of the plaintiff's online subscriber service by sending thousands of unsolicited advertisements via electronic mail to CompuServe's subscribers, despite CompuServe's requests to stop.[31] The Ohio court relied on the Restatement (Second) of Torts § 217(b), which provides that "a trespass to chattel may be committed by intentionally using or intermeddling with the chattel in possession of another,"[32] to find that the defendant's intrusion into CompuServe's systems was sufficiently tangible to constitute trespass.[33] The court reasoned that the loss of disk space and processing power caused harm to CompuServe's business reputation and the goodwill of its customers.[34]

The action was upheld against the defendant's arguments that CompuServe had consented to its use by providing a service that allowed subscribers to receive e-mail from anyone on the Internet.[35] Because CompuServe had notified the defendant that it no longer consented to its use of the computer equipment, and because the CompuServe policy denied unauthorized parties the ability to send unsolicited e-mail, the defendant's continued use was a trespass.[36]

2. False Designation of Origin and Trademark Dilution

In *America Online, Inc. v. IMS*, plaintiffs brought two additional actions against a spammer for false designation of origin and trademark dilution under the Lanham Act.[37] The Lanham Act "is designed to make actionable the misleading use of marks in interstate commerce and to protect those engaged in interstate commerce against unfair competition."[38]

To find defendants liable under false designation of origin, the plaintiffs in *AOL* had to prove the elements of a three part test: "(1) the alleged violator must employ a false designation; (2) the false designation must deceive as to origin, ownership or sponsorship; and (3) the plaintiff must

30. 962 F. Supp. 1015 (S.D. Ohio 1997).

31. *Id.* at 1017.

32. *Id.*

33. *Id.*

34. *Id. See also* America Online, Inc. v. IMS, 24 F. Supp. 2d 548, 551 (E.D. Va. 1998) (holding that defendant's intentional and unauthorized transmission of 60 million unsolicited e-mails resulted in AOL's loss of goodwill and business, and was unquestionably actionable in trespass).

35. *CompuServe*, 962 F. Supp. at 1023-24.

36. *Id.* at 1024. The court relied on Restatement (Second) of Torts § 217, Comment f, which states: "The actor may commit a new trespass by continuing an intermeddling which he has already begun, with or without the consent of the person in possession. Such intermeddling may persist after the other's consent, originally given, has been terminated." *See id.* (citation and internal quotation marks omitted). *Cf.* Intel Corp. v. Hamidi, 71 P.3d 296 (Cal. 2003) (denying an injunction for an action in trespass against a defendant who transmitted multiple e-mails through his former employer's computer system, but caused no physical damage or functional disruption).

37. *IMS*, 24 F. Supp. 2d at 548.

38. *Id.* at 551.

believe that 'he or she is likely to be damaged by such [an] act.'"[39] The court in *AOL* found that because defendant's messages contained "aol.com" in the header, they were likely to cause confusion as to the source of origin.[40] Furthermore, AOL members were actually deceived into thinking that AOL approved of the defendant's bulk mailing tactics, and such confusion caused damage to AOL's business.[41]

In response to the action for trademark dilution, the court applied § 1125(c) of the Lanham Act to assess whether another person's use of AOL's famous mark diluted its distinctive quality.[42] AOL was required to show ownership of the mark and the likelihood of dilution, through either "blurring" or "tarnishment."[43] The court found that plaintiffs clearly owned the AOL mark, since it was registered with the U.S. Patent and Trademark Office, and it was "used and recognized throughout the world" in connection with its online products and services.[44] AOL also proved the likelihood of dilution by pointing to more than 50,000 complaints a day regarding the defendant's junk e-mail.[45] As a result, AOL was entitled to summary judgment on both counts.[46]

3. Breach of Contract

Plaintiffs have also been successful in suing spammers for breach of contract. In *Hotmail Corp. v. Van$ Money Pie Inc.*,[47] a California district

---

39. *Id.* at 551 (citing 15 U.S.C. § 1125(a)(1)). *See also* America Online, Inc., v. LCGM, Inc., 46 F. Supp. 2d 444 (E.D. Va. 1998). This case established a five part test for false designation of origin: "(1) a defendant uses a designation; (2) in interstate commerce; (3) in connection with goods and services; (4) which designation is likely to cause confusion, mistake or deception as to origin, sponsorship, or approval of defendant's goods or services; and (5) plaintiff has been or is likely to be damaged by these acts." *Id.* at 449.

40. *IMS*, 24 F. Supp. 2d at 551.

41. *Id.*

42. *Id.* at 552. *See also* 15 U.S.C. § 1125(c).

43. *IMS*, 24 F. Supp. 2d at 552. "[D]ilution by 'blurring' may occur where the defendant uses or modifies *the plaintiff's trademark* to identify *the defendant's goods and services,* raising the possibility that the mark will lose its ability to serve as a unique identifier of the plaintiff's product." Deere & Co. v. MTD Prods., Inc., 41 F.3d 39, 43 (2d Cir. 1994) (emphasis in original). "'Tarnishment' generally arises when the plaintiff's trademark is linked to products of shoddy quality, or is portrayed in an unwholesome or unsavory context likely to evoke unflattering thoughts about the owner's product." *Id.*

44. *IMS*, 24 F. Supp. 2d at 552.

45. *Id.* at 552. *See also* America Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444 (E.D. Va. 1998) (upholding actions under the Lanham Act, Computer Fraud and Abuse Act, Virginia's Computer Crimes Act, and trespass to chattels).

46. *IMS*, 24 F. Supp. 2d at 552. The amount of damages awarded to AOL was deferred until a Report and Recommendation was issued, detailing the proof. *See id.*; *see also* Classified Ventures v. Softcell Mktg., Inc., 109 F. Supp. 2d 898, 901 (N.D. Ill. 2000) (finding that defendant's unauthorized use of the plaintiff's "name and mark in connection with defendant's spam e-mail messages constitute[d] service mark infringement, dilution and unfair competition").

47. 1998 U.S. Dist. LEXIS 10729 (N.D. Cal. 1998).

court found that by obtaining a number of Hotmail's mailboxes and using them to facilitate the sending of spam and pornography, defendants expressly breached Hotmail's "Terms of Service."[48]

Similarly, a Canadian court upheld a counterclaim for breach of "emerging principles of Netiquette" where plaintiffs sent bulk e-mail at the rate of 200,000 e-mails per day.[49] The plaintiff's actions were contrary to a contractual provision with the Internet service provider that users would agree to follow accepted "Netiquette" when sending e-mail messages.[50] This "breach of Netiquette" principle was analogized to a breach of contract, and the court dismissed the plaintiffs' claim in favor of the defendant.[51]

4. Remedies

Civil actions against spammers have also resulted in injunctions, money damages, or both. In *Register.com v. Verio, Inc.*, for example, the plaintiff sought an injunction barring defendant from using automated software to access and collect information for the purpose of mass marketing.[52] The District Court of New York granted a preliminary injunction because the plaintiff was able to show that it would suffer irreparable harm without such relief, and it was likely to succeed on claims of unfair competition and false designation of origin.[53] Alternatively, plaintiffs received damages in *America Online, Inc. v. National Health Care Discount, Inc.*, where the Northern District Court of Iowa found that defendant's e-mailers, who had sent 135 million pieces of e-mail to the plaintiff ISP's members, had committed an actionable trespass.[54] The defendants were liable for $2.50 per thousand pieces of unsolicited bulk e-mail, for total actual damages in

---

48. *Id.* at *16-17. The "Terms of Service" specifically prohibited the unauthorized use of commercial e-mail and pornography. *Id.* at *17. The court in that case also upheld actions under the Lanham Act, Computer Fraud and Abuse Act, Fraud and Misrepresentation, and Trespass to Chattels. *Id.* at *9-20.

49. *See* Ontario Inc. v. Nexx Online, Inc., [1999] O.R. 3d 40.

50. *Id.* at 41, 50. Plaintiffs here sued the defendants for breach of contact when the latter disconnected the plaintiff's website after it continued to send bulk e-mails. *Id.* However, "plaintiff [was] in breach of its terms justifying disconnection of service." *Id.* at 50. The court articulated six reasons why spam was considered "unacceptable":

> (1) the recipient pays far more, in time and trouble as well as money, than the sender does, unlike advertising through the postal service;
> (2) the recipient must take the time to request removal from the mailing list, and most spammers claim to remove names on request but rarely do so;
> (3) many spammers use intermediate systems without authorization to avoid blocks set up to avoid spam;
> (4) many spam messages are deceptive and partially or entirely fraudulent[;]
> (5) spammers often use false return addresses to avoid the cost of receiving responses;
> (6) some forms of spam are illegal in various jurisdictions in the United States.

Id. at 45-46.

51. *Id.*

52. Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238 (S.D.N.Y. 2000), *aff'd*, 356 F.3d 393 (2d Cir. 2004).

53. *Register.com, Inc.*, 126 F. Supp. 2d at 255.

54. America Online, Inc. v. Nat'l Health Care Disc., Inc., 174 F. Supp. 2d 890, 900 (N.D. Iowa 2001).

the amount of $337,500.[55]

Courts have even allowed substantial monetary damages against spammers. In *Earthlink, Inc. v. Carmack*, the court awarded a judgment of $16,409,640 against a spammer who had used stolen or bogus credit card and bank account numbers to fraudulently purchase hundreds of dial-up Internet accounts.[56] The extraordinary judgment in that case resulted from a combination of various costs incurred by Earthlink as a result of the defendant's violations, as well as punitive damages intended "to serve as a clear message . . . that such crime and misconduct will not be tolerated."[57]

In sum, without specific anti-spam legislation in place, it has been possible to sue spammers in common law tort and breach of contract actions, as well as under federal trademark and computer abuse statutes. Before the federal Can-Spam Act,[58] it appears from the cases cited above that the most successful actions were brought by large ISPs against the most egregious violators.[59] In response to the increasing number of common law actions, however, many states began to legislate against spam in an attempt to provide clearer criminal and civil remedies, and a forum through which injured companies and consumers, as well as ISPs, could rid the world of spam.[60]

B. State Legislation

In December 2003, thirty-six states had enacted some kind of legislation against spam.[61] These "Unsolicited Commercial E-mail" ("UCE") statutes usually fall into two categories: 1) provisions *against* the falsifying of information, such as inaccurate subject headers or untruthful routing information; and 2) provisions that *require* conduct, like subject matter labeling (e.g. "ADV: ADULT" for sexually explicit material) or "opt-out" mechanisms (allowing the recipient to unsubscribe from future mailings).[62] The first category usually withstands constitutional challenges and will not be discussed in detail here, while the latter may be subject to dormant

55. *Id.* at 901. The district court here permanently enjoined the defendant from sending further unsolicited e-mails through the plaintiff's system. *Id.* at 902.

56. Earthlink, Inc. v. Carmack, 2003 U.S. Dist. LEXIS 9963 (N.D. Ga. 2003).

57. *Id.* at *19.

58. *See infra* Part IV.

59. *See* cases cited *supra* Part II.A.

60. *See* Sorkin, *supra* note 7. Legislatures have also legitimized regulating spam due to the extraordinary amount of cost-shifting and burden imposed on consumers. *See* Jack L. Goldsmith & Alan O. Sykes, *The Internet and the Dormant Commerce Clause*, 110 YALE L.J. 785, 818 (2001) ("Bulk e-mail can raise costs to Internet service providers and Internet users in terms of wasted time, slower operating systems, lost accounts, repairs, equipment, and the like.").

61. *See* Sorkin, *supra* note 7.

62. Booher & Morris, *supra* note 9, at 360.

Commerce Clause and First Amendment scrutiny.[63]

For example, a statute from the second category was recently enacted in Texas.[64] That statute requires subject lines to begin with "ADV" for general advertisements and "ADV: ADULT ADVERTISEMENT" for any adult material.[65] Texas is also one of the few states to grant qualified immunity to Internet service providers (ISPs).[66] This allows ISPs to sue spammers for clogging their wires, but does not allow a spam recipient to sue the ISP for its role in spamming.[67]

Additionally, Utah passed the "Unsolicited Commercial and Sexually Explicit Email Act,"[68] allowing for hundreds of class action suits against both local and national defendants.[69] This Act requires "ADV" in the subject line for commercial e-mails, and "ADV: ADULT" for sexually explicit e-mails.[70]

Also in the second category, the Virginia anti-spam statute claims to be the toughest law, since nearly half of the world's Internet traffic passes through that state via AOL, Inc.[71] Spammers who produce the most offensive and persistent e-mail solicitations face a class six felony, which carries a prison term of between one and five years, plus a fine.[72] The law also authorizes the Attorney General to seize profits, computer equipment and all property connected with the crime.[73]

Most recently, California enacted an amendment to its existing anti-spam legislation, prohibiting advertisers from sending unsolicited commercial e-mail without the prior consent or existing business relationship of the recipient.[74] This "opt-in" amendment came into effect in January 2004.[75] The provision applies to all senders of unsolicited e-mail who are located in California, as well as those not located in California sending junk e-mail *to* California recipients.[76] The bill authorizes the recipient of unsolicited e-mail to recover actual damages, or liquidated

---

63. *See infra* Part III.

64. TEX. BUS. & COM. CODE ANN. §§ 46.001-.0011 (Vernon Supp. 2004).

65. *Id.* § 46.003.

66. *Id.* § 46.011.

67. John D. Saba, Jr., *eProclamation: No More Spam in Texas*, 66 TEXAS BAR J. 660.

68. UTAH CODE ANN. §§ 13-36-101-105 (Supp. 2004).

69. *See* Gregory M. Saylin & Spencer J. Cox, *The Unsolicited Email Act and Anti-Spam Litigation*, 16 UTAH B.J. 26 (2003).

70. UTAH CODE ANN. § 13-36-103.

71. *See* VA. CODE ANN. §§ 8.01-323.1, 18.2-152. (Michie 2003); *see also Virginia Claims Toughest Anti-Spam Law in Nation*, COMPUTER & INTERNET LAW, July 2003, at 34.

72. VA. CODE ANN. §§ 18.2-153.1B (Michie 2003).

73. *Id.* §§ 2.2-511, 18.2-152.1, 152.12. Virginia's statute has survived due process challenges at the district court level. *See* Verizon Online Servs. v. Ralsky, 203 F. Supp. 2d 601 (E.D. Va. 2002) (extending long-arm jurisdiction under VA. CODE ANN. § 8.01-328.1 to out-of-state defendants who sent unsolicited bulk e-mail to an ISP in Virginia, over a challenge that the statute violated the due process clause).

74. CA. BUS. & PROF. CODE §§ 17529.2-4 (West 2003).

75. Id. § 17529 (West Supp. 2003).

76. *Id.* §§ 17529.2-4 (West Supp. 2003). This provision has recently been pre-empted by the Can-Spam Act. *See* Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, Pub. L. No. 108-187, § 8(b), 117 Stat. 2699, 2716 (2003).

damages in the amount of $1000 per e-mail, up to $1,000,000 per incident.[77]

Because these statutes run the gamut in terms of conduct required and conduct prohibited, inconsistent standards abound.. Accordingly, some defendant spammers have asserted personal jurisdiction or due process defenses in states where they are not residents.[78] Several statutes have also been challenged under the dormant Commerce Clause, which prevents states from enacting legislation that affects residents across state borders.[79] Finally, underlying any action against an e-mail advertiser, whether brought in tort or under statute, is the extent of First Amendment protection available.[80]

Each of these constitutional issues will be discussed in turn, beginning with an analysis of the First Amendment as it applies to the Internet and to advertising in general.

III. CONSTITUTIONAL CONCERNS

A. The First Amendment

The First Amendment provides that: "Congress shall make no law . . . abridging the freedom of speech. . . ."[81] Courts have often been divided over the application of this Amendment to different types of speech.

In *Rowan*, the mailer's right to communicate was challenged only by an affirmative act of the addressee notifying the sender that he did not want further mailing from that sender.[82] Relying on the ancient notion that "'a man's home is his castle,'" the Court reasoned that "[n]othing in the Constitution compels us to listen to or view any unwanted communication, whatever its merit."[83] "[N]o one has a right to press even 'good' ideas on an unwilling recipient."[84]

However, the Internet is an entirely different medium for purposes of communication. A strict standard of review has been in place since *Reno v. ACLU*[85] when the Supreme Court declared that "[t]he Internet [g]ets [f]ull First Amendment [p]rotection."[86] The Court distinguished *Reno* from *FCC*

77. § 17529.8.

78. *See, e.g.*, Rannoch, Inc. v. Rannoch, Corp., 52 F. Supp. 2d 681 (E.D. Va. 1999); Verizon v. Ralsky, 203 F. Supp. 2d 601 (E.D. Va. 2002), discussed *infra* Part III.B.

79. *See, e.g.*, State v. Heckel, 24 P.3d 404 (Wash. 2001); Ferguson v. Friendfinders, Inc., 115 Cal Rptr. 2d 358 (2002), discussed *infra* Part III.C.2.

80. U.S. CONST. amend. I.

81. U.S. CONST. amend. I.

82. Rowan v. United States Post Office Dep't, 397 U.S. 728, 737 (1970).

83. *Id.*

84. *Id.* at 738.

85. 521 U.S. 844 (1997).

86. Timothy Wu, *Application-Centered Internet Analysis*, 85 VA. L. REV. 1163, 1170 (1999). In

v. Pacifica Foundation,[87] where it found that First Amendment interests could be curtailed for broadcast media when there was a privacy interest at stake, but only where capable of transmitting patently offensive material directly into people's homes.[88] In refusing to draw an analogy between the Internet and broadcast media, the *Reno* Court reasoned that warnings could be more effective on the Internet, whereas in broadcasting they could not protect viewers from undesired content.[89] In addition, there was only a remote possibility of encountering indecent material on the Internet by mistake, "Internet sites were not [as] scarce" as broadcast channels, "there was no extensive history of government regulation over the Internet," and the Internet did not share the invasive qualities of broadcast media.[90]

While *Reno* concerned the regulation of indecent material over the Internet, anti-spam policies and regulations fall under the broader category of commercial speech.[91] The extent of protection available for commercial speech has been transformed through recent cases. Thus, a review of the Commercial Speech Doctrine as it has evolved over the last half century is in order.

1. The Commercial Speech Doctrine

Commercial speech has historically been afforded much less protection than political and other noncommercial speech.[92] The reason for the distinction, as Justice Stevens articulated in *44 Liquormart, Inc. v. Rhode*

Reno, the Communications Decency Act of 1996 (CDA), which was an attempt to regulate the "knowing transmission of 'obscene or indecent' messages to any recipient under 18 years of age," came under constitutional attack. Reno v. ACLU, 521 U.S. 844 (1997). The Supreme Court agreed with the lower court decision that the CDA was constitutionally overbroad, thereby chilling the expression of adults. *Reno*, 521 U.S. at 862. The Court also found that terms used in the regulation, such as "patently offensive" and "indecent," were "inherently vague." *Id.*

A strict scrutiny standard requires the Government to "show that the challenged restriction on speech is narrowly tailored to promote a compelling government interest and that no less restrictive alternative would further that interest." Am. Library Ass'n v. United States, 201 F. Supp. 2d 401, 454 (2002) (citing United States v. Playboy Entm't Group, Inc., 529 U.S. 803, 813 (2000)). Under a rational basis review, on the other hand, "the challenged restriction need only be reasonable." *Id.*

87. 438 U.S. 726 (1977).

88. *See* Marcus, *supra* note 2, at 278.

89. *See Reno*, 521 U.S. at 870.

90. *See* Mark A. Lemley, *Place and Cyberspace*, 91 CAL. L. REV. 521, 531 (2003) (citing *Reno*, 521 U.S. 844, 867, 868-69 (1997)). Perhaps the *Reno* Court's partial reliance on the argument that the Internet is less invasive than television is somewhat obsolete, now that advertising on the Internet has become more accessible. As one author has remarked: "*Reno*'s assurance that 'The Internet Gets Full First Amendment Protection' can look pretty thin when there are 49,000 new messages in your inbox, or when your so-called cyberlife consists of deleting ads for pyramid schemes and porn sites." Wu, *supra* note 86, at 1173.

91. "Commercial" speech is "expression related solely to the economic interests of the speaker and its audience." Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of N.Y., 447 U.S. 557, 561 (1980).

92. *See, e.g.*, Ohralik v. Ohio State Bar Ass'n, 436 U.S. 447, 456 (1978) ("Rather than subject the First Amendment to such . . . devitalization, we instead have afforded commercial speech a limited measure of protection, commensurate with its subordinate position in the scale of First Amendment values, while allowing modes of regulation that might be impermissible in the realm of noncommercial expression.").

Island, is "to protect consumers from misleading, deceptive, or aggressive sales practices."[93] However, numerous cases demonstrate that courts will allow the First Amendment to trump statutes or regulations that inhibit commercial speech without substantial justification.[94]

Central Hudson Gas & Electric Corp. v. Public Service Commission of NY was the first significant case to set down the standard of review for statutes that attempt to regulate commercial speech.[95] The Supreme Court in *Central Hudson* reasoned that, although the Constitution affords commercial speech less protection than other types of speech, "[c]ommercial expression not only serves the economic interest of the speaker, but also assists consumers and furthers the societal interest in the fullest possible dissemination of information."[96]

Central Hudson announced a four-part test to determine whether the commercial speech at issue was constitutionally protected.[97] First, the expression "must concern lawful activity and not be misleading."[98] The second question is whether or not the government's interest in regulating is substantial.[99] If both of these inquiries yield positive answers, the court "must determine whether the regulation directly advances the governmental interest asserted, and [finally,] whether it is not more extensive than necessary to serve that interest."[100] The latter two prongs of the test have been tweaked by subsequent cases.[101]

Modifying the third prong of the *Central Hudson* test, for example, the Court in *Edenfield v. Fane* established that "a government body seeking to uphold the constitutionality of a restriction of commercial speech 'must demonstrate that the harms it recites are real and that its restriction will in fact alleviate them to a material degree.'"[102] However, in *United States v.*

---

93. 44 Liquormart, Inc. v. Rhode Island, 517 U.S. 484, 501 (1996).

94. *See, e.g.*, Cincinnati v. Discovery Network, Inc., 507 U.S. 410, 440 (1993) (Rehnquist, C.J., dissenting); United States v. Edge Broad. Co., 509 U.S. 418, 434 (1993); Edenfield v. Fane, 507 U.S. 761, 762 (1993); Bd. of Trs. v. Fox, 492 U.S. 469, 478 (1989); *Central Hudson*, 447 U.S. at 557.

95. *Central Hudson*, 447 U.S. at 557. In that case, the New York Public Service Commission had promulgated a regulation that banned promotional advertising by electric utility companies operating in the state. *Id.* at 558. Appellant argued that the ban was a violation of its First Amendment rights. *Id.* at 560.

96. *Id.* at 561-62.

97. *Id.* at 566.

98. *Id.*

99. *Id.*

100. *Id.* In essence, the court in *Central Hudson* modified the "strict scrutiny" standard of review, by which the Supreme Court has traditionally applied a two part test to fundamental rights to determine if: 1) there is a compelling state interest for the state to regulate, and 2) the means are narrowly tailored to further that interest. *See* Grutter v. Bollinger, 539 U.S. 306, 326 (2003) (laying out the strict scrutiny test).

101. For a full discussion of the development of the Commercial Speech Doctrine, see generally Marcus, *supra* note 2.

102. *Id.* at 274 (citing Edenfield v. Fane, 507 U.S. 761, 762 (1993)).

Edge Broad. Co., the Court allowed more flexibility to the Government in proving its harms, stating that the Government need not "make progress on every front before it can make progress on any front."[103] In that case, the Court found that a federal statute barring radio broadcasts of state lotteries by radio licensees in non-lottery states did not violate the Constitution since it furthered the state interest in avoiding exposure by citizens in the non-lottery state to lottery advertising.[104] The government needed only show that the regulation reduced the advertising, which would correspond to a decrease in demand for gambling.[105]

The Supreme Court refined the application of the fourth prong of the *Central Hudson* test in *Board of Trustees v. Fox*,[106] when it held that regulations that inhibit commercial speech will pass the test only if they are "'narrowly tailored' to serve a significant governmental interest."[107] That fit did not necessitate the "best" fit, but merely one that was in proportion to the interests served.[108]

2. An Exception for Private Actors

Private actors do not have a duty to protect speech to the same extent as state actors.[109] Therefore, in common law actions by ISPs and individuals against spammers, the First Amendment has not been a successful defense.[110] In *CompuServe*, for example, defendants relied on the First Amendment to argue that they had a right to continue sending spam to plaintiff's computer systems.[111] However, CompuServe is a private actor rather than the government or a public utility.[112] The court in *CompuServe* admitted that if a private actor has some amount of control over a central avenue of communication, it may be treated like a public utility, and held to the same First Amendment standard.[113] Nevertheless, the First Amendment

103. United States v. Edge Broad. Co., 509 U.S. 418, 434 (1993).

104. *Id.* at 434.

105. *Id.*

106. 492 U.S. 469 (1989).

107. *Id.* at 478. In this case, a university had promulgated regulations concerning the use of school property for commercial purposes. *Id.* at 471-72. Students who had been arrested for violating the regulation sought a declaratory judgment against the university under the overbreadth doctrine (which allows suits by plaintiffs where First Amendment rights have been violated). *Id.* The Supreme Court reversed and remanded the lower court's decision, since it had not determined the validity of the university's resolution in the context of commercial and non-commercial speech. *Id.* at 486.

108. *Id.* at 478. This standard was interpreted to require not the elimination of all less restrictive means available, but only that the regulation not burden "substantially more speech than is necessary to further the government's legitimate interests." *Id.* (quoting Ward v. Rock Against Racism, 491 U.S. 781, 799 (1989)).

109. *See* Hudgens v. NLRB, 424 U.S. 507, 513 (1976) ("[T]he constitutional guarantee of free speech is a guarantee only against abridgement by government, federal or state.") (citing Columbia Broad. Sys., Inc. v. Democratic Nat'l Comm., 412 U.S. 94 (1973)).

110. *See supra* Part II.A.

111. CompuServe v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1025 (1997).

112. *Id.*

113. *Id.*

did not trump a private actors' right to bring a common law action for trespass where there were adequate alternative avenues of communication for the defendants.[114]

Thus, although the Commercial Speech Doctrine plays a large role in determining the application of anti-spam legislation to public utilities and state actors, it has not been a successful defense against private actors.

B. Personal Jurisdiction and Due Process

Another major issue to overcome in an action against spammers is one of jurisdiction. "[A]nonymity and decentralization of the Internet means that individual jurisdictions may not have the resources to locate and prosecute even the most egregious spammers."[115] However, even when they are able to locate those individuals, state courts face the problem of bringing them within the state's long-arm statute, and finding intent on the part of the defendant to reach consumers and businesses within that state.

For example, in *Rannoch, Inc. v. Rannoch Corp.*,[116] the issue was whether the defendant, a Texas corporation, had performed a sufficient number of Internet activities to bring it within the jurisdiction of the plaintiff's home state, Virginia.[117] In that case, the plaintiff sued Rannoch Corp. for trademark infringement under the Lanham Act due to the use of its name in commerce.[118] The plaintiff asserted that jurisdiction was established by the ability of Virginia residents to access the defendant's domain name.[119] The district court of Virginia followed a two step process to determine jurisdiction:

> First, courts must ascertain whether a plaintiff has made a *prima facie* showing that Virginia's long-arm statute reaches the non-resident defendant given the cause of action alleged and the nature

---

114. *Id.* at 1026; *see also,* Cyber Promotions, Inc. v. American Online, Inc., 948 F. Supp. 436 (E.D. Pa. 1996):

> By providing its members with access to the Internet through its e-mail system so that its members can exchange information with those members of the public who are also connected to the Internet, AOL is not exercising *any* of the municipal powers or public services traditionally exercised by the State. . . .

Id. at 442. The defendant in that case likewise was not subject to First Amendment protection in sending unsolicited advertisements via AOL's e-mail network where alternative means of communication still existed. *Id.* at 442-43.

115. Bruce E.H. Johnson, *Is There a Constitutional Right to Bombard the Public with Penis Enlargement Proposals?*, COMM. LAW., Summer 2003, at 3, 5.

116. 52 F. Supp. 2d 681 (1999).

117. *Id.* at 682.

118. *Id.* Here, the plaintiff was a Virginia corporation that sold computer and engineering services in the field of aviation. *Id.* The Defendant of the same name was a one-person business, operating out of Texas and providing activities for individuals who enjoyed steam railroading. *Id.*

119. *Id.* at 683.

> of the defendant's Virginia contacts. Second, a court must determine whether the exercise of personal jurisdiction in the circumstances is consistent with the Due Process Clause, that is, whether the long-arm statute's reach in the circumstances exceeds its constitutional grasp.[120]

The court reached the conclusion that although the defendant's activities may be sufficient to support jurisdiction under Virginia's long-arm statute, it was not enough to satisfy the due process analysis.[121] It reasoned that the mere placement of a website on the Internet with knowledge that a Virginia resident *might* access it was not sufficient to show purposeful availment of the laws of Virginia, any more than the laws of another state.[122]

The Eastern District of Virginia again reviewed the issue of personal jurisdiction in *Verizon Online Services, Inc. v. Ralsky*.[123] In *Verizon*, the plaintiffs sued for trespass to chattels after the defendants sent millions of unsolicited bulk e-mails to the plaintiff's online subscribers.[124] The court applied *Rannoch*'s two-step process, but reached the opposite conclusion.[125] *Purposefully* sending e-mails to recipients with accounts through a Virginia ISP, thereby causing a tort in Virginia, was purposeful availment of the laws of Virginia, and thus subject to the state's long-arm statute.[126] The court explained that "[b]y allegedly transmitting millions of e-mails to make money at Verizon's expense, knowing or reasonably knowing that such conduct would harm Verizon's e-mail servers, Defendants should have expected to get dragged into court [in the state] where their actions caused the greatest injury."[127]

These cases indicate that personal jurisdiction will continue to be an issue for actions against spammers at the state level. If spammers have not intentionally availed themselves of the laws of another state by knowingly sending their messages across borders, it will not be easy for a recipient resident of that state to sue them.

---

120. *Id.*

121. *Id.* at 687. "[T]he Due Process Clause requires that no defendant shall be haled into court unless defendant has 'certain minimum contacts [with the state] . . . such that the maintenance of the suit does not offend traditional notions of fair play and substantial justice.'" *Id.* at 685 (quoting Intern'l Shoe Co. v. Washington, 326 U.S. 310 (1945)). Jurisdiction is only appropriate where the defendant has purposely directed his activities toward residents of the state in question and the litigation arises out of those activities. *Id.*; *see also* Media3 Tech., LLC v. Mail Abuse Prevention Sys., LLC, 2001 U.S. Dist. LEXIS 1310 (D.C. Mass. 2001). This court listed several additional factors for finding that the exercise of jurisdiction is reasonable:

> (1) the burden imposed on the defendant by requiring an appearance in the state; (2) the forum state's interest in adjudicating the dispute; (3) the plaintiff's interest in obtaining convenient and effective relief; (4) the judiciary's interest in obtaining the most efficient resolution of the controversy; and (5) public policy concerns.

Id. at *18-19 (citing Burger King Corp. v. Rudzewicz, 471 U.S. 462, 477 (1985)).

122. *Rannoch*, 52 F. Supp. 2d at 685-86.

123. 203 F. Supp. 2d 601 (E.D. Va. 2002).

124. *Id.* at 604.

125. *Id.* at 617-18.

126. *Id.*

127. *Id.* at 618-19.

C. The Dormant Commerce Clause

The most common avenue of attack against UCE statutes is via the "dormant" Commerce Clause of the Constitution,[128] the name given to the negative implication of the Commerce Clause.[129] The Commerce Clause grants Congress the power "[t]o regulate Commerce with foreign Nations, and among the several States."[130] The *dormant* Commerce Clause doctrine is "the principle that the states impermissibly intrude on this federal power when they enact laws that unduly burden interstate commerce."[131]

The Supreme Court has articulated a variety of tests to distinguish between the types of state regulations the Commerce Clause permits, and those it prohibits.[132] The tests include:

> (1) whether a state statute explicitly favors in-state over out-of-state economic interests (the "protectionist test");[133]
>
> (2) whether a statute's practical effect is "to control conduct beyond the boundaries of the state" (the "extraterritorial effect test");[134]
>
> (3) whether a sufficiently negative "effect would arise if not one, but many or every, state adopted similar[, but inconsistent,] legislation" (the "inconsistent regulation test");[135] and
>
> (4) whether the benefit the state receives from the statute is clearly outweighed by the burden that it imposes on interstate commerce (the "undue burden test").[136]

The "protectionist" test usually will not apply to UCE statutes since they do not openly discriminate against out-of-state interests, treating all spammers alike.[137] But the "extraterritorial effects" test applies where the statutes "regulate activities that occur wholly outside the state that has enacted such a statute."[138] Almost every UCE statute fails that test.[139] For

128. Booher & Morris, *supra* note 9, at 355.
129. *Id.* at 356.
130. U.S. CONST. art. I, § 8, cl. 3.
131. State v. Heckel, 24 P.3d 404, 409 (Wash. 2001).
132. Booher & Morris, *supra* note 9, at 356.
133. *Id.* (citing Brown-Forman Distillers Corp. v. N.Y. State Liquor Auth., 476 U.S. 573, 579 (1986)).
134. *Id.* (citing Healy v. Beer Inst., 419 U.S. 324, 336-37 (1989)).
135. *Id.* (citing *Healy*, 419 U.S. at 336-37) (alteration in original).
136. *Id.* (citing Pike v. Bruce Church, 397 U.S. 137, 142 (1970)).
137. *Id.*
138. *Id.*

example, some statutes extend jurisdiction to non-residents within the limits of the state's long-arm statute, some apply to any e-mail sent through an in-state network, some apply where the sender has reason to know that it will reach the state's residents, and some have various other limitations that could affect out-of state citizens.[140] As a result, it is virtually impossible for senders to know which statutes govern their conduct, and the "states with the most restrictive UCE statutes effectively regulate the conduct of all senders. . . ."[141]

UCE statutes may also fail the "inconsistent regulation" test since the labeling requirements vary from state to state.[142] Some statutes require "ADV:" in the subject line for general advertisements, while others require "ADV: ADVERTISING."[143] Some require "ADV: ADLT" for sexually explicit material, while others require "ADV-ADULT."[144]

Finally, the statutes could foreseeably fail the "undue burden" test where senders do not know which statute will apply to their commercial e-mail, resulting in higher costs to comply with all such provisions and lost opportunities to consumers.[145]

1. Application to Internet Regulation

Both federal and state cases have applied the dormant Commerce Clause analysis in Internet regulation cases. In *American Libraries Ass'n v. Pataki*,[146] plaintiffs challenged a statute that attempted to regulate the Internet transmission of material that was harmful to minors.[147] The New York district court applied the extraterritorial effects test to find that website owners and senders had no way of ensuring that New York residents were unable to access their sites.[148] It was thus impossible to limit the statute to activities within the state of New York.[149] The statute also failed the undue burden test because the costs associated with complying with the statute were excessive in relation to the benefit conferred on the state.[150] Finally, in

---

139. *Id.*
140. *Id.*; *see also* Sorkin, *supra* note 7.
141. Booher & Morris, *supra* note 9, at 357.
142. *Id.*; *see also* Sorkin, *supra* note 7.
143. *See generally* Sorkin, *supra* note 7.
144. *See id.*
145. Booher & Morris, *supra* note 9, at 357-58.
146. 969 F. Supp. 160 (S.D.N.Y. 1997).
147. *Id.* at 163-64. The statute at issue was N.Y. Penal Law § 235.21(3) (McKinney 2004). *Id.*
148. *Id.* at 177.
149. *Id.*

> The nature of the Internet makes it impossible to restrict the effects of the New York Act to conduct occurring within New York. An Internet user may not intend that a message be accessible to New Yorkers, but lacks the ability to prevent New Yorkers from visiting a particular Website or viewing a particular newsgroup posting or receiving a particular mail exploder.

Id.

150. *Id.* The court reasoned that although the protection of children from harmful sexual material was a "quintessentially legitimate state objective," the state could not avoid the second part of the

applying the "inconsistent regulation" test, the court expressed the view that the Internet demanded consistent treatment through national regulation, or it would be paralyzed altogether.[151] Thus, the district court struck the statute as unconstitutional.[152]

2. Application to Anti-Spam Legislation

Courts have applied a slightly different Commerce Clause analysis in UCE statute cases. In *State v. Heckel*,[153] the Supreme Court of Washington overturned a lower court decision that the state's UCE statute was "'unduly restrictive and burdensome'" on interstate commerce.[154] Rather than applying each of the four tests above, the court applied a two-part analysis to determine 1) "whether the state law openly discriminates against interstate commerce in favor of intrastate economic interests"[155] and, if not, 2) whether the interstate burden is balanced with the local benefits.[156]

The statute at issue in *Heckel* was in the first category of statutes that prohibit conduct,[157] applying to senders who knew or had reason to know they were sending fraudulent e-mails to Washington residents.[158] The

---

test, which required it to assess the impact on interstate commerce. *Id.* at 177-78. Imposing such a burden on senders whose only contact with the state was via the Internet would be analogous to "New York bounty hunters dragging pedophiles from the other 49 states into New York." *Id.* at 178. Furthermore, the chilling effect on the worldwide net would likely exceed the number of cases prosecuted in New York. *Id.* at 179.

151. *Id.* at 181.

> The Internet, like the rail and highway traffic at issue in the cited cases, requires a cohesive national scheme of regulation so that users are reasonably able to determine their obligations. Regulation on a local Level, by contrast, will leave users lost in a welter of inconsistent laws, imposed by different states with different priorities.

Id. at 182; *see also* Am. Civil Liberties Union v. Johnson, 194 F.3d 1149 (10th Cir. 1999) (striking down on similar grounds a New Mexico statute (N.M. Stat. Ann. § 30-37-3.2) that prohibited the electronic dissemination of harmful materials to minors). "Even if it is limited to one-on-one e-mail communications . . . there is no guarantee that a message from one New Mexican to another New Mexican will not travel through other states en route." *Id.* at 1161.

152. *Am. Libraries Ass'n*, 969 F. Supp. at 183-84.

153. 24 P.3d 404 (Wash. 2001).

154. *Id.* at 406.

155. *Id.* at 408 (Wash. 2001).

156. *Id.* at 409. This test is based on the view that the "extraterritorial effects," "inconsistent regulations" and "undue burden" tests are rolled into one. *See* Booher & Morris, *supra* note 9, at 359; *see also* Goldsmith & Sykes, *supra* note 60, at 804 ("[The] extraterritoriality analysis under the dormant Commerce Clause must be more fine-grained. It must, that is, distinguish between permissible and impermissible out-of-state costs that result from the regulation of cross-border externalities."). Likewise, the "inconsistent regulations" test simply enhances the "undue burden" test by highlighting a potential risk of allowing states to create different regulatory regimes in relation to the benefits conferred on the state. *See* Booher & Morris, *supra* note 9, at 359; *see also* Goldsmith & Sykes, *supra* note 60, at 807 ("[T]he proliferation of different state regulations may impose compliance costs that outweigh any plausible regulatory benefits. Viewed this way, the inconsistent-regulations cases, too, are a variant of balancing analysis.").

157. *See supra* Part II.B.

158. *See* WASH. REV. CODE § 19.190.

Washington court upheld the regulation since it narrowly prohibited the use of any misleading information in commercial e-mails.[159] The benefit of limiting potential harm to Washington businesses outweighed any conceivable burden to the e-mail senders.[160]

UCE statutes in the second category that require conduct[161] have likewise been challenged under the dormant Commerce Clause.[162] In *Ferguson v. Friendfinders, Inc.*, the California Court of Appeals rejected the *American Libraries* notion that *any* regulation of the Internet was a violation of the dormant Commerce Clause.[163] Although the statute at issue broadly encompassed "conduct by persons or entities doing business in California who transmit unsolicited advertising materials,"[164] the court applied a balancing test like that in *Heckel* to determine that

> California has a substantial legitimate interest in protecting its citizens from the harmful effects of deceptive UCE and . . . section 17538.4 furthers that important interest. By requiring disclosure of the advertising and/or adult nature of an unsolicited e-mail in the subject line, section 17538.4 establishes a quick and simple way of identifying UCE without having to read it first.[165]

The statute's benefits outweighed the burden on interstate commerce, by facilitating the elimination of fraud and deception.[166] The additional requirements, such as "ADV:" in the subject line, caused a negligible burden in light of the state's interests.[167] Thus, the dormant Commerce Clause again

---

159. *Heckel*, 24 P.3d at 413.

160. *Id.*

161. *See supra* Part II.B.

162. *See* Ferguson v. Friendfinders, Inc., 115 Cal. Rptr. 2d 258 (Ct. App. 2002).

163. *Id.* at 260.

164. *Id.* The former California statute required:

> that a "person or entity conducting business in this state" who causes an unsolicited e-mail document to be sent (1) establish a toll-free telephone number or valid sender operated return e-mail address that recipients may use to notify the sender not to e-mail further unsolicited documents; (2) include as the first text in the e-mailed document a statement informing the recipient of the toll-free number or return address that may be used to notify the sender not to e-mail any further unsolicited material; (3) not send any further unsolicited advertising material to anyone who has requested that such material not be sent; and (4) include in the subject line of each e-mail message "ADV:" as the first four characters or "ADV:ADLT" if the advertisement pertains to adult material.

Id. (citation omitted).

165. *Ferguson*, 115 Cal. Rptr. 2d at 268.

166. *Id.*. The court relied on *Heckel* to find that truthfulness requirements only deterred spammers from sending fraudulent e-mail, and thus directly reduced the volume of spam. *Id.* (citing State v. Heckel, 24 P.3d 404, 411 (Wash. 2001)).

167. *Id.* ("[T]he cost of placing particular letters in the subject line of the e-mail and including a valid return address in the message itself 'is appreciably zero in terms of time and expense.'" (quoting California's Attorney General)). Others argue that California actually misapplied the undue burden test, since the fact that the California statute did not prohibit falsification, but only required "ADV:" in the subject line made it harder to justify the limited benefits that such a statute would provide. Booher & Morris, *supra* note 9, at 364.

However, this California anti-spam statute was still in effect when a judgment of two million dollars was entered against a bulk e-mailer under section 17538 in 2004. *See* Liane Jackson,

proved unsuccessful as a challenge to a UCE statute..

Nevertheless, possibly out of fear that challenges to state statutes *would* succeed, overloading the courts and creating inconsistent standards with respect to Internet regulation, the federal government pushed legislation that would apply to spammers on a national level.[168] This federal legislation will at least eliminate the issues associated with the dormant Commerce Clause and Personal Jurisdiction. However, Commercial Speech protection may still be relevant and will be discussed below.

IV. THE CAN-SPAM ACT OF 2003

A. The Law

After numerous revisions and various nicknames, the Can-Spam Act (the "Act") was introduced into Congress in January 2003 as "An Act To regulate interstate commerce by imposing limitations and penalties on the transmission of unsolicited commercial electronic mail via the Internet."[169] After being signed into law by the President in December 2003, it took effect in January 2004.[170]

The Act was based on findings that the convenience or efficiency of electronic mail was being compromised by the unprecedented growth of unsolicited commercial e-mail.[171] Bulk e-mails had resulted in costs not only to recipients who could neither control the rate nor the amount received, but also to Internet service providers and businesses with infrastructures that could not handle the volume.[172] Furthermore, a growing number of e-mails consisted of pornographic, false or misleading

---

California Reins In Spammers; State of California v. Willis, CORP. LEGAL TIMES, Jan. 2004, at 50 ("Santa Clara County prosecutors are hoping a $2 million judgment against a spammer will serve as a deterrent to others sending junk mail over the Internet. The hefty penalty is the largest to date against senders of unsolicited e-mail, and it's the first such lawsuit in California."). The bigger problem is how to collect the judgment, since the defendants did not even show up in court. *Id.*; *see also* Complaint for Injunction, Civil Penalties and Other Equitable Relief, State v. Willis, (Super. Ct. Cal. 2002) (No. CV811428).

168. Some commentators fear that the Act was actually rushed into law to pre-empt California's more stringent opt-in provision. *Just A Start; Anti-Spam Law Is a Good Start, but it Needs to be Strengthened*, BUFFALO NEWS, Dec. 20, 2003, at B4 [hereinafter "Just A Start"].

169. Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, Pub. L. No. 108-187, 117 Stat. 2699 (2003) (codified at 15 U.S.C. § 7701). For an analysis of the proposed Can-Spam Act when it was introduced in 1999, see Vasilios Toliopoulos, *Legislative Updates: Regulating Your Internet Diet: The Can-Spam Act of 1999*, 10 DEPAUL-LCA J. ART & ENT. L. & POL'Y 175 (1999). For an in-depth discussion of various other anti-spam proposals, see also, Derek D. Simmons, Comment, *No Seconds On Spam: A Legislative Prescription to Harness Unsolicited Commercial E-mail*, 3 J. SMALL & EMERGING BUS. L. 389 (1999).

170. Controlling the Assault of Non-Solicited Pornography and Marketing Act § 16.

171. *Id.* § 2(a)(2).

172. *Id.* § 2(a)(4),(6).

information in the subject lines, some disguising the source, and many failing to provide recipients with an opt-out mechanism.[173] On the basis of these findings, Congress determined that the government had a substantial interest in nationwide regulation of false and misleading commercial e-mail.[174]

The Act applies to senders who:

1) use a protected computer without authorization,[175]

2) intend to deceive recipients as to the message origin by using another server,[176]

3) materially falsify the header information,[177]

4) register five or more accounts with a materially false identity,[178] or

5) falsely represent oneself to be the owner of a registered address.[179]

The Act also provides for criminal penalties for repeat and serious offenders.[180]

---

173. *Id.* § 2(a)(5), (7)-(9).

174. *Id.* § 2(b).

175. 18 U.S.C.§ 1037(a)(1). This provision is specifically directed toward some common techniques that spammers use to obtain e-mail addresses, such as "harvesting" and hacking into another person's computer system to send UCE from that system. *See* Controlling the Assault of Non-Solicited Pornography and Marketing Act § 4(b)(2)(A)(i). "Harvesting" is a technique through which spammers can generate a number of e-mail addresses by using a software program that compiles lists from websites, user groups, and chat rooms. *See Email Address Harvesting: How Spammers Reap What You Sow*, FTC Consumer Alert, *available at* http:// www.ftc.gov/bcp/conline/pubs/alerts/spamalrt.htm (last visited Mar. 28, 2005). Spammers can also hack into other systems by inserting a "Trojan Horse" program, a program that takes control of unsuspecting downloader's computers. *See* S. REP. NO. 108-170 (2003).

176. 18 U.S.C. § 1037(a)(2). This provision criminalizes the spammer technique of using third parties' open servers to re-transmit e-mail without the server owner's knowledge. *See* S. REP. NO. 108-170.

177. 18 U.S.C. § 1037(a)(3). The Act defines "materially falsified" as information that "is altered or concealed in a manner that would impair the ability of a recipient of the message . . . to identify, locate, or respond to a person who initiated the electronic mail message . . ." *Id.* § 1037(d)(2). The purpose of this provision is to allow users to be able to identify trusted senders and use "white lists" to receive e-mail only from those senders. *See* S. REP. NO. 108-170.

178. 18 U.S.C. § 1037(a)(4). This provision targets a spammer technique called "account churning," by which a spammer can register for multiple accounts using false information and send bulk spam from one after the other. *See* S. REP. NO. 108-170.

179. 18 U.S.C. § 1037(a)(5). This provision attacks the hacker spamming technique of hijacking large blocks of unused Internet addresses and using them to send spam. *See* S. REP. NO. 108-170.

180. 18 U.S.C. § 1037(b). Enhanced penalties are provided against those convicted of various other fraud and sexual exploitation offenses if they involve sending mass amounts of mail. Can-Spam Act, *supra* note 12, at § 4(b)(2)(B).

The Act requires a valid return e-mail address or other mechanism by which the recipient can opt-out of future e-mail.[181] Each message must contain clear identification as an advertisement, notice of the recipient's opportunity to opt-out, and a valid physical postal address of the sender.[182] After a recipient requests to opt-out, the sender or any of its agents must cease all unsolicited e-mail to the recipient within ten business days.[183]

With regard to civil remedies, the Act allows each state's attorney general to bring an action in the local district court to enjoin a defendant from further violations, or to obtain damages in the amount of loss suffered by the state's resident recipient.[184] Statutory damages are available, up to $250 per e-mail violation, with a two-million-dollar maximum.[185] Damages are also available to Internet service providers (ISPs) who are adversely affected by the spammer's violations.[186] Although the Can-Spam Act pre-empts state statutes that require conduct,[187] it does not eliminate those that prohibit conduct, such as the falsification of information in the body of the e-mail.[188] It also allows ISPs to continue implementing anti-spam policies.[189]

The Act contains several provisions for future implementation and consideration. It calls for the FTC to consider a "Do-Not-E-Mail" registry, similar to the FTC's recently implemented "Do-Not-Call" registry.[190] Finally, Congress asks for international cooperation as studies on the effectiveness of cross-border enforcement against spammers continue.[191]

---

181. Controlling the Assault of Non-Solicited Pornography and Marketing Act § 5(a)(3)(A).

182. *Id.* § 5(a)(5)(A). This does not apply if the recipient has given prior affirmative consent, of course. *Id.* § 5(a)(5)(B). A separate prohibition is included for the transmission of any unsolicited "sexually oriented material" via commercial e-mail without clear labeling as prescribed by the Federal Trade Commission (FTC). *See id.* § 5(d). The FTC has 120 days after the enactment of the Act to prescribe the marks to be used for such sexually oriented material. *Id.* § 5(d)(3). Criminal penalties are prescribed against those in violation of this provision as well. *Id.* § 5(d)(5).

183. *Id.* § 5(a)(4)(A)(i). It is also illegal for the sender to sell or lease the recipient's e-mail address to another party after such request. *Id.* § 5(a)(4)(A)(iv).

184. *Id.* § 7(f)(1), (3). Injunctive relief is also available without a showing of knowledge on the part of the defendant. *Id.* at § 7(f)(2).

185. *Id.* § 7(f)(3)(A)-(B).

186. *Id.* § 7(g). These could include an injunction, actual losses, or statutory damages in the amount of one hundred dollars per 5(a)(1) e-mail violation (prohibition against false or misleading information) or twenty-five dollars per any other violation, up to one million dollars. *Id.* § 7(g)(1), (3).

187. Such statutes include those that require specific subject header labeling and opt-in or opt-out mechanisms. *See* Sorkin, *supra* note 7; *see also infra* § II.B.

188. Controlling the Assault of Non-Solicited Pornography and Marketing Act § 8(b)(1). The Act also does not extend to actions brought under state trespass, contract, or tort law, or laws that relate to fraud or computer crime. *Id.* § 8(b)(2).

189. *Id.* § 8(c).

190. *Id.* § 9.

191. *Id.* § 10(b)2.

B. Criticism and Commentary

There are a variety of different opinions on the immediate effect of the new federal legislation. Some commend Congress' effort to institute a national standard for spam regulation, while others emphasize the number of issues that the Act does not eliminate.

BigFootInteractive, a provider of strategic electronic marketing solutions, praised the positive effects of the law, such as pre-emption of state laws, identification of fraudulent uses of e-mail, and prohibition of "harvesting."[192] The Coalition Against Unsolicited Commercial E-Mail (CAUCE), a leading anti-spam activist group, has noted, however, that the law gives limited enforcement capabilities to "overworked regulatory and law enforcement agencies, rather than giving consumers legal tools with which to protect their own inboxes."[193] CAUCE has also remarked that the Act "gives each marketer in the United States one free shot at each consumer's e-mail inbox," forcing companies to use costly anti-spam technologies and company resources to block the messages."[194]

European anti-spam activists have called the Act a "serious mistake" since it only regulates rather than prohibits spam.[195] By actually making spam legal in the United States, the Act is essentially inviting an onslaught of unsolicited messages from Asia, and areas with even less prohibitions.[196]

Frustration has also been expressed at the fact that some states' tougher anti-spam measures will be circumvented by a less impactful federal law.[197] By pre-empting statutes that require conduct, such as the prior explicit consent of a user (opt-in), the Act essential back tracks any progress states have made in the way of eliminating spam. CAUCE remarked that California's opt-in law, which was set to go into effect in January 2004, was

---

192. BigFootInteractive, *Commentary on the Can-Spam Act of 2003 (S.877), available at*: http://www.bigfootinteractive.com/canspam/CAN-SPAM_Commentary.pdf (last visited Mar. 14, 2005). This group has also put out some suggestions for improving upon the Act. *Id.*

193. *See CAUCE Statement on Can-Spam Act* [hereinafter CAUCE Statement], *available at* http://www.cauce.org/news/2003.shtml (Dec. 16, 2003). CAUCE opines, from the standpoint that unsolicited commercial e-mail should be outlawed altogether, that the law was passed with scarcely any input from the marketing industry and ISP lobbies, or "the interests of America's consumers and business Internet users." *Id.*

194. CAUCE Statement, *supra* note 193. This is a reaction to the opt-out scheme provided for in the Act, which allows a first time e-mail transmission to a recipient, as long as the latter is given a means to reject future unsolicited commercial e-mails. *See also* Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, Pub. L. No. 108-187, § 5(a)(3)(A), 117 Stat. 2699, 2707 (2003). CAUCE Chairman Scott Hazen Mueller worries that:

> [i]t only makes that spam slightly more truthful. It also gives a federal stamp of approval for every legitimate marketer in the U.S. to start using unsolicited e-mail as a marketing tool. Congress has listened to the marketers and not to consumers, and we have no faith that this law will significantly reduce the amount of spam that American Internet users receive.

CAUCE Statement, *supra* note 193.

195. *See Spamhaus Position on CAN-SPAM Act of 2003* (S.877/HR 2214), *available at* http://www.spamhaus.org/position/CAN-SPAM_Act_2003.html (Dec. 20, 2003).

196. *See id.*

197. *Just A Start*, *supra* note 168.

passed *because* the opt-out law was found to be a failure.[198] In support of pre-emption, however, Can-Spam advocates point to the issues inherent in state regulation of a borderless problem.[199]

While consumers and business owners seem generally concerned over the effectiveness of the new law, there are also constitutional concerns that prevent Congress from acting more broadly.[200] These concerns are of more direct relevance to the analysis in this Comment.

C. First Amendment Analysis

In assessing the constitutionality of the Act, courts will likely return to the Commercial Speech doctrine as articulated in *Central Hudson*, and clarified in subsequent cases.[201] Senator Hatch has remarked that the Act[202] does not raise constitutional concerns because "rather than targeting speech, the bill instead targets e-mailing techniques used to steal computer services and trespass on private computers and computer networks."[203] Furthermore, it "addresses only commercial e-mail messages . . . and only when such messages are misleading by virtue of falsifying their point of origin."[204] Thus, the first prong of *Central Hudson* would not be satisfied.[205]

Despite this assurance that the Act is constitutionally sound, the Federal Trade Commission may follow through with some of the Act's suggestions, such as subject header requirements, a "Do-Not-E-mail" registry, and cooperation with international fora.[206] In those contexts, it may be necessary to consider some potential constitutional arguments.

1. Labeling Requirements

There is a likely First Amendment challenge against labeling requirements imposed by the government,[207] based on limitations to compulsory speech recognized in various precedent cases.[208] The argument

198. CAUCE Statement, *supra* note 193.

199. *See* BigFootInteractive, *supra* note 191.

200. *See* S. REP. NO. 108-170 (2003).

201. *See supra* Part III.A.1.

202. *See* S. REP. NO. 108-170, at 4. His comments were specifically related to the Criminal Spam Act, an amendment to the Can-Spam Act. *Id.*

203. *Id.*

204. *Id.*

205. Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n, 447 U.S. 557, 566 (1980) (holding that in commercial speech cases, a court must first determine that the expression concerns lawful activity and is not misleading).

206. *See* Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, Pub. L. No. 108-187, §§ 10(b)(2), 11(2), 117 Stat. 2699, 2717 (2003).

207. *Id.* § 11(2); *see also id.* § 5(d) (requiring explicit labeling of any sexual material that may be harmful to minors).

208. *See* Johnson, *supra* note 115, at 8 (citing Bd. of Educ. v. Barnette, 319 U.S. 624 (1943) and

would likely turn not on the actual content of the speech required, like "ADV" in the e-mail subject line, but rather on the effect of the labeling.[209] The label would allow users to more easily filter all spam, effectively shutting down solicitation by e-mail.[210] However, the distinction from precedent cases upholding this argument is that, although the government may impose the label, it is the user who is ultimately making the decision to filter out e-mail, after the sender has had an opportunity to reach him or her.[211] Thus, the burden placed on the sender by the labeling requirement is minimal, and courts would likely find a reasonable fit between the government's purpose in preventing the transmission of false information and the means imposed by the Act.[212]

Currently, the Act merely requires honest subject lines, so that consumers will not be tricked into opening misleading messages.[213] Thus, constitutional arguments against compulsory speech will likely be unsucessful.

2. The "Do-Not-E-Mail" Registry

The Can-Spam Act also calls for the FTC to consider the implementation of a "Do-Not-E-mail" registry, much like the "Do-Not-Call" registry provided for in the Telephone Consumer Protection Act (TCPA).[214] "[Eighty-three percent] of Americans are either extremely or very likely to register for the [do-not-e-mail] list making it more popular than the telemarketing 'do-not-call list.'"[215] At the same time, the Direct Marketing Association (DMA) has expressed some concern that a "Do-Not-E-Mail" registry would do nothing but forestall the ability of legitimate e-mail marketers to reach consumers.[216]

If the list is ultimately implemented despite these concerns, it would be helpful to review the TCPA and recent commercial speech challenges to that Act, in order to predict potential constitutional problems.

Pac. Gas & Elec. Co. v. Pub. Util. Comm'n, 475 U.S. 1 (1986) (striking down a requirement that electric utility companies include messages from opposing consumer groups in its envelopes)).

209. Johnson, *supra* note 115, at 8.

210. Johnson, *supra* note 115, at 8.

211. *Id.*

212. *See supra* Part III.A.

213. Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, Pub. L. No. 108-187, § 5(a)(2), 117 Stat. 2699, 2706-07 (2003). *See also* Jacquelyn Trussell, *Is the Can-Spam Act the Answer to the Growing Problem of Spam?*, 16 LOY. CONSUMER L. REV. 175, 182 (2004).

214. *See* Controlling the Assault of Non-Solicited Pornography and Marketing Act § 9; *see also* Telephone Consumer Protection Act of 1991, Pub. L. No. 102-243, 105 Stat. 2394 (1991). A "Do-Not-E-Mail" registry would essentially operate as a national database on which individuals could place their names and e-mail addresses to opt-out of receiving future unsolicited e-mails.

215. *Americans Ready to Delete Spam for Good; Survey Finds 83% Are Likely to Register for a "Do-Not-Spam List"* BUS. WIRE, Dec. 19, 2003 [hereinafter Americans Ready]. The statement was made by a representative from Synovate, a leading global market research firm. *Id.*

216. *See* Press Release, Direct Marketing Association, *The DMA Supports National Ant-Spam Law* (Dec. 8, 2003), *at* http://www.the-dma.org/cgi/disppressrelease?article=531.

a. The Telephone Consumer Protection Act (TCPA)

The TCPA was amended in 1991 to prohibit unsolicited faxes and prerecorded telephone calls to a residential line or business.[217] In *Destination Ventures v. FCC*, a direct marketing company that advertised via facsimile argued that the TCPA's restrictions were unconstitutional, since the government had singled out unsolicited advertisements, without showing that they were any less damaging than prank faxes or other types of faxes.[218] In considering this challenge, the Ninth Circuit Court of Appeals rearticulated the commercial speech doctrine:[219]

> Regulation of commercial speech must directly advance a substantial governmental interest in a manner that forms a "reasonable fit" with the interest. . . . The burden is on the government to demonstrate the reasonable fit. . . . The government's burden "is not satisfied by mere speculation or conjecture; rather, a governmental body seeking to sustain a restriction on commercial speech must demonstrate that the harms it recites are real and that its restriction will in fact alleviate them to a material degree."[220]

Applying this analysis, the court disagreed with the direct marketer's argument, finding no dispute that "unsolicited commercial fax solicitations are responsible for the bulk of advertising cost shifting."[221] Congress' ban was reasonable in light of its goal to reduce those costs, and the First Amendment did not require complete elimination of cost shifting before proactively addressing this problem.[222] Thus the TCPA has withstood

---

217. *See generally* Telephone Consumer Protection Act §§ 1-4. These provisions were clarified in a recent case against a telemarketer who violated the TCPA by calling an Ohio resident with a prerecorded message. Charvat v. Crawford, 799 N.E.2d 661 (Ohio 2003). In that case, the defendants argued that their calls were not "advertising" within the meaning of the Act, since they were simply providing the recipient with an opportunity to receive information. *Id.* at 663, 665 (citing 47 C.F.R. § 64.1200(f)(10)). The Ohio court disagreed, holding that "a prerecorded message that contains free offers and information about services and that asks the consumer to call a toll-free number to learn more is an unsolicited advertisement under the TCPA if sent without the called party's express invitation or permission." *Id.* at 666. Such calls were inadmissible under the Act. *Id.*

218. Destination Ventures, Ltd. v. FCC, 46 F.3d 54, 56 (9th Cir. 1995).

219. *See supra* Part III.A.1.

220. *Destination Ventures*, 46 F.3d at 55-56 (citing Cent. Hudson Gas and Elec. v. Pub. Serv. Comm'n, 447 U.S. 557, 566; Bd. of Trustees v. Fox, 492 U.S. 469, 480 (1989); and quoting Edenfield v. Fane, 507 U.S. 761, 770 (1993)).

221. *Id.* at 56.

222. *Id.* at 56. *See also* Covington & Burling v. Int'l Marketing & Research, Inc., 2003 WL 21384825, *3-4 (D.C. Super. Ct. April 27, 2003). In that case, the defendant sent 1,634 unsolicited faxes to the plaintiff's business, advertising vacation packages, advanced cellular communications, and more, despite repeated demands to stop. *Id.* The D.C. Superior court found that defendant's advertisements were misleading because they did not identify their senders, and thus failed even the

constitutional scrutiny at the circuit court level. However, the "Do-Not-Call" list that was implemented as a result of the TCPA has been somewhat more controversial.[223]

The National Do-Not-Call Registry is now managed and enforced by the FTC, the FCC, and the States.[224] As of October 2003, the registry is "open for business, putting consumers in charge of the telemarketing calls they get at home"[225] by allowing them to put their names on a national database that must be checked by marketers prior to making solicitations by telephone. Critics of a "Do-Not-E-Mail" list would likely point to recent challenges against this federal Do-Not-Call list.[226]

In *Mainstream Mktg. Services, Inc. v. FTC*, the district court in Colorado sustained an argument that the registry would create a burden on commercial speech, by singling it out from other types of speech.[227] The court began by applying the first prong of *Central Hudson* to determine that the registry was overbroad, since it affected all commercial speech whether or not it was deceptive.[228] Applying the second prong of *Central Hudson*, the court acknowledged that the government had a substantial interest in "protecting the well-being, tranquility, and privacy of the home [as] the highest order in a free and civilized society."[229] However, the third and fourth prongs of the *Central Hudson* test were not satisfied, since the interests did not justify treating commercial speech differently than non-commercial speech.[230] The district court reasoned that the harms sought to

---

first prong of the *Central Hudson* test. *Id.* at *3. Under the second and third prongs of *Central Hudson*, the court found that the government's interest in protecting consumers from the economic burden of unsolicited advertising was substantial enough to outweigh the defendant's commercial speech rights. *Id.* Finally, under the fourth prong, Congress' interest was not excessive, since it did not ban advertising by fax entirely, but merely required the consent of recipients before doing so. *Id.* at *4.

223. The Federal Trade Commission enacted a Rule with guidelines similar to that of the FCC's TCPA. 16 CFR Part 310; *see also* "Do Not Call" Provisions of Telemarketing Sales Rule, 64 Fed. Reg. 66124 (Nov. 24, 1999), *available at* http://www.ftc.gov/bcp/rulemaking/tsr/tsrrulemaking/tsrfrn991124.pdf (last visited Mar. 29, 2005). The Telemarketing Sales Rule (TSR) was promulgated in response to a congressional directive in the Telemarketing and Consumer Fraud and Abuse Prevention Act "to prescribe rules prohibiting deceptive and abusive telemarketing acts or practices." *Id.* at 66125 (citing 51 U.S.C. § 6101). Enacted into law in December 1995, this TSR similarly contains provisions for the implementation of a national "Do-Not-Call" registry. *Id.* Unlike the TCPA, which provides a private right of action for consumers who receive telemarketer calls in violation of the FCC's regulation, the TSR can be enforced by the Commission or the States. *Id.*

224. *See* FEDERAL TRADE COMMISSION, THE DO NOT CALL REGISTRY, *at* http://www.ftc.gov/donotcall/ (last visited Mar. 14, 2005).

225. *See id.*

226. *See, e.g.*, Mainstream Mktg. Servs., Inc. v. FTC, 283 F. Supp. 2d 1151 (D. Colo. 2003); *see also* Fraternal Order of Police v. Stenehjem, 287 F. Supp. 2d 1023 (D.N.D. 2003).

227. *Mainstream Mktg. Servs., Inc*, 283 F. Supp. 2d at 1168. Since there were exemptions for political or charitable speech, the argument was that there should be a privacy-based or prevention-of-abuse reason in support of such disparate treatment. *Id.*

228. *Id.* at 1162.

229. *Id.* at 1164. The court relied on the ancient notion expressed in precedent cases that "a man's home is his castle," and the right to be left alone was "'the most comprehensive of rights and the right most valued by civilized men.'" *Id.* (citations omitted).

230. *Id.* at 1167.

be prevented by banning commercial calls were just as likely to continue with non-commercial calls.[231]

The Tenth Circuit Court of Appeals reversed the district court's decision in February 2004.[232] Deviating from the district court's analysis of the final two prongs of *Central Hudson*, the court found a "reasonable fit" between the registry and the justifications.[233] "A reasonable fit exists between the do-not-call rules and the government's privacy and consumer protection interests if the regulation directly advances those interests and is narrowly tailored."[234] The court rearticulated the "narrowly tailored" standard as not the least restrictive measure available, but merely a "proportional response."[235]

In its analysis, the Tenth Circuit first denied the telemarketer's assertion that the registry was under-inclusive because it did not apply to political or charitable callers.[236] It reasoned that under-inclusiveness of commercial speech was a basis for a First Amendment claim only if it made the regulatory framework so irrational that it failed to advance its goals.[237] The Do-Not-Call list, however, would reduce a substantial number of invasive or abusive calls, thereby directly advancing the government's goals.[238]

The Tenth Circuit also found that the registry was narrowly tailored because it did not over-regulate protected speech, but simply restricted unwanted calls.[239] Furthermore, the regulation was not too restrictive, since "both sellers and consumers [were left] with a number of options to make and receive sales offers."[240]

The Tenth Circuit finally rejected the telemarketers' proposed alternatives, such as a company-specific approach, by which companies maintain their own do-not-call lists.[241] The court reasoned that this approach put the burden on the consumer to call every telemarketing company, such requests were often ignored, and the method had already been proven ineffective.[242] Thus, there were no less burdensome alternatives that would accomplish the government's objectives equally well.[243]

---

231. *Id.*
232. Mainstream Mktg. Servs., Inc. v. FTC, 358 F.3d 1228 (10th Cir. 2004), *cert. denied*, 125 S. Ct. 47 (2004).
233. *Id.* at 1238.
234. *Id.* (citing Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n, 447 U.S. 557, 564-65 (1980)).
235. *Id.* (citing Bd. of Trs. of State Univ. of N.Y. v. Fox, 492 U.S. 469, 480 (1989)).
236. *Id.*
237. *Id.* at 1238-39.
238. *Id.* at 1240.
239. *Id.* at 1241.
240. *Id.* at 1243.
241. *Id.* at 1244-45.
242. *Id.*
243. *Id.* at 1245.

A similar analysis was recently applied in *Fraternal Order of Police v. Stenehjem*, in which charitable organizations challenged a state statute that prohibited telemarketers (both commercial and non-commercial) from calling residents who registered for a state do-not-call list.[244] The court found that the portions in the statute regarding charitable speech were overbroad, since unlike commercial speech, charity involves speech that is fully protected by the First Amendment.[245] With regard to the commercial portions of the statute, however, the court found that there was a "reasonable fit" between the legislative goals and the means chosen to accomplish them.[246] The court reasoned that the do-not-call lists deter fraudulent telemarketers and allow an individual householder the private choice to decide whether or not to put his or her number on the list.[247] Finally, the statute did not ban commercial calls altogether, and it left marketers with reasonable alternatives to advertise.[248] Thus, the portions of the statute pertaining to commercial speech withstood constitutional scrutiny.

These cases show that "do-not-call" lists, whether provided for nationally or at the state level, will pass constitutional muster if they target solely commercial speech, and leave the power to opt-out in the hands of the individual.

b. Application to the Can-Spam Act

Given the outcome of these recent cases, it is likely that a "Do-Not-E-Mail" list would also be constitutionally sound, since the FTC's goals to prevent fraud and protect privacy within the realm of spam are the same as those in telemarketing.[249] Moreover, allowing consumers to put their own names on a national list would protect the sacred principle of individual autonomy.[250]

A distinction may be made between spam and telemarketing, however, in the fact that e-mail has been considered less intrusive than the telephone call. As noted in dicta in *Mainstream*:

> The intrusion upon residential privacy at issue here is the ringing of a telephone. That ringing may be more frequent than the consumer would like. It may come at times which are inconvenient. It may be disruptive. *Unlike junk mail or electronic spam*, it cannot be

244. Fraternal Order of Police v. Stenehjem, 287 F. Supp. 2d 1023 (D.N.D. 2003).

245. *Id.* at 1028. For fully protected speech cases, the first inquiry is whether or not the regulation is content based, meaning that the kind of speech at stake determines the law that applies. *Id.* If it is content-based, it is presumptively invalid. *Id.*

246. *Id.* at 1027-28. Again, the goals were essentially to protect the privacy of the home and the public from fraud and abuse. *Id.*

247. *Id.* at 1027-28.

248. *Id.*

249. *See* Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, Pub. L. No. 108-187, § 2, 117 Stat. 2699-2700 (2003).

250. *See* Rowan v. United States Post Office Dep't, 397 U.S. 728, 736-37 (1970) (discussing the principle of individual autonomy); *see also supra* Part II.

> dealt with at a time chosen by the recipient. It is invariably unwanted and adds to the stress of daily life.[251]

As a result of this distinction, it is possible that the third prong of *Central Hudson* would not be satisfied.[252] The individual already has some autonomy over the inconvenience caused by spam, being able to choose when to view it or delete it.[253] However, if it can be shown that a substantial number of commercial e-mail is false or misleading, or that it causes significant damage to consumers or businesses, then courts may find that the government interest outweighs that of the telemarketers.[254] Further, if the government can show that the list will decrease the number of illegal e-mails, while allowing the consensual transmission of e-mail to continue, then the means employed for the end may be reasonable and not too excessive.[255]

The Can-Spam Act in its current state does not require labeling or a do-not-e-mail list, but is merely directed towards eliminating false or misleading information and illegal spamming techniques.[256] If the FTC does end up implementing these provisions, however, there is a chance that direct marketers will get frustrated with the move toward an opt-in scheme.[257] Furthermore, when the FTC considers its duty to collaborate with global anti-spam strategists, it will be necessary to once again draw upon the balancing test set down in *Central Hudson* to ensure that all rights are protected. First, let us turn to the international regulations already in place.

V. SPAM LAWS OUTSIDE THE UNITED STATES

The Can-Spam Act includes a provision directing the FTC to cooperate with international fora to strategize and determine regulations that will potentially impact spammers outside the U.S. as well as within.[258] The

---

251. Mainstream Mktg. Servs., Inc. v. FTC, 284 F. Supp. 2d 1266, 1270 (D. Colo. 2003) (emphasis added).

252. *See* Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of NY, 447 U.S. 557, 566 (1980).

253. See Mainstream Mktg. Servs. Inc., 284 F. Supp. 2d at 1270.

254. In fact, e-mail is arguably *more* intrusive nowadays than the telephone. Since it is possible to turn a phone off and not answer calls, telemarketing may not be as disruptive as the *Mainstream* court proclaimed. Mainstream Mktg. Servs., Inc. v. FTC, 284 F. Supp. 2d 1266, 1270 (D. Colo. 2003). Meanwhile, e-mail has undeniably become one of the primary sources of communication around the world. *See* Patrick Seitz, *Next Wave Of Advances In Tech Will "Surprise Us," Gates Predicts; Software's Only Begun to Impact How We Live, Work and Learn, He Says*, INV. BUS. DAILY April 26, 2004, at A01.

255. *See Central Hudson*, 447 U.S. at 566. This is the fourth prong of the *Central Hudson* test. *Id.*

256. *See supra* notes 167-71 and accompanying text.

257. *See supra* notes 250-55.

258. Controlling the Assault of Non-Solicited Pornography and Marketing Act § 2(12).

importance of this provision lies in the need for a uniform system of regulation, especially given the fact that many spammers have retreated to countries with less stringent or no restrictions in the wake of legislation in the U.S.[259]

A. The European Directives

Though Europe has not experienced spam as acutely as the U.S., the European Union (E.U.) has reacted to the spam scare by establishing a variety of different schemes.[260] Spammers in Europe may be directly impacted by some or all of them.[261]

The first Directive to potentially impact the fight against spam was The Data Protection Directive of 1995.[262] The Directive defines "personal data" as "any information relating to an identified or identifiable natural person" and mandates that it should be collected fairly for a specified purpose.[263] The French government further specified that: "[t]he manner in which e-mail addresses are collected on the Internet must be in conformity with the rules laid down by data protection legislation and with the rights of the persons concerned."[264] Relying on these definitions of data protection, arguments can be made against spamming techniques, such as "harvesting" addresses.[265] However, the Directive had not yet directly broached that subject.[266]

In 1997, the E.U. passed a Telecommunications Directive, which, like the United States' TCPA, "forbids the use of automated dialing or fax machines for the purposes of direct marketing without the prior consent of the consumer."[267] This followed the earlier Distance Selling Directive, drafted in 1992 to require an opt-in scheme for fax and automated calls and

---

259. *See, e.g., China: Please Delete*, BUS. CHINA, Oct. 11, 2004, at 5 (discussing the fact that China is now the source of most of the world's unsolicited e-mail).

260. *See* John Magee, *The Law Regulating Unsolicited Commercial E-Mail: An International Perspective*, 19 SANTA CLARA COMPUTER & HIGH TECH. L.J. 333 (2003). The reason for the absence of litigation can perhaps be explained by the fact that the transposition deadlines for some of the Directives mentioned in this section are relatively recent, and it has not occurred to a number of Member States to seek legal remedies for violations. Serge Gauthronet & Etienne Drouard, *Unsolicited Commercial Communications and Data Protection* 5, 87 (Jan. 2001), *available at* http://europa.eu.int/comm/internal_market/privacy/docs/studies/spamstudy_en.pdf [hereinafter ARETE Report]. Furthermore, the usual response by spam recipients is to complain to their ISP, because the inconvenience caused is not perceived as sufficiently serious to warrant legal proceedings. *Id.* at 87.

261. *See* Magee, *supra* note 260, at 363-64.

262. *Id.* at 365-66; *see also* Council Directive 95/46/EC, 1995 O.J. (L 281) 31 (1995) [hereinafter Dir. 95/46/EC], *available at* http://europa.eu.int/comm/internal_market/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf.

263. Dir. 95/46/EC, *supra* note 262, at 38. *See also* Magee, *supra* note 260, at 365.

264. ARETE Report, *supra* note 260, at 84. In line with this reasoning, a company in Spain who sent unsolicited e-mails despite requests to cease, was sued under the Spanish version of the E.U.'s Data Protection Directive. *Id.* at 83-84. The Spanish Data Protection Agency found that an individual's e-mail address constituted personal data for purposes of the Directive. *Id.*

265. Magee, *supra* note 260, at 365-66.

266. *Id.* at 364.

267. *Id.* at 366-67; *see also* Council Directive 97/66/EC, 1998 O.J. (L 24) 1 (2000).

an opt-out scheme for other communication channels.[268] Though e-mail was not explicitly mentioned in that Directive, it is assumed that the phrase "other communication channels" comprises e-mail, thus implicating an opt-out scheme.[269]

The Electronic Commerce Directive was the first legislation in Europe to explicitly refer to unsolicited commercial e-mail, calling it "undesirable for consumers and information society service providers."[270] This Directive established a requirement for labeling as well as an "opt-out register" to be checked by marketers regularly, thus promoting the less stringent standard by which e-mail marketers can continue to send unsolicited e-mails.[271] After its publication in October 1998, the issue of whether to require an opt-in or opt-out mechanism was deliberated further among the E.U. Member States, European online industry organizations, ISPs, associations of consumers and Internet users, and national data protection authorities.[272]

It was not until the Electronic Communications Privacy Directive was proposed in 2000 that the E.U. first suggested the stricter compulsory opt-in standard for unsolicited commercial e-mail marketers.[273] This scheme would require the explicit consent of the recipient prior to sending any commercial e-mail, forbid the concealment of identity by the spammer, and mandate a valid address by which the recipient may opt-out.[274]

After hammering through an opt-in proposal for two years, the Directive on Privacy and Electronic Communications ("E-Communications Directive") was finally adopted on July 12, 2002.[275] This Directive is an extension of the Data Protection Directive of 1995[276] as well as an adaptation of the Telecommunications Directive to the electronic communications sector.[277] It requires the prior explicit consent of recipients before sending any communications by means of automated calling machines, fax, or e-mail.[278] The Directive does make two exceptions to this

268. Magee, *supra* note 260, at 367-68.

269. *See* ARETE Report, *supra* note 260, at 73-75.

270. Magee, *supra* note 260, at 368 (quoting Council Directive 2000/31/EC, 2000 O.J. (L 178) 1,5 (2000), *available at* http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/l_178/l_17820000717en00010016.pdf).

271. *Id.* at 368-69.

272. ARETE Report, *supra* note 260, at 78-79.

273. Magee, *supra* note 260, at 370.

274. *Id.* at 371-73.

275. *See* Dir. 2002/58/EC, *supra* note 15.

276. *Id.* at 37-38.

277. *Id.* at 37. It defines communications as including "any naming, numbering or addressing information provided by the sender of a communication or the user of a connection to carry out the communication." *Id.* at 38. One significant goal of the Directive was to harmonize the relevant Directives to minimize the obstacles to electronic communications in Europe. *Id.* at 37.

278. *Id.* at 45. The Directive defines consent as "given by any appropriate method enabling a freely given specific and informed indication of the user's wishes, including by ticking a box when visiting an Internet website. *Id.* at 38.

"opt-in" rule: (1) allowing a marketer to contact customers who have provided electronic contact information in the context of a business transaction,[279] and (2) allowing a marketer to contact non-natural persons.[280] In both cases, the recipient of unsolicited communication must have the clear opportunity to refuse further contact.[281]

B. Impact of the Directive on Privacy and Electronic Communications

In response to the recommendation that Member States transpose the Directive by October 2003,[282] many countries have implemented the opt-in scheme in the form of local laws.[283] Critics have remarked, however, that adding another local law will not make an obvious difference: "Responsible companies will observe regulations and life will become more difficult for them while the real nuisances will still be out there causing problems."[284]

The opt-in mechanism (which is even stricter than the United States' opt-out) is viewed as too "soft" and, at times, ineffective.[285] For example, companies that have retrieved e-mail addresses from customers in the course of a sale or service can then use that address for marketing purposes, even if the customer has previously opted out.[286]

On the other end of the spectrum, the Direct Marketing Association is concerned that "parts of the regulations may cause uncertainty for businesses."[287] Most British companies are "not up to speed" on how they may affect their online advertising formats.[288] Further, the Directive could have serious repercussions for marketers who are not prepared for the

---

279. *Id.* at 45.

280. *Id.* at 46.

281. *Id.* at 45-46.

282. *Id.* at 46.

283. In the U.K., for example, the new law mimics the Directive. Lee, *supra* note 17, at 8. In Italy also, the Data Protection Authority issued a ruling that enforces the "opt-in" mechanism. *See* Esther Van Weert, *Privacy Authority Clamps Down On Spammers*, WORLD EBUSINESS LAW REPORT, *available at* http://www.worldebusinesslawreport.com/ (Oct. 14, 2003). The ruling establishes that marketers must:

> [1] obtain a recipient's informed consent before sending any advertising or promotional material via email; [2] ensure that all communications contain their full contact details; [3] give recipients the opportunity to exercise their privacy rights (e.g., the right to revoke consent and to request information about the data source) in every communication; and [4] ascertain whether all the individuals listed in a database that has been bought from a third party have consented to receive advertising and promotional material.

Id. See also Emily Booth, *Vox-Pop: How Will the EC Directive Affect Digital Marketers?*, REVOLUTION, *available at* 2004 WL 55093565 (Jan. 1, 2004) [hereinafter Booth].

284. Lee, *supra* note 16, at 8.

285. *Id.*

286. *See* Dir. 2002/58/EC, *supra* note 15, at 45; John Naughton, *Business: The Networker: Expect to Keep Hitting That Delete Button*, THE OBSERVER, Dec. 14, 2003, at 8.

287. Lee, *supra* note 16, at 8.

288. Naughton, *supra* note 286, at 8. This includes a legitimate concern over how to design the "tick-the-box" option, wherein a customer essentially opts in to future mailings. *Id.* "To be legal from now on, the label on such a check-box must say 'tick here if you wish to receive marketing information.' Failure to tick the box can no longer be construed as passive consent." *Id.*

changes.[289] "For a marketing company to be found guilty of spamming (even if the e-mail was sent innocently) and fined would be extremely damaging, not only to the firm but to the brands it represents."[290]

As a result, marketers will need to implement stringent guidelines to clarify the motives of their messages so they won't be confused with spam.[291] The best way to do so, it is argued, "is to build in-house opt-in lists, which can be used to target customers during all [their] online campaigns."[292] This method ensures that marketers will target customers who have specifically agreed to receive communications.[293]

In regard to these more stringent guidelines, the regulations are commended for creating better data management in the industry.[294] There is a greater balance between what consumers can control via opt-in and who marketers can target with valuable communications.[295] Thus, the "focus on relationships and increased value for consumers should lead to the creative content of digital communications being increasingly tailored and relevant."[296]

C. Fundamental Rights and Freedoms

The Directive on Privacy and Electronic Communications also proposes not to "alter the existing balance between the individual's right to privacy and . . . lawful interception of electronic communications."[297] However, it does not directly address the freedom of expression that is a corollary to the First Amendment protection in the United States.[298] Some understanding of Article 10 of the European Convention for the Protection of Human Rights

---

289. Booth, *supra* note 283.

290. *Id.* For example, a breach could result in a summary prosecution and fines up to five thousand pounds. *Id.*

291. *Id.*

292. *Id.*

293. *Id.*

294. *Id.*

295. *Id.*

296. *Id.* This harmonizing view is essentially the premise behind a permission-based marketing scheme. ARETE Report, *supra* note 260, at 23-24. The ARETE report noted the success of several permission based marketing schemes, prior to enacting the Directive. *Id.* at 40-47. It also highlighted methods by which marketers could acquire the personal data they needed, such as placing opt-in forms on their website, which visitors must complete to subscribe, and sending a second welcome e-mail (double opt-in mechanism). *Id.* at 50-55.

297. Dir. 2002/58/EC, *supra* note 275, at 38. These provisions are guarantees of the European Convention for the Protection of Human Rights and Fundamental Freedoms that relate to the right to privacy and freedom from governmental interference. *See* European Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, arts. 7, 8, 213 U.N.T.S. 221 [hereinafter ECHRFF], *available at* http://www.echr.coe.int/Convention/webConvenENG.pdf.

298. However, Section III, Article 9 of the Data Protection Directive provides for exemptions from its provisions where "necessary to reconcile the right to privacy with the rules governing freedom of expression." Dir. 95/46/EC, *supra* note 15, at 42.

and Fundamental Freedoms (ECHRFF) is necessary for recognizing the scope of this right in Europe.

1. Commercial Speech under the European Convention

Although European countries do not have the same expansive constitutional protections as the United States, member states of the European Union are protected by the ECHRFF. Article 10 of that Charter 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."[299]

There is limited case law concerning the extent of commercial speech allowed by Article 10. However, there are some cases that may shed some light on the balance between the protection of individual privacy and the right to freely communicate in Europe.

In *Barthold v. Germany*, the European Court of Human Rights (ECHR) determined that commercial speech was directly connected with Article 10 freedoms.[300] In that case, a veterinary surgeon challenged a rule of professional conduct obliging him to refrain from advertising and publicity.[301] In reaching its decision, the ECHR relied on both E.U. and U.S. law to reason that "[r]egulation in this sphere is of course legitimate . . . but in order to maintain the free flow of information any restriction imposed should answer a 'pressing social need' and not mere expediency."[302] The ECHR found that there was no pressing social need to refrain from advertising altogether, so the regulation was overbroad in the context of Article 10.[303]

The ECHR similarly weighed freedom of expression against a legitimate need for quality and balance of television programs in *Demuth v. Switzerland*.[304] The applicant here claimed that the federal council's decision not to give him a license to broadcast his show violated Article 10.[305] The ECHR disagreed because, although the refusal to grant a license interfered with the applicant's right to expression, the interference was justified by the policies of the television programs to "contribute 'to general, varied and objective information to the public' [and] . . . 'bring closer to the

299. ECHRFF, *supra* note 297, art. 10. The Convention further provides that:
> 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 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. art. 10(2).

300. Barthold v. Germany, App. No. 8734/79, 7 Eur. H.R. Rep. 383, 397-98 (1985).

301. *Id.* at 396.

302. *Id.* at 408.

303. *Id.*

304. Demuth v. Switzerland, App. No. 38743/97, 38 Eur. H.R. Rep. 423 (2002).

305. *Id.* at 428.

public, the diversity of the country'; and . . . 'promote Swiss cultural enterprise.'"[306] The ECHR did acknowledge, however, that in order to encourage the free flow of information, supervision of such policies must be strict when they interfered with Article 10 rights and freedoms.[307]

In *Casado Coca v. Spain*, the ECHR again discussed the issue of whether advertising restrictions infringed upon the freedoms provided for in Article 10.[308] There, the Barcelona Bar Council brought disciplinary proceedings against a lawyer who placed advertisements in local newspapers.[309] The ECHR found that the lawyer was guaranteed freedom of expression by Article 10, regardless of whether his aim was profit-making, rather than political or artistic.[310] While the ECHR recognized that advertising may sometimes be restricted, especially to prevent the transmission of unfair competition and untruthful or misleading information, any restrictions must be closely scrutinized by the Court.[311]

Despite this "close scrutiny" standard, the ECHR in *Casado Coca* ultimately gave deference to the Barcelona Bar, since, although the bar banned advertising, it still authorized members to express their views to the media, make themselves known, and take part in the public debate.[312] The Bar rules were designed to protect the interests of the public while ensuring respect for its members.[313] Thus, the Bar authorities and Spain's courts were in a better position to determine the appropriate balance between the interests involved.[314]

2. Application of Article 10 to Electronic Commerce Directives

Article 10 and the scope of protection for commercial speech will likely be referenced in challenges against European anti-spam regulations. In the Netherlands, for example, there has already been some indication that the new model code for e-mail marketing, adapted from the latest "E-Communications" Directive, will be challenged as inconsistent with freedom

306. *Id.* at 434.

307. *Id.* at 433.

308. Casado Coca v. Spain, App. No. 15450/89, 18 Eur. H.R. Rep. 1 (1994).

309. *Id.* at 2-3.

310. *Id.* at 20. The distinction was made because traditionally, a stricter standard of protection is afforded speech that is artistic, literary or political. *See* Dir. 95/46/EC, *supra* note 262, Recital 17. However, the ECHR noted that Article 10 "does not apply solely to certain types of information or . . . forms of expression, in particular those of a political nature; it also encompasses artistic expression [and] information of a commercial nature. . . ." *Casado Coca*, 18 Eur. H.R. Rep. at 20 (citations omitted).

311. *Id.* at 15.

312. *Id.* at 2.

313. *Id.*

314. *Id.*

of expression.[315] The argument is that the language adopted for the opt-in regime is unclear, since it does not specify what types of practices constitute "consent."[316] As a result, direct marketers are claiming that any limitations on established practices, like trading e-mail addresses, would curtail their freedoms.[317]

An action against the "E-Communications" Directive was recently brought by an e-mail marketer in Spain who controlled an Internet site that sent unsolicited e-mails with an easy opt-out mechanism.[318] The applicant argued that, upon the Directive's implementation, his business would incur substantial cost from the need to send registered letters to each of his correspondents *before* sending Internet mailings.[319] He argued further that the Directive violated his freedom of expression, protected under Article 10 of the European Convention, among other treaties.[320] However, the Court of the First Instance (Fourth Chamber) denied standing to the applicant, since the Directive did not individually concern him.[321] The Directive had merely affected the applicant's capacity as an Internet user just as it affected other business users on the Internet.[322] Because the action was rendered inadmissible, there was not a substantial discussion of the Directive's impact on Article 10 freedoms.

Should an Article 10 argument be raised in another case against European anti-spam regulations, it is hard to predict exactly what the ECHR would decide. Based on *Demuth v. Switzerland*, the ECHR likely would strictly scrutinize any regulation that prevented the free flow of information and expressions.[323] At the same time, unlike the outright ban on public advertising in *Barthold v. Germany*, the elimination of unwanted, unsolicited e-mail will likely be recognized as a "pressing social need."[324] Finally, as long as advertisers have alternate means to reach the public, the ECHR can legitimize anti-spam regulations in the interests of individual privacy.[325] Within that line of reasoning, the ECHR would likely validate the opt-in

315. *See* Louis Jonker, *Marketing Organizations Argue Over Trade in E-mail Addresses*, WORLD EBUSINESS LAW REPORT, *available at* http://www.worldebusinesslawreport.com (Oct. 1, 2003).

316. For example, one company that already has an established business relationship with a consumer will trade e-mail addresses with another company. It is unclear under the Directives whether the latter company would have the consent required by an opt-in regime to contact the recipients of the traded e-mail addresses. *See* Dir. 2002/58/EC, *supra* note 275, at 45 ("[W]here a natural or legal person obtains from its customers their electronic contact details for electronic mail, in the context of the sale of a product or service . . . the same natural or legal person may use these electronic contact details for direct marketing of its own similar products.").

317. Jonker, *supra* note 315.

318. Vannieuwenhuyze-Morin v. European Parliament, *available in French at* http://europa.eu.int/eur-lex/pri/fr/oj/dat/2003/c_007/c_00720030111fr00210021.pdf (last visited Mar. 31, 2005).

319. *Id.*

320. *Id.*

321. *Id.*

322. *Id.*

323. *See* Demuth v. Switzerland, App. No. 38743/97, 38 Eur. H.R. Rep. 423 (2002).

324. *See* Barthold v. Germany, App. No. 8734/79, 7 Eur. H.R. Rep. 383, 397-98 (1985).

325. *See* Casado Coca v. Spain, App. No. 15450/89, 18 Eur. H.R. Rep. 1 (1994).

scheme, since it is not an outright ban on e-mail advertising, but rather a permission based alternative.

In conclusion, the European Directive calls for an opt-in scheme that may seriously affect the way marketers do business. It is likely that this provision will survive challenges based on Article 10 of the European Convention, if ever asserted, since the elimination of unsolicited e-mail is a pressing social need, and there are alternate means of advertising. Thus, it will be important at this stage to reach a consensus on the international scope of Europe's opt-in scheme, if it is to have any impact on spammers around the world.

VI. THE CALL FOR RECONCILIATION - CAN SPAM BE ELIMINATED?

> The rise of the global computer network is destroying the link between geographical location and (1) the power of [the] local [government] to assert control over online behavior; (2) the effects of online behaviour on individuals or things; (3) the legitimacy of [the efforts of] a local [sovereign to enforce rules applicable to] global phenomena; and (4) the ability of physical location to give notice of which sets of rules apply.[326]

Given the universal nature of the Internet, jurisdiction matters not only in the United States, but around the world.[327] Some commentators say that it should be determined by where the Internet server is located.[328] Others contend that mere physical presence in a particular state does not provide sufficient contacts to create jurisdiction over a Web site.[329]

In Europe, the Electronic Commerce Directives employ a "country of origin" approach to determine jurisdiction over ISPs.[330] This approach dictates that, without an agreement to the contrary, law will govern in "the country in which an [ISP] maintains a fixed establishment, regardless of where the Web site or server is located."[331] Despite these provisions, unsolicited spam will continue to pose enforcement problems, since laws in

---

326. Magee, *supra* note 260, at 379 (quoting David R. Johnson & David Post, *Law and Borders - The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1370 (1996) (advocating self-regulation of the Internet on a global level)).

327. *See* Goldsmith & Sykes, *supra* note 160, at 825-26.

328. *See* Andre R. Jaglom, *Liability On-Line: Choice of Law and Jurisdiction on the Internet, or Who's In Charge Here?*, *available at* http://www.tanhelp.com/newsworthy/Articles/LiabilityOn-Line.pdf (last visited Mar. 31, 2005).

329. *Id.* at 2-3.

330. *Id.* at 11.

331. *Id.* This principle does not apply to consumer transaction contracts, for which consumers remain protected by the laws of their own nation. *Id.* However, the Directives recommend that companies selling over the Internet consider jurisdiction both with regard to electronic transactions in general, and "with regard to how the contract is executed and performed." *Id.*

individual countries will not have any power over messages originating from other countries.[332] Thus it will be necessary to reach a common ground, both legally and technologically.

A. An Opt-In Scheme in the U.S.?

The essential difference between the European and American approach to anti-spam legislation is that the former mandates an opt-in scheme.[333] A report put out by the E.U.'s ARETE Commission in January 2001 included an exhaustive study of the spam problem and what individual countries were doing about it.[334] In advocating the more stringent opt-in approach to spam, the authors of the ARETE report relied on the theory that permission-based marketing was a more effective way to meet consumers who were willing to participate in an exchange.[335] These authors noted that the opt-out approach, on the other hand, "amounts to giving the e-mail user a sponge to mop up a flood of commercial messages which will never run dry . . . depriv[ing] Internet users of their rights over their own mailboxes."[336]

Should Congress decide to amend the Can-Spam Act to bring it into conformity with the European scheme, the question remains whether an opt-in scheme would pass constitutional muster.[337] In this analysis, courts would likely draw on cases challenging the Telephone Consumer Protection Act (TCPA), and specific provisions relating to prerecorded telephone calls and unsolicited facsimiles.[338] They may note that an opt-in scheme is already essentially in place for the use of fax and pre-recorded advertising.[339] The

---

332. One writer reported:

> Legislation varies, even within the EU. . . . In Germany it is far easier to deal with spam than here, but in the U.S. it is not, although California has just introduced regulations. An international treaty would be the best way forward, but some of the countries we are talking about don't even have proper domestic legislation.

See Lee, *supra* note 16, at 8 (internal quotations omitted).

In the UK, where spam legislation has already taken effect, critics also say: "It is hard to see what any regulations in this country can do. . . . A lot of problem spams come from overseas, often Asia or the U.S., so it makes little difference that there is legislation in the UK." *Id.*

333. *See generally* Brandon Mitchener, *Europe Blames Weaker U.S. Law for Spam Surge*, WALL ST. J., Feb. 3, 2004, at B1.

334. ARETE Report, *supra* note 260, at 5.

335. *Id.* at 23. The authors relied on SETH GODIN, PERMISSION MARKETING: TURNING STRANGERS INTO FRIENDS, AND FRIENDS INTO CUSTOMERS (Simon & Schuster 1999) for this approach. *Id.* at 23-24. They also pointed to an IMT Strategies report that indicated a greater response rate for permission based e-mails. *Id.* at 25-26 (citing IMT, *Permission E-mail: The Future of Direct Marketing*, *available at* http://ezine-tips.com/list-tips/list-advertising/19991207.shtml). That study showed that 70% of Internet users clicked either a few times, several times, or often on advertising messages sent by permission, compared with just 30% in the case of unsolicited e-mails. *Id.* at 26.

336. *Id.* at 65.

337. Europe has been calling for the U.S. to crack down on spam by using on opt-in scheme. Mitchener, *supra* note 334, at B1. The Organization for Cooperation and Development also meets on a regular basis to encourage greater international law-enforcement cooperation to fight spammers. *Id.*

338. *See supra* Part IV.C.

339. *See* U.S.C. § 227(b)(1)(A)-(D).

court has upheld this scheme in challenges such as *Mainstream* on two primary grounds: "[O]ne was that a fax coming in would occupy the line and prevent legitimate business activities, and the second was that unsolicited faxes shifted the costs of advertising to the recipient, forcing it to incur paper and toner charges."[340] Just as with faxes, sending large volumes of e-mail shifts advertising costs to the consumer, while the cost to the spammer is negligible.[341]

It is possible that an outright ban on spam would limit commercial expression by eliminating solicitation. The Supreme Court has recognized that "solicitation allows direct and spontaneous communication between buyer and seller . . . so solicitation produces more personal interchange between buyer and seller than would occur if only buyers were permitted to initiate contact."[342] Thus, even if the government were to show a substantial interest in minimizing costs to consumers, courts would most likely find that a total prohibition on spam would violate the Constitution.[343]

However, an opt-in scheme is not an outright ban on spam. Advertisers still have an opportunity to reach consumers, as long as they obtain consent through legitimate transactions.[344] There are also multiple avenues to continue communicating with the public, such as television commercials, banner ads, and other online mechanisms. Some concern may be appropriate on the part of smaller businesses who cannot afford more savvy advertising techniques. However, courts would need to carefully balance these interests against the damage caused to Internet communications by the volume of unwanted spam.[345]

Even were an opt-in scheme to be deployed in the United States, it is likely that spam will continue to thrive, due to easy access to consumer information and limited enforcement mechanisms against spammers without a physical address.[346] Thus, because of the limited scope of both the Can-Spam Act and the European Directives, it is necessary to consider alternate means of ridding the world of spam.

---

340. Johnson, *supra* note 115, at 7.

341. *Id.* One potential distinction is that use of phones and faxes may completely block business' use of the phone lines, while use of e-mail does not necessarily block Internet connections, at least for users with large storage space. *Id.*

342. Edenfield v. Fane, 507 U.S. 761, 766 (1992).

343. *See* Johnson, *supra* note 115, at 8.

344. *See supra* notes 77-78 and accompanying text.

345. Johnson, *supra* note 115, at 7.

346. *See* Naughton, *supra* note 286, at 8; *see generally* Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, Pub. L. No. 108-187, §§ 5(a)(3), 5(a)(6), 7, 11, 117 Stat. 2699, 2707-08, 2711, 2717 (2003) (providing only for "who" may bring an action against those who violate the Act, not "how").

B. Self-Regulation

Law in Cyberspace is slowly evolving into a balance between governmental micromanagement and decentralized regulation by website owners and companies.[347] Without stringent government regulation in the realm of spam, companies have considered methods of self-governance.[348]

Microsoft has an anti-spam policy that prohibits the use of MSN services "in any manner associated with the transmission, distribution or delivery of any unsolicited bulk or unsolicited commercial e-mail."[349] In addition to prohibiting users from delivering spam to any of Microsoft's MSN services or customers, the policy does not allow users to:

> [1] use or contain invalid or forged headers; [2] use or contain invalid or non-existent domain names; [3] employ any technique to otherwise misrepresent, hide or obscure any information in identifying the point of origin or the transmission path; [4] use other means of deceptive addressing; [5] use a third party's [I]nternet domain name, or be relayed from or through a third party's equipment, without permission of the third party; [6] contain false or misleading information in the subject line or otherwise contain false or misleading content. . . .[350]

Microsoft provides for enforcement of its policies by blocking messages from a particular Internet domain, or taking legal action.[351]

Similarly, America Online's anti-spam policy "does not authorize the use of its proprietary computers and computer network (the AOL Network') [sic] to accept, transmit or distribute unsolicited bulk e-mail sent from the Internet to AOL members."[352] The policy prohibits the use of invalid or forged headers, deceptive advertising, or harvesting.[353] AOL will also take legal and technical steps to prevent the unauthorized use of e-mail.[354]

The Direct Marketing Association (DMA) is a strong advocate of self-regulation techniques, and in fact has set up its own "Electronic Mail Preference Service" ("e-MPS") to allow users to opt-out of unsolicited e-mail.[355] However, the DMA's methods have been criticized by anti-spam activists because: 1) opt-out lists are based on the principle that the onus is on users to take action, 2) ISPs can't opt-out of an entire domain, and 3) the

---

347. For a full discussion of governance on the Internet, *see The Culture of Cyberspace*, 93 AM. SOC'Y INT'L L. PROC. 354 (1999) [hereinafter "Culture of Cyberspace"].

348. *See, e.g.*, Microsoft Anti-Spam Policy, http://privacy.msn.com/anti-spam (last modified Sept. 2003); AOL Unsolicited Bulk E-Mail Policy, http://postmaster.info.aol.com/guidelines/bulk_email.html (highlighting some common anti-spam policies by private actors).

349. *See* Microsoft Anti-Spam Policy, *supra* note 348.

350. *See id.*

351. *See id.*

352. *See* AOL Unsolicited Bulk E-Mail Policy, *supra* note 348.

353. *Id.*

354. *Id.* AOL's policy lists actions under the Computer Fraud and Abuse Act, the Virginia Computer Crimes Act, and the CAN-SPAM Act of 2003. *Id.*

355. ARETE Commission, *supra* note 260, at 29.

DMA wants to preserve unsolicited commercial e-mail as a powerful marketing tool, rather than solely permission based.[356]

Although these policies inherently require legal enforcement, many would argue that "[t]he most successful battle against spam is being waged through technology by large companies and ISPs."[357] This is largely because those companies have the resources and means to employ a variety of different filtering techniques.[358] The ultimate question is whether any of the policies above will be able to succeed in eliminating spam in the face of continually sophistocated technology.

C. How to Fight Back

While bulk e-mail has shown no sign of waning since its inception.[359] there is a plethora of measures available for individuals to keep the spam at bay. For example, an international group called "The Spamhaus Project" regularly releases "block lists," which block incoming spam from direct spam sources.[360] Similarly, some anti-spam groups provide black lists, consisting of the IP addresses of repeat spammers.[361] The lists allow corporate systems to block messages from those addresses.[362] A potential problem with this technique is that, in order to save legitimate messages, users must know how to reverse the process by creating "white list" addresses.[363] A recently implemented program called "Mailblocks" is a web-based service that allows users to apply a challenge/response system, by which a sender must answer a question prior to sending the e-mail.[364] Automated spam systems will fail this test, either because they can't respond, or because they use false return addresses.[365]

Microsoft has suggested a new approach to the elimination of spam. It is currently working with e-mail providers to set up a sort of "caller ID" system for the Internet.[366] Under this system, ISPs and corporate e-mail

---

356. *Id.*

357. Johnson, *supra* note 115, at 4.

358. *Id.*

359. *See, e.g., Bulk Email Software*, http://www.americaint.com/bulk-email-software/email-marketing-software.html (last visted Mar. 31, 2005) (providing more information on the latest bulk e-mail products on the market).

360. *See* The Spamhaus Project, http://www.spamhaus.org/ (last visited Mar. 15, 2005).

361. Johnson, *supra* note 115, at 4.

362. *Id.*

363. *Id.* "White lists" would consist of addresses from which the user *will* accept messages. *Id.*

364. Walter S. Mossberg, *Mailblocks Will Keep Your Mail Spam-Free, Without the Guesswork*, WALL ST. J., Feb. 19, 2004, at B1.

365. *Id.* Mailblocks also allow users to receive "good" automated e-mail, like online newsletters or purchase confirmations, by creating "tracker" addresses, which are used to sign up for various services. *Id.*

366. Robert A. Guth & Mylene Mangalindan, *Microsoft Takes "Caller ID" Tack Against Spam*, WALL ST. J., Feb. 25, 2004, at B3.

users would be required to post legitimate addresses, thus creating a registry for e-mail recipients seeking to authenticate messages.[367] This method would verify the e-mail senders' identities, rather than just filter out unwanted mail.[368]

Although the computer software industry is getting smarter with its anti-spam filters,[369] spammers have become equally more creative with the words (or non-words) they use in order to avoid such filters. For example, you might see solicitations for diet pills and other unsolicited goods using phrases that often have nothing to do with the marketer's pitch, like "congratulatory salaam transferred flatulent statesmen."[370]

Individuals can also do a lot on their own, however, to eliminate unwanted spam. "Tech Live," an online magazine with continual updates on computer issues, gives some tips to beat spammers.[371] These include: 1) installing a spam filter, 2) using several different e-mail accounts,[372] 3) using "at" instead of "@" for the e-mail address,[373] 4) never unsubscribing to spam[374] and 5) never participating in a transaction with a spam marketer.[375]

Although many of these techniques are tedious and time-consuming, they may be the only way, and indeed, a necessary way to truly attack the spam problem.

VII. CONCLUSION

Because it appears that an opt-out scheme will be largely ineffective against spammers who follow the guidelines, the recent enactment of the Can-Spam Act will do little to rid our inboxes of unwanted mail.[376] However, it is a step in the right direction, if it supplements the efforts of direct marketing organizations and Internet service providers to implement technologically feasible methods to give consumers autonomy over their

---

367. *Id.*

368. *Id.*

369. *See Symantec Products and Services*, http://www.symantec.com/product/ (last visited Mar. 31, 2005) (providing news and information on the latest products put out by Symantec and IBM).

370. Pui-Wing Tam, *Fruitcake Debutantes Defined by O, and Other Spam Tricks*, WALL ST. J., May 28, 2004, at B1.

371. *See* Lindsay Martell, *Fight Spam: Tips for Stopping the Endless Barrage of Unwanted Email*, *available at* http://www.g4tv.com/techtvvault/features/43639/Fight_Spam.html (last visited Mar. 15, 2005).

372. *Id.* For example, use one for online sign-ups, another for newsletters, and a personal one strictly for closest friends and family. *Id.*

373. *Id.* This is because spam engines won't recognize it as an e-mail address, but humans would change it back. *Id.*

374. *Id.* That's how they figure out your live e-mail address. *Id.*

375. *Id.*

376. *See Can-Spam Law Violations Continue at High Rate for Second Month in a Row, According to Audiotrieve InBoxer Anti-Spam Study*, BUS. WIRE, Feb. 10, 2004. Studies show that "[m]ore than 86 percent of the spam messages studied violated at least one aspect of the CAN-SPAM law and most violated almost all of the provisions." *Id.* Thus "CAN-SPAM is failing to stop the plague of unwanted email messages." *Id. See also* Ryan J. Foley & Don Clark, *Spam Pact Toughens Penalties, But Critics See a Lack of Muscle*, WALL ST. J., Nov. 24, 2003, at A3; *see also supra* Part IV.

inboxes.[377] Moreover, the current provisions of the Can-Spam Act are likely to pass constitutional muster, since the government's interest in protecting the public from fraud and deceptive marketing tactics is substantial, and the elimination of illegal spamming techniques is not excessive.[378] If a "Do-Not-E-Mail" registry were implemented by the FTC, it may withstand constitutional challenge as well, due to recent decisions upholding the "Do-Not-Call" list.[379]

While it seems as though the opt-in scheme proposed by the European Directives will be more effective at stamping out spam on an international level, there remain some constitutional concerns with its implementation in the United States.[380] The opt-in scheme poses potential problems for newly developed businesses that do not already have a broad consumer base.[381] Unless U.S. courts recognize that an opt-in scheme would allow for alternate means of communication, such as permission-based marketing, then this scheme would likely be subject to the limitations of the Constitution.[382]

Self-regulation and filtering technology remain available to consumers who wish to rid their inboxes of unsolicited e-mail altogether. Technology is subject to error, however, and the fight continues to escalate as spammers become more sophisticated. Thus, while technology and the law attempt to meet on common ground, the rock of Sisyphus rolls right back down. And it appears that the only way to beat spam completely is by the individual stroke of the "delete" key.[383]

Amy G. Marino[384]

377. *See supra* Part VI.C.

378. *See supra* Part IV.C.

379. *See supra* Part IV.C.2.b.

380. *See supra* Part VI.A.

381. *See generally* Brandon Mitchener, *Europe Blames Weaker U.S. Law for Spam Surge*, WALL ST. J., Feb. 3, 2004, at B1.

382. *See supra* note 110-12 and accompanying text.

383. *See generally* Zuzel, *supra* note 2.

384. J.D. Candidate 2005. B.A./B.M., Oberlin College and Conservatory 1998. Thank you, Mark and Matthew, and all who encouraged me to finish this comment and my law school education. The topic can be attributted to the spammers who still invade my inbox.