STATE REGULATION OF UNSOLICITED COMMERCIAL E-MAIL

By Sabra-Anne Kelin

A disgruntled employee (E) of a major corporation (C) wants to discuss with other employees the employment practices of C. Since C has many employees, E decides that the best way to contact all of them is via e-mail. E sends an e-mail message to all of C's employees at their business e-mail addresses. The e-mail presents some of C's employment practices and asks the employees to share their experiences. C sues E for sending unsolicited e-mail to its employees. The cause of action is for trespass to chattels, the chattels being C's network of e-mail servers.

The preceding situation is not a law school hypothetical—it actually happened.[1] The employee was Kourosh Hamidi, and the corporation was Intel.[2] On June 16, 1999, a state court permanently enjoined Hamidi and his nonprofit organization Former And Current Employees of Intel ("FACE Intel") from sending unsolicited e-mail to addresses on Intel's computer systems.[3] Hamidi appealed the order on July 2, 1999.[4]

The Intel/Hamidi controversy illustrates one of many problems created by the increased use of and sensitivity to unsolicited e-mail. The private sector has tried to control unsolicited e-mail, but so far the proposed solutions are unacceptable. As for the public sector, state anti-spam legislation might be a viable alternative. However, in the past year, two state laws regulating unsolicited e-mail have been held unconstitutional under the dormant Commerce Clause.[5] This Note surveys the problem of unsolicited e-mail and examines its possible solutions. Due to the constitutional limi-

1. Motion for Summary Judgment Tentative Ruling, Intel Corp. v. Hamidi, No. 98-AS-05067, 1999 WL 450944 (Cal. Super. Apr. 28, 1999).

2. *Id.*

3. Order for Entry of Final Judgment, Intel Corp. v. Hamidi, No. 98-AS-05067 (Cal. Super. June 16, 1999), *available at* http://cyber.law.harvard.edu/msvh/hamidi/finalorder.html.

4. Notice of Appeal, Intel Corp. v. Hamidi, No 98-AS-05067 (Cal. Super. July 2, 1999), *available at* http://eon.law.harvard.edu/openlaw/intelvhamidi/appealnotice.html. For more information on the Intel v. Hamidi case, see FACE Intel, *at* http://www.faceintel.com/ (last visited Feb. 11, 2001); Jocelyn Dabeau, Berkman Center for Internet & Society (Harvard Law School), Intel v. Hamidi, *at* http://eon.law.harvard.edu/openlaw/intelvhamidi/ (last modified Feb. 20, 2000).

5. *See infra* Part II.B.2.

tations on state legislation, federal legislation represents the most promising means to address the problems associated with unsolicited e-mail.

I. E-MAIL AND THE RISE OF SPAM

Approximately 116.5 million Americans have used the Internet.[6] Although the Internet comprises many telecommunications technologies, such as the World Wide Web, telnet, and Internet Relay Chat, the most widely used application is electronic mail ("e-mail").[7] Nearly two years ago, it was estimated that 2.2 billion e-mail messages were sent worldwide daily, which translates to 803 billion sent annually.[8]

E-mail resembles conventional paper-based mail. Both can be used to send either a personalized message to one person or an impersonal message to many people simultaneously. Sending "bulk mail" (impersonal messages with many recipients) is an easy way to reach a large audience. Frequently commercial in nature, bulk e-mail consists largely of advertisements or solicitations for charitable donations. Since its recipients often do not want it,[9] bulk e-mail is commonly referred to as "junk" e-mail or "spam."[10] People who send spam are called "spammers."

---

6. U.S. DEP'T OF COMMERCE, FALLING THROUGH THE NET: TOWARD DIGITAL INCLUSION 33 (2000), http://search.ntia.doc.gov/pdf/fttn00.pdf.

7. *Id.* at 47. About eighty percent of Internet users have used electronic mail. *Id.*

8. Calvin Whang, Comment, *An Analysis of California's Common and Statutory Law Dealing with Unsolicited Commercial Electronic Mail: An Argument for Revision*, 37 SAN DIEGO L. REV. 1201, 1203 n.6 (2000) ("Of the 2.2 billion electronic messages sent daily, some analysts think that 10% or 220 million messages are spam.").

9. A survey of over 1,000 Internet users reported that 43% of users hate bulk e-mail, and 25% consider it bothersome; 68.5% of respondents reported that junk e-mail is not useful at all. Barry D. Bowen, *Controlling Unsolicited Bulk E-mail*, UNIX INSIDER, *at* http://www.sunworld.com/sunworldonline/swol-08-1997/swol-08-junkemail.html (last modified Jan. 22, 2001).

10. Other commonly used phrases include "unsolicited bulk e-mail" ("UBE") and "unsolicited commercial e-mail" ("UCE"). Bulk e-mail can be either commercial (such as an advertisement) or non-commercial (such as a joke or chain letter). Both types are equally costly to Internet Service Providers ("ISPs") and recipients (see *infra* notes 14 to 19 and accompanying text). However, the spam controversy generally focuses on commercial bulk e-mail, since that is the most common type of bulk e-mail. Some state statutes regulate all unsolicited e-mail, whether commercial or not (Virginia, West Virginia, Oklahoma, Connecticut, and Rhode Island). These statutes raise many First Amendment issues, since the First Amendment protects non-commercial speech more than it protects commercial speech. This Note addresses only commercial spam.

Recently, advertisers have begun to take advantage of the low cost of sending bulk e-mail.[11] In 1999, analysts estimated that 80.3 billion pieces of junk e-mail are sent each year.[12] A recent study found that over ninety percent of e-mail users receive spam at least once a week, while almost fifty percent of users receive spam six or more times per week.[13] As the number of bulk e-mail messages has grown, so has the burden bulk e-mail imposes on Internet Service Providers ("ISPs") and recipients. A recent study estimated that ten percent of ISP revenues are used to combat spam.[14] ISPs suffer most of this loss[15] in the form of customer attrition[16] and extra costs for staffing (due to increased traffic and user complaints) and hardware (to obtain more storage and bandwidth).[17] Spam can also cause networks to shut down completely.[18] Costs imposed on the recipient include money spent for Internet access time to download, read, and delete the spam.[19]

---

11. It is much less expensive to send bulk e-mail than conventional mail. Each additional piece of conventional mail requires both another paper copy and additional postage. With e-mail, however, the only cost to the sender is typing one more e-mail address into the recipient list. The true cost of bulk e-mail is shifted to other parties, such as the sender's ISP, the recipients' ISPs, and the recipients themselves. The sender never bears the additional costs imposed on the ISPs and the recipients. *Junk E-mail: Hearings Before the Senate Subcomm. on Communications of the Senate Comm. on Commerce, Science and Transportation*, 105th Cong. (1998), *available at* 1998 WL 12761269 (statement of Deirdre Mulligan, Staff Counsel, The Center for Democracy and Technology).

12. Whang, *supra* note 8, at 1203 n. 6.

13. Gartner Group, *ISPs and Spam: The Impact of Spam on Customer Retention and Acquisition* 4, http://www.brightmail.com/global/pdf/gartner.pdf (June 14, 1999).

14. Whang, *supra* note 8, at 1207 n.42.

15. Spam can cost ISPs hundreds of thousands of dollars per year. Bowen, *supra* note 9.

16. ISPs lose seven percent of their new customers every year to spam. Gartner Group, *supra* note 13, at 8-9.

17. *Id.* at 12.

18. Whang, *supra* note 8, at 1208. In response to these losses, ISPs have sued spammers, such as Cyber Promotions, for damages. *See, e.g.*, CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015 (S.D. Ohio 1997) (enjoining Cyber Promotions from sending any unsolicited advertisements to any electronic mail address maintained by CompuServe); Am. Online, Inc. v. Cyber Promotions, Inc., 948 F. Supp. 436 (E.D. Pa. 1996) (allowing America Online to block Cyber Promotions from sending unsolicited e-mail advertisements over the Internet to members of America Online).

19. *See* Gartner Group, *supra* note 13, at 7. In addition, it is likely that ISPs will transfer their spam-related expenses to their customers.

II. PRIVATE AND LEGISLATIVE RESPONSES TO SPAM

In response to rising spam costs, the private and public sectors have attempted to curtail spam.[20] This section begins with an overview of the private sector's response to spam, including norms, technology, and organizations. It then describes state legislative responses to spam, including general approaches to anti-spam legislation and specific anti-spam laws.

A. Private Responses to Spam

The private responses to spam consist primarily of enforcement of Internet social norms.[21] Like other societal norms, Internet norms are largely unwritten. However, since most Internet users dislike spam,[22] commentators have argued that spamming violates Internet norms, sometimes referred to as "netiquette."[23] Indeed, violation of netiquette can sometimes have legal consequences.[24] ISPs and other private organizations are the primary actors in the private-sector spam regulation area.[25]

---

20. The private sector responded to spam first, followed by the public sector. Although spam has only recently become a widespread problem (see *supra* note 12 and accompanying text), the private sector recognized that unwanted e-mail was a potential problem in the early days of the Internet. *See, e.g.*, J. Postel, *On the Junk Mail Problem*, Network Working Group Request for Comments (RFC): 706, NIC #33861 (Nov. 1975), *available at* http://www.landfield.com/rfcs/rfc706.html; P. Denning, *Electronic Junk*, 25 COMMUNICATIONS OF THE ACM 163 (1982).

21. "Norms" have been described as "systems of rules and sanctions created and administered without reliance on State 'authority,' and outside of any formal State-managed process." David G. Post, Of Black Holes and Decentralized Law-Making in Cyberspace (Jan. 31, 2000) (unpublished manuscript), http://www.temple.edu/lawschool/dpost/blackhole.html.

22. *See supra* note 9.

23. M. Mitchell Waldrop, *Culture Shock on the Networks*, 265 SCIENCE 879, 880 (1994) (describing netiquette as "the unwritten rules that tell users not to waste other people's time with irrelevant electronic chatter—and especially, not to sully the network with self-serving advertisements and junk mail"); Joshua A. Marcus, Note, *Commercial Speech on the Internet: Spam and the First Amendment*, 16 CARDOZO ARTS & ENT. L.J. 245, 247 (1998) ("Netiquette, among other things, established that advertisers wishing to advertise on-line should confine their activities to sites where advertisements would be welcomed."). "Netiquette" is a combination of the words "net" (for Internet) and "etiquette."

24. Recently, a Canadian court held a spammer liable for violation of these somewhat vague netiquette rules. 1267623 Ontario Inc. v. Nexx Online Inc., [1999] 1999 Ont. Sup. C.J. LEXIS 465 (Ont. Sup. Ct. Just.).

25. At least one commentator has suggested that private self-regulation is the "most attractive" way to regulate the Internet. *See* Christopher S.W. Blake, Note, *Destination Unknown: Does the Internet's Lack of Physical Situs Preclude State and Federal Attempts to Regulate It?*, 46 CLEV. ST. L. REV. 129, 157 (1998).

1. *How ISPs and Other Organizations Control Spam*

ISPs control spam via their contractual use policies. Recently, ISPs have begun to include Internet norms regarding spam in their use policies.[26] While some of these use policies use the vague term "netiquette" to indicate acceptable behavior,[27] others explicitly disallow using the ISP to send spam.[28]

Because sending spam involves two ISPs, the sender's and the recipient's, a use policy can combat spam in two ways: by preventing subscribers from sending spam, and by blocking incoming spam from outside users. The first way obtains its legal power from the contract that the subscriber signed with the ISP. The second method, blocking incoming e-mail, does not have the same legal power because the outside user has no contract with the recipient's ISP.[29] Thus, to control spam, an ISP uses filtering software.[30] Once detected by the filtering software, spam can be

---

26. For example, America Online's ("AOL") Unsolicited Bulk E-mail Policy explicitly forbids using AOL's network to "accept, transmit or distribute unsolicited bulk e-mail sent from the Internet to AOL members." America Online, Inc., Unsolicited Bulk E-Mail, *at* http://www.aol.com/info/bulkemail.html (last visited Jan. 31, 2001). Yahoo's Terms of Service prohibit using the Service to "upload, post, email, transmit or otherwise make available any unsolicited or unauthorized advertising, promotional materials, 'junk mail,' [or] 'spam' . . . or any other form of solicitation, except in those areas (such as shopping rooms) that are designated for such purpose." Yahoo! Inc., Terms of Service § 6(g), *at* http://docs.yahoo.com/info/terms/ (last visited Jan. 31, 2001).

27. Carl S. Kaplan, *An Argument for 'Netiquette' Holds up In Court*, N.Y. TIMES ON THE WEB, July 16, 1999, *at* http://www.nytimes.com/library/tech/99/07/cyber/cyberlaw/16law.html. *1267623 Ontario* involved an ISP policy that required users to conform to netiquette. *1267623 Ontario*, 1999 Ont. Sup. C.J. LEXIS 465, *5.

28. *See* Kaplan, *supra* note 27.

29. However, some state laws give ISP policies the force of law. In general, these laws allow ISPs to sue spammers for trespass to chattels (the chattels being the ISP's computer system). *See, e.g.*, CAL. BUS. & PROF. CODE § 17538.45 (West Supp. 2000) (discussed *infra* Part II.B.2.b); *see also* Dan L. Burk, *The Trouble with Trespass*, 4 J. SMALL & EMERGING BUS. L. 27 (2000) (criticizing the use of trespass to chattels to prohibit electronic communications); Carl S. Kaplan, *Treat EBay Listings as Property? Lawyers See a Threat*, N.Y. TIMES ON THE WEB, July 28, 2000, *at* http://www.nytimes.com/library/tech/00/07/cyber/cyberlaw/28law.html.

30. One example of a spam-filtering product made for ISPs is Brightmail Anti-Spam. *See* Brightmail, Inc., *Brightmail Anti-Spam*, *at* http://www.brightmail.com/isp/anti-spam/ (last visited Feb. 11, 2000). Common ways of detecting spam include examining the subject line and body of the e-mail for frequent use of words such as "make money" and "free offer." Since the computer performs the detection, the detection is not perfect. Thus, there might be false positives (messages which are not spam but are treated like spam) and false negatives (messages which are spam but are not caught by the system). Blocking some non-spam e-mail and allowing some spam e-mail to go through are the major drawbacks of using filtering software. For a good overview of how filtering

automatically deleted or sent to a special folder in the recipient's mailbox. The first method results in the ISP automatically blocking all spam, while the second allows the recipient to choose whether to read or delete the spam.

Many consumer organizations also combat spam. The most vocal and active U.S. organizations include the Coalition Against Unsolicited Commercial Email ("CAUCE"),[31] SueSpammers.org,[32] and Junk Busters.[33] These organizations share knowledge about recent spam legislation and cases and information about how to combat spam personally and via legislative and lobbying activities.[34] In addition, one of these private organizations, Mail Abuse Prevention System ("MAPS"), produces the Realtime Blackhole List ("RBL")—a list of "hosts and networks which are known to be friendly, or at least neutral, to [spammers] either to originate or relay spam or to provide spam support services."[35] MAPS distributes the RBL to ISPs so that they can block e-mail coming into their networks from blacklisted networks. In order to produce the RBL, MAPS uses its own definition of spam. According to the RBL, acceptable e-mail solicitations must include a double-opt-in system.[36]

---

software works, see ALAN SCHWARTZ & SIMSON GARFINKEL, STOPPING SPAM 74-85 (1998).

31. http://www.cauce.org/ (last visited Feb. 14, 2000).

32. http://www.suespammers.org/ (last visited Feb. 14, 2000).

33. http://www.junkbusters.com/ (last visited Feb. 14, 2000).

34. Foreign anti-spam organizations include the European Coalition Against Unsolicited Commercial Email ("EuroCAUCE"), *at* http://www.euro.cauce.org/en/ (last visited Feb. 11, 2001), the Coalition Against Unsolicited Bulk Email, Australia ("CAUBE.au"), *at* http://www.caube.org.au/ (last visited Feb. 11, 2001), and CAUCE India, *at* http://www.india.cauce.org/ (last visited Feb. 11, 2001). The spam industry has recently started regulating itself. On September 14, 2000, fifteen companies, including DoubleClick, Inc., and Yesmail.com, announced their intent to form a coalition to design e-mail standards to limit unsolicited e-mail. Press Release, Responsible Electronic Communications Alliance ("RECA"), *E-mail Marketing Companies Announce Coalition to Promote Standards, Consumer Choice* (Sept. 2000), *at* http://www.responsibleemail.org/.

35. Paul Vixie & Nick Nicholas, *Realtime Blackhole List: Getting into the MAPS RBL*, *at* http://mail-abuse.org/rbl/candidacy.html (last revised Feb. 2, 2000).

36. The first opt-in occurs when a new subscriber asks to receive mailings by submitting her e-mail address to the would-be mailer. The second opt-in occurs when the subscriber later confirms or verifies her desire to receive mail. Thus, a double-opt-in system requires verification of new mailing-list subscriptions. *See* Mail Abuse Prevention System, LLC, *Basic Mailing List Management Guidelines for Preventing Abuse*, *at* http://mail-abuse.org/manage.html (last revised Nov. 7, 2000).

2. *Results of Spam Control by ISPs and Organizations*

Using an ISP's policies to control incoming spam imposes a large burden on spammers, which may outweigh the cost benefits of spamming entirely, causing the spammer to abandon his activities.[37] While this is the goal of many people,[38] it is important to examine why and how this burden comes about.

By definition, spammers send the same e-mail to many recipients, each of whom belongs to an ISP, of which there are thousands in the United States alone.[39] Thus, one piece of spam may arrive at many different ISPs. To comply with the use policy of each ISP, a spammer must obtain the policy of each ISP, learn the requirements it places on incoming e-mail, and modify the spam so that it complies with each ISP's policy. Since each ISP can have a different—and potentially conflicting—use policy, it may be very difficult for one e-mail to comply with every ISP's policy. For example, one ISP policy could require that the subject line of spam begin with "ADV:", while another policy could require that the subject begin with "advertisement:". One e-mail cannot comply with both of these requirements.

The problem of complying with many different use policies is generally referred to as the problem of conflicting obligations.[40] If ISP use poli-

---

37. *See* Kenneth D. Bassinger, Note, *Dormant Commerce Clause Limits on State Regulation of the Internet: The Transportation Analogy*, 32 GA. L. REV. 889, 912 (1998) ("With the recent flurry of [Internet rules] and the inconsistency among them, a rapidly changing regulatory structure could have serious chilling effects on the development of Internet commerce."); Dan L. Burk, *Federalism in Cyberspace*, 28 CONN. L. REV. 1095, 1132 (1996) ("If [online businesses] were subject to the regulation of the recipient jurisdiction, online commerce would face an almost insurmountable burden in attempting to predict what requirements might be imposed upon it."); Am. Libraries Ass'n v. Pataki, 969 F. Supp. 160, 181 (S.D.N.Y. 1997) ("Regulation by any single [entity] can only result in chaos, because at least some [entities] will likely enact [rules] subjecting Internet users to conflicting obligations. Without the limitations imposed by the Commerce Clause, these inconsistent regulatory schemes could paralyze the development of the Internet altogether.").

38. Note that some types of unsolicited e-mail may be socially desirable, such as those that inform recipients of recent events like crime waves or computer viruses. In addition, some people may argue that even unsolicited advertisements can be socially desirable.

39. In 1999, there were 5,775 ISPs in the United States. That number is expected to increase to 7,785 in 2000. Press Release, Cahners In-Stat Group, *National ISPs Stand to Gain Most in Growing U.S. Market* (Sept. 25, 2000), *at* http://www.instat.com/pr/2000/is0004sp_pr.htm.

40. The problem of conflicting obligations will be revisited in Part III.B.2.b, which discusses this problem with respect to state laws.

cies do in fact conflict, any sender might be unable to send one version of an e-mail message to recipients at two different ISPs while complying with both ISPs' use policies. Thus, conflicting obligations may silence mass e-mailers, whether commercial or not, creating a potentially unacceptable chilling effect on speech.

Turning to the MAPS system of spam control, while the RBL has successfully reduced the amount of spam received by its subscribers, it has been strongly criticized.[41] First, critics argue that single-opt-in systems are a valid way of obtaining permission from users to send them bulk e-mail.[42] Since MAPS requires a double-opt-in system, bulk e-mailers who obtain single-opt-in permission are nonetheless placed on the RBL.[43] This disagreement over the definition of "spam" is important, since the widespread use of the RBL results in MAPS' definition being applied to the entire Internet.

Critics also argue that MAPS' methods are overbroad:[44] If one user sends spam from an ISP, then all users of that ISP are placed on the

---

41. *See* Post, *supra* note 21. For MAPS' response to these criticisms, see Paul Vixie, *MAPS RBL Rationale*, *at* http://mail-abuse.org/rbl/rationale.html (last revised July 19, 2000).

42. "Members can join [Harris Interactive's online] panel only after registering at the company's or one of 26 other sites that recruit panel members. Individuals must elect to opt-in or opt-out. . . . [MAPS], at their sole discretion, have defined what constitutes 'unsolicited'. . . . The entire process is subjective and unevenly applied." Press Release, Harris Interactive, *Harris Interactive Files Suit Against AOL, Microsoft, Qwest and Other ISPs Over Restraint of Trade* (July 31, 2000), *at* http://www.harrisinteractive.com/news/index.asp?NewsID=127&HI_election=All. Harris Interactive, an Internet-based market research firm that was placed on the RBL, sued MAPS on July 31, 2000. *Id.* The suit was dropped on September 13, 2000. Press Release, Harris Interactive, *Harris Interactive Drops ISP Lawsuit* (September 13, 2000), *at* http://www.harrisinteractive.com/news/index.asp?NewsID=145&HI_election=All.

43. Yesmail.com, a permission-based e-mail marketing firm that was placed on the RBL, sued MAPS in July 2000. Oscar S. Cisneros, *Yesmail Fights Blacklist Threat*, WIRED NEWS (July 18, 2000), *at* http://www.wirednews.com/news/ebiz/0,1272,37621,00.html. A federal district court sustained a temporary injunction barring MAPS from adding Yesmail.com to the RBL. *Id.* Yesmail and MAPS have since come to an agreement whereby Yesmail will change its e-mail policies, and MAPS will not place Yesmail on the RBL. Press Release, Mail Abuse Prevention System, LLC, *yesmail.com and MAPS Reach Agreement Over Email Permission Standards* (Aug. 1, 2000), *at* http://mail-abuse.org/pressreleases/2000-08-01.html.

44. [W]hat often happens is that the actual point of origination of the offending email can't be found (email return addresses are easily faked or omitted entirely). That in no way deters RBL. . . . [T]hey are then free to "shoot the messenger", and you are "guilty by association". You are guilty because someone you don't know sent an email to someone else that you also don't know.

RBL.[45] Thus, the RBL frequently blocks people who are not spammers. Since the RBL is a completely private enterprise, there is little recourse to change this policy or root out these false positives and remedy the situation by removing the innocent parties from the RBL. Consequently, RBL usage has blocked many legitimate e-mail messages.

Finally, many ISPs use the RBL to filter their e-mail, but because MAPS is a private organization, the public has little (if any) input into how it runs, including who is placed on the RBL. Thus, if MAPS chose to, it could cause the ISPs (and all of their subscribers) to shun an entire group of Internet users by placing these users' e-mail addresses on the RBL. Moreover, MAPS could choose to censor these users based on, for example, their public expression of a viewpoint with which MAPS disagrees.[46] This scenario demonstrates the need for oversight and a public voice in spam regulation.

B. Legislative Responses to Spam

Legislation seems like a promising solution to control spam. The process is public, the system implementers would be accountable, and the rules would have a real effect because they have the force of law.[47] The United States and foreign countries[48] have enacted many laws to decrease spam in order to reduce its burden on ISPs and recipients. This section first describes the general categories of spam laws. It then examines some actual spam laws, focusing on those of Washington and California.

Internet Frontier, RBL—Power Without Accountability, *at* http://www.ifn.net/rblstory.htm (last visited Jan. 25, 2001).

45. Vixie & Nicholas, *supra* note 35.

46. This possibility has already occurred in the world of website filtering software. Declan McCullagh, *The CyberSitter Diaper Change*, TIME DIGITAL (Jan. 12, 1997), *at* http://www.time.com/time/digital/daily/0,2822,11595,00.html. CyberSitter blocks websites that criticize it, including an article in Time magazine. Greg Lindsay, *CyberSitter Decides to Take a Time Out*, TIME DIGITAL (Aug. 8, 1997), *at* http://www.time.com/time/digital/daily/0,2822,12392,00.html.

47. Legislation is not a panacea because spam is a nationwide, even worldwide, problem. Even if spam were outlawed in an entire country, it could still be sent into that country from elsewhere. Thus, outlawing spam in the United States may simply result in spam being sent via foreign ISPs that are not subject to U.S. laws.

48. For information on anti-spam activities in foreign countries, see http://www.spamlaws.com/eu.html (European Union) and http://www.spamlaws.com/world.html (other countries).

1. *Categories of Spam Laws*

Spam laws can be categorized based on how they address the spam problem.[49] E-mail messages contain many pieces of information that tell the recipient about the sender. These include the return address, which specifies who sent the e-mail, and the header, which specifies the route the e-mail traveled through the Internet to reach the recipient.[50] Most anti-spam laws regulate the information conveyed in these two identifiers.[51]

Laws that seek to regulate spam must first define unsolicited commercial e-mail. A North Carolina statute provides a common statutory definition of "unsolicited": "not addressed to a recipient with whom the initiator has an existing business or personal relationship and not sent at the request of, or with the express consent of, the recipient."[52] In addition, North Carolina defines "commercial electronic mail" as "messages sent and received electronically consisting of commercial advertising material, the principal purpose of which is to promote the for-profit sale or lease of goods or services to the recipient."[53]

Once a specific e-mail has been identified as spam, the law attempts to control it in some way. For example, some laws require senders to place the phrase "ADV:" in the subject line of spam e-mail.[54] Often, spam laws

---

49. Max P. Ochoa, Legislative Note, *Recent State Laws Regulating Unsolicited Electronic Mail*, 16 COMPUTER & HIGH TECH. L.J. 459, 461 (2000).

50. *Id.* at 462.

51. *Id.* Various other types of statutes also cut down on spam, for example by outlawing software that facilitates the sending of spam. *See, e.g.*, VA. CODE ANN. § 18.2-152.4(b) (Supp. 2000). This type of statute may be unconstitutional on First Amendment grounds because sometimes software is speech. *See, e.g.*, Junger v. Daley, 209 F.3d 481, 485 (6th Cir. 2000). Other states give courts long-arm jurisdiction over out-of-state spammers so that they can be prosecuted. *See, e.g.*, OKLA. STAT. tit. 15, § 776.3 (Supp. 2000). In addition, all states have passed laws that create safe harbors for ISPs. These laws shield ISPs from liability due to transmission of spam, *see, e.g.*, W. VA. CODE ANN. § 46a-6G-3(4) (Michie 1999), or attempts to prevent spam, *see, e.g.*, W. VA. CODE ANN. § 46a-6G-3(1)—(3) (Michie 1999). Lastly, state laws differ as to who may sue spammers. Possible plaintiffs include ISPs, recipients of spam, and state attorney generals. Ochoa, *supra* note 49, at 464. Violations of spam statutes may be either civil or criminal offenses, depending on the state. *Id.*

52. N.C. GEN. STAT. § 14-453(10) (1993).

53. *Id.* § 14-453(1b) (1999).

54. *See, e.g.*, CAL. BUS. & PROF. CODE § 17538.4(g) (West Supp. 2000), discussed *infra*; TENN. CODE ANN. § 47-18-2501(e) (Supp. 2000); COLO. REV. STAT. § 6-2.5-103(4) (Supp. 2000).

allow ISPs and recipients to sue spammers for damages if they fail to comply with state laws.[55]

Another type of anti-spam law, consumer protection statutes, requires that advertisers not mislead buyers with false information. Spammers may violate these statutes by deliberately providing false information to hide their identities, thereby avoiding complaints and lawsuits from recipients and ISPs. For instance, spammers may modify their messages to contain falsified ("spoofed") return addresses and header information. Thus, one way to make spammers accountable for their actions is to use or adapt existing consumer protection statutes to outlaw misleading information in spam.

As applied to spam, consumer protection statutes generally require that no misleading subject line be used and that the sender of the e-mail not alter, misrepresent, or obfuscate the return address or header information.[56] While they do not prevent spam, these laws (1) help recipients identify spam via relevant subject lines; (2) make e-mail messages more traceable via the correct header information; and (3) make spammers accountable for their actions via the correct return address. Such statutes may provide some real protection for consumers. For example, in one state court case, the state sued a spammer for sending bulk e-mail with false return addresses.[57] The court held the spammer liable under a state consumer fraud statute and granted an injunction against the spammer.[58]

2. *Actual State Spam Laws*

In July 1997, Nevada became the first state to enact an anti-spam law;[59] since then, sixteen other states have also passed spam laws.[60] Commentators have questioned the constitutionality of state spam laws,[61] citing issues such as the First Amendment[62] and the dormant Commerce

---

55. *See, e.g.*, CAL. BUS. & PROF. CODE § 17538.45 (Supp. 2000), discussed *infra*; 1999 Conn. Acts 160 (Reg. Sess.); IDAHO CODE § 48-603E(4) (Michie Supp. 2000).

56. *See, e.g.*, CAL. PENAL CODE § 502(c)(9) (West 1999); R.I. GEN. LAWS § 11-52-7 (2000); VA. CODE ANN. § 18.2-152.4(A)(7) (Supp. 2000).

57. People v. Lipsitz, 663 N.Y.S.2d 468 (Sup. Ct. 1997).

58. *Id.* at 477.

59. NEV. REV. STAT. ANN. §§ 41.705 (Michie 1999) (introduced Jan. 1997, enacted July 1997, effective July 1, 1998).

60. California, Colorado, Connecticut, Delaware, Idaho, Illinois, Iowa, Louisiana, Missouri, North Carolina, Oklahoma, Rhode Island, Tennessee, Virginia, Washington, and West Virginia. Scot M. Graydon, *Much Ado About Spam: Unsolicited Advertising, the Internet, and You*, 32 ST. MARY'S L. J. 77, 98 n.124 (2000).

61. *See* Burk, *supra* note 37, at 1096-97; Bassinger, *supra* note 37.

62. For an overview of the subject, see Marcus, *supra* note 23.

Clause.[63] Although a number of cases have addressed the problem of Internet content regulation and the dormant Commerce Clause,[64] only recently have any state spam laws been held unconstitutional under the dormant Commerce Clause. The next two sections discuss the Washington and California spam laws that were held to violate the dormant Commerce Clause.

a) Washington Anti-Spam Law

The Unsolicited Electronic Mail Act ("UEMA")[65] became operative on June 11, 1998, thereby making Washington the first state to effect public spam regulation.[66] The UEMA applies to e-mail sent from a computer in Washington or to an e-mail address that belongs to a Washington resident.[67] The Act explicitly prohibits spoofing[68] and also provides that spoofing violates Washington's consumer protection act.[69] ISPs and recipients can recover damages of $1,000 or $500 respectively, or actual damages (whichever is greater).[70] Lastly, the UEMA immunizes an ISP from liability for good faith blocking of the receipt or transmission through its servers of e-mail that violates the Act.[71]

---

63. Other problems with state spam statutes include obtaining personal jurisdiction over the spammer. *See generally* Blake, *supra* note 25.

64. *See* Am. Libraries Ass'n v. Pataki, 969 F. Supp. 160, 169 (S.D.N.Y. 1997) (temporarily restraining the enforcement of New York's Internet Decency Law ("IDL") on dormant Commerce Clause grounds); Am. Civil Liberties Union v. Johnson, 4 F. Supp. 2d 1029, 1029 (D.N.M. 1998); *aff'd*, 194 F.3d 1149 (10th Cir. 1999) (enjoining action under an Internet content-related statute on dormant Commerce Clause grounds). The *Pataki* opinion has been criticized. *See* Charles R. Topping, Student Article, *The Surf Is Up, But Who Owns the Beach?—Who Should Regulate Commerce On the Internet?*, 13 N.D. J.L. ETHICS & PUB. POL'Y 179, 206 (1999) (suggesting that the IDL can escape dormant Commerce Clause problems by restricting its application to conduct occurring only in New York); James E. Gaylord, Note, *State Regulatory Jurisdiction and the Internet: Letting the Dormant Commerce Clause Lie*, 52 VAND. L. REV. 1095, 1116-17 (1999) (suggesting that the extraterritoriality principle relied on in *Pataki* will soon no longer be valid).

65. WASH. REV. CODE ANN. § 19.190 (West 1999).

66. Ochoa, *supra* note 49, at 461 n.12.

67. WASH. REV. CODE ANN. § 19.190.020(1) (West 1999).

68. Specifically, it is illegal to send unsolicited commercial e-mail that "[u]ses a third party's internet domain name without permission of the third party, or otherwise misrepresents any information in identifying the point of origin or the transmission path" or "[c]ontains false or misleading information in the subject line." *Id.*

69. *Id.* § 19.190.030.

70. *Id.* § 19.190.040.

71. *Id.* § 19.190.050.

A Washington trial court recently held that the UEMA violates the dormant Commerce Clause.[72] In a brief opinion, the court held that the Act "violate[d] the Federal Interstate Commerce Clause of the United States Constitution [and was] unduly restrictive and burdensome."[73] The State Attorney General has appealed the decision.[74]

b) California Anti-Spam Laws

Three new spam laws took effect in California on January 1, 1999.[75] The Bowen Bill amended California's "junk fax" law[76] to require spam[77] to meet two requirements. First, the subject line of a spam message must begin with the characters "ADV:".[78] Second, the body of a spam message must contain a toll-free phone number or e-mail address that the recipient can use to notify the sender not to send her any more spam.[79] Violations

---

72. Order on Civil Motion Granting Defendant's Summary Judgment, Washington v. Heckel, No. 98-2-25480-7SEA (Wash. Super. Mar. 10, 2000).

73. *Id.*

74. News Release, Attorney General of Washington, *AG's Office Files Notice of Appeal in Anti-Spam E-mail Lawsuit* (Apr. 6, 2000), *at* http://www.wa.gov/ago/releases/rel_spam_040600.html.

75. David Kramer, *California's New Anti-Spam Laws*, Wilson Sonsini Goodrich & Rosati Library, *at* http://www.wsgr.com/library/libfileshtm.asp?file=spam.htm (last visited Feb. 1, 2001).

76. CAL. BUS. & PROF. CODE § 17538.4 (West Supp. 2000).

77. The statute contains a slightly different definition of "unsolicited commercial e-mail" than the definition used in Business and Professions Code § 17538.45. Namely, UCE is defined as

> any e-mailed document or documents consisting of advertising material for the lease, sale, rental, gift offer, or other disposition of any realty, goods, services, or extension of credit that . . . are addressed to a recipient with whom the initiator does not have an existing business or personal relationship [and] are not sent at the request of, or with the express consent of, the recipient.

Id. § 17538.4(e).

78. "In the case of email that consists of unsolicited advertising material for the lease, sale, rental, gift offer, or other disposition of any realty, goods, services, or extension of credit, the subject line of each and every message shall include 'ADV:' as the first four characters." *Id.* § 17538.4(g).

> If these messages contain information that consists of unsolicited advertising material for the lease, sale, rental, gift offer, or other disposition of any realty, goods, services, or extension of credit, that may only be viewed, purchased, rented, leased, or held in possession by an individual 18 years of age and older, the subject line of each and every message shall include "ADV:ADLT" as the first eight characters.

Id. § 17538.4(g). Approximately twenty-five percent of spam has adult content. Gartner Group, *supra* note 13, at 5.

79. CAL. BUS. & PROF. CODE § 17538.4(a)(2) (West Supp. 2000).

constitute a misdemeanor,[80] but the statute does not give ISPs or spam recipients a private cause of action against spammers.

On June 2, 2000, a San Francisco trial court held that the Bowen Bill violates the dormant Commerce Clause.[81] In a short opinion, the judge found that the statute "unconstitutionally subject[ed] interstate use of the Internet to inconsistent regulations, therefore violating the dormant Commerce Clause . . . ."[82] The next section discusses the constitutionality of the Bowen Bill.

Courts have not yet considered California's other two spam laws. Section 502 of the Penal Code,[83] originally added by California's Comprehensive Computer Data Access and Fraud Act, provides criminal penalties[84] for spoofing[85] if it causes damage to one or more computers.[86] Victims may also bring a civil suit against an offender convicted under Section 502.[87] In this manner, parties whose domain names have been spoofed by spammers can be compensated.

Section 17538.45 of the Business & Professions Code,[88] the Miller Bill, gives an ISP the right to sue people who use its network to send spam.[89] The Miller Bill allows an e-mail service provider[90] to sue someone who sends unsolicited commercial e-mail[91] either from the ISP or to an

---

80. *Id.* § 17534.

81. Order Sustaining Defendants' Demurrer Without Leave to Amend, Ferguson v. Friendfinder, Inc., No. 307309 (Cal. Super. June 2, 2000).

82. *Id.*

83. CAL. PENAL CODE § 502 (West 1999).

84. *Id.* § 502(d).

85. Specifically, the statute prohibits the unauthorized use of another party's domain name in connection with the sending of electronic mail messages. *Id.* § 502(c)(9).

86. *Id.*

87. *Id.* § 502(e)(1).

88. CAL. BUS. & PROF. CODE § 17538.45 (West Supp. 2000). For criticism of the Bowen Bill and the Miller Bill, see Whang, *supra* note 8.

89. For constitutional analysis of this statute, see David T. Bartels, *Review of Selected 1998 California Legislation: Business Associations and Professions: Canning Spam: California Bans Unsolicited Commercial E-mail*, 30 MCGEORGE L. REV. 420, 430 (1999) (suggesting that the statute does not violate the dormant Commerce Clause).

90. The statute defines "electronic mail service provider" as "any business or organization qualified to do business in California that provides registered users the ability to send or receive electronic mail through equipment located in this state and that is an intermediary in sending or receiving electronic mail." CAL. BUS. & PROF. CODE § 17538.45(a)(3) (West Supp. 2000).

91. The statue defines "electronic mail advertisement" (i.e., commercial e-mail) as any "electronic mail message, the principal purpose of which is to promote, directly or indirectly, the sale or other distribution of goods or services to the recipient." *Id.* § 17538.45(a)(1). "Unsolicited" is defined as "addressed to a recipient with whom the

ISP subscriber. Thus, the ISP can sue both registered users of the ISP and outsiders.[92] If successful,[93] the ISP can recover damages for network clogs or crashes.[94]

III. THE DORMANT COMMERCE CLAUSE AND ITS EFFECT ON THE CONSTITUTIONALITY OF THE BOWEN BILL

Washington and California courts have found that certain state spam statutes violate the dormant Commerce Clause. Unfortunately, neither opinion revealed the court's reasoning. This section fills that gap by outlining the major dormant Commerce Clause doctrines and tests and then applying them to the Bowen Bill, the California statute held unconstitutional in *Ferguson v. Friendfinder.*

The Supreme Court has held that the Commerce Clause[95] contains a negative implication, the dormant Commerce Clause, which prohibits states from regulating interstate commerce.[96] Because Congress has the

---

initiator does not have an existing relationship" and "is not sent at the request of or with the express consent of the recipient." *Id.* § 17538.45(a)(2).

92. This possibility was discussed *supra* Part II.A.1.

93. To succeed, the ISP must prove that (1) its mail servers are physically located in California; (2) the defendant transmitted spam (either from the ISP or to an ISP subscriber) by using a California mail server; (3) the defendant's use of the California mail servers was in violation of the ISP's use policy; and (4) the defendant had advance notice that his spam transmission would use the ISP's California mail servers in violation of the ISP's policy. CAL. BUS. & PROF. CODE § 17538.45 (West Supp. 2000).

94. Specifically, the ISP can recover $50 per spam e-mail sent (up to $25,000 per day) or actual damages, whichever is greater. *Id.* § 17538.45(f)(1).

95. The Commerce Clause states that "Congress shall have Power . . . [t]o regulate Commerce . . . among the several States." U.S. CONST. art. I § 8 cl. 3.

96. "[T]he negative or dormant implication of the Commerce Clause prohibits state taxation or regulation that discriminates against or unduly burdens interstate commerce and thereby impedes free private trade in the national marketplace." General Motors Corp. v. Tracy, 519 U.S. 278, 287 (1997) (internal quotation marks omitted). *See generally* Martin H. Redish & Shane V. Nugent, *The Dormant Commerce Clause and the Constitutional Balance of Federalism*, 1987 DUKE L.J. 569 (1987).

The dormant Commerce Clause first arose in dicta in *Gibbons v. Odgen*, when Chief Justice Marshall noted that "when a State proceeds to regulate commerce . . . among the several States, it is exercising the very power that is granted to Congress, and is doing the very thing which Congress is authorized to do." 22 U.S. (9 Wheat.) 1, 199-200 (1824). However, the Court did not officially acknowledge the negative aspect of the Commerce Clause until *Willson v. Black Bird Creek Marsh Co.*, 27 U.S. (2 Pet.) 245 (1829). In *Willson*, Marshall noted that state legislation might fail if it were "repugnant to the power to regulate commerce in its dormant state." *Id.* at 252. Such legislation did fail in the *Passenger Cases*. Smith v. Turner; Norris v. City of Boston, 48 U.S. (7 How.) 283 (1849). In those cases, the Court held (5-4) that statutes imposing bond requirements and

power to regulate interstate commerce, states cannot pass laws that unduly interfere with such regulation.[97] Over the years, the Court has struck down many state laws that offend the dormant Commerce Clause by affecting interstate commerce.[98] Note that the dormant Commerce Clause does not absolutely bar state regulation of interstate commerce. As part of its Commerce Clause powers, Congress can always explicitly authorize a state to act in a particular area otherwise precluded by the dormant Commerce Clause.[99] In such cases, Congress allows the states to regulate certain activities, rather than imposing its own law.

A. The Bowen Bill Falls within the Scope of the Dormant Commerce Clause

In its modern form, the dormant Commerce Clause prohibits states from discriminating against or unduly burdening interstate commerce. As a preliminary matter, the dormant Commerce Clause applies only to statutes that regulate activities that are within Congress' commerce power. The commerce power encompasses both interstate commerce itself, such as items shipped across state lines, and activities that affect interstate commerce, like shipping and transportation mechanisms (also known as "instruments of interstate commerce").

The Bowen Bill can violate the dormant Commerce Clause only if the area it regulates, spam, falls within the broad sweep of Congress's Commerce Clause power. There can be little doubt that sending spam qualifies as interstate commerce or an instrument of interstate commerce. Many courts have held that Internet communication, specifically e-mailing im-

---

taxes on immigrants arriving at state ports were unconstitutional. However, the dormant Commerce Clause's role in the ruling is unclear. Only three of the eight separate opinions clearly relied on the dormant Commerce Clause for their results.

Some commentators doubt the legitimacy of the dormant Commerce Clause. *See, e.g.*, Julian N. Eule, *Laying the Dormant Commerce Clause to Rest*, 91 YALE L.J. 425, 446-55 (1982); Redish & Nugent, *supra*, at 575-76; Richard D. Friedman, *Putting the Dormancy Doctrine Out of Its Misery*, 12 CARDOZO L. REV. 1745 (1991); Amy M. Petragnani, *The Dormant Commerce Clause: On Its Last Leg*, 57 ALB. L. REV. 1215, 1243 (1994).

97. *See* Cooley v. Board of Wardens, 53 U.S. (12 How.) 299, 317-19 (1851); *Willson*, 27 U.S. (2 Pet.) at 245; *Gibbons*, 22 U.S. (9 Wheat.) at 5-6.

98. *See, e.g.*, Dean Milk Co. v. City of Madison, 340 U.S. 349 (1951) (produce regulations); S. Pac. Co. v. Arizona *ex rel.* Sullivan, 325 U.S. 761 (1945) (railroad regulations).

99. LAURENCE H. TRIBE, AMERICAN CONSTITUTIONAL LAW § 6-33 (3d ed. 2000); Glenn Harlan Reynolds, *Virtual Reality and "Virtual Welters": A Note on the Commerce Clause Implications of Regulating Cyberporn*, 82 VA. L. REV. 535, 541 n.20 (1996).

ages through the Internet, qualifies as interstate commerce.[100] Assuming that spam is commercial in nature, spam that crosses state lines is interstate commerce. Moreover, even if both sender and recipient are in the same state, the spam may still cross state lines before it reaches its destination and thus qualify as interstate commerce.[101]

In addition, many courts and commentators have argued that the Internet itself is an instrument of interstate commerce.[102] If so, then Congress may regulate the entire Internet, including spam.[103] These arguments rely on the similarities between the Internet and traditional instruments of interstate commerce, such as highways and railroads. Namely, both mechanisms transport commercial items across state lines.[104]

In *American Libraries Ass'n v. Pataki*,[105] the leading case in this area, a federal district court struck down on dormant Commerce Clause grounds a state law that prohibited sexual contact over the Internet between adults and minors.[106] In reaching this conclusion, the court reasoned that the "Internet is analogous to a highway or railroad. . . . [T]he similarity between the Internet and more traditional instruments of interstate commerce leads to analysis under the Commerce Clause."[107] Other cases where an Internet content regulation failed dormant Commerce Clause scrutiny include *ACLU v. Johnson*[108] and *Cyberspace Communications v. Engler*.[109]

---

100. United States v. Schooley, 1997 WL 517486 at *1 (A.F. Ct. Crim. App., Aug. 11, 1997); United States v. Carroll, 105 F.3d 740, 742 (1st Cir. 1997); United States v. Thomas, 74 F.3d 701, 706-09 (6th Cir. 1996).

101. Am. Libraries Ass'n v. Pataki, 969 F. Supp. 160, 171 (S.D.N.Y. 1997). In fact, the judge in *Pataki* stated that "no [intrastate] communications exist." *Id.*

102. *See id.* at 173; H. Joseph Hameline & William Miles, *The Dormant Commerce Clause Meets the Internet*, BOSTON B.J., Oct. 1997, at 21-22; Blake, *supra* note 25, at 141-42; Burk, *supra* note 37, at 1125-26. *See generally* Bassinger, *supra* note 37.

103. Some critics worry that declaring that the Internet is an instrument of interstate commerce will result in the states' inability to regulate the Internet at all. *See, e.g.*, Hameline & Miles, *supra* note 102, at 22.

104. The Internet is a "conduit for transporting digitized information goods such as software, data, music, graphics, and videos . . . ." Burk, *supra* note 37, at 1125-26.

105. 969 F. Supp. 160 (S.D.N.Y. 1997).

106. *Id.* at 160. The court found that the statute had extraterritorial effects and placed a burden on interstate commerce that exceeded its benefit to its local interest. *Id.* at 169.

107. *Id.* at 161.

108. 4 F. Supp. 2d 1029 (D.N.M. 1998); *aff'd*, 194 F.3d 1149 (10th Cir. 1999) (upholding an injunction against enforcing a New Mexico law that sought to restrict children from Internet pornography).

109. 55 F. Supp. 2d 737 (E.D. Mich. 1999) (stopping enforcement of a Michigan law that sought to prohibit using computers or the Internet to disseminate pornography to minors); *aff'd*, 2000 U.S. App. LEXIS 29359 (6th Cir. November 15, 2000).

Thus, spam regulation comes within the commerce power either because spam is interstate commerce or because the Internet is an instrument of interstate commerce. Since spam regulation is within the commerce power, it is subject to dormant Commerce Clause limits. The rest of the analysis addresses whether the Bowen Bill in fact violates the dormant Commerce Clause.

B. The Bowen Bill Violates the Dormant Commerce Clause by Imposing Inconsistent Obligations on Interstate Spam

The Supreme Court clearly articulated the test for whether a state statute violates the dormant Commerce Clause in *Oregon Waste Systems v. Department of Environmental Quality*.[110] In *Oregon Waste Systems*, the Court analyzed an Oregon statute that imposed a surcharge for in-state disposal of solid waste generated out-of-state. "The first step in analyzing any law subject to judicial scrutiny under the negative [dormant] Commerce Clause is to determine whether it regulates evenhandedly with only incidental effect on interstate commerce, or discriminates against interstate commerce."[111] Since the surcharge depended on whether the waste was generated out-of-state,[112] the Court held that the statute was facially discriminatory and thus violated the dormant Commerce Clause.[113] Under *Oregon Waste Systems*, a court first determines whether the spam statute discriminates against interstate commerce. If it regulates evenhandedly, then the court analyzes the law's effect on interstate commerce. If it excessively burdens interstate commerce, then it may violate the dormant Commerce Clause despite its evenhandedness.

1. Discriminating Against Interstate Commerce and the Extraterritoriality Doctrine

In the dormant Commerce Clause context, "discrimination" means "differential treatment of in-state and out-of-state economic interests that benefits the former and burdens the latter."[114] State statutes that facially discriminate against interstate commerce trigger strict scrutiny and are

110. 511 U.S. 93 (1994).
111. *Id.* at 99.
112. *Id.*
113. *Id.* at 108.
114. *Id.* at 99.

usually invalid.[115] The statute will be held invalid unless the state can show that it has no other way to advance a legitimate local interest.[116]

In the realm of spam laws, differential treatment might involve only prohibiting spam that originated *outside* the recipient's state. The Bowen Bill states that "[n]o person or entity conducting business in this state"[117] may send spam to "a California resident via an electronic mail service provider's service or equipment located in this state."[118] Since the Bowen Bill applies equally to spam that originates either outside or inside of California,[119] it does not feature differential treatment.[120]

A state also directly discriminates against interstate commerce by attempting to project its law into other states. In *Edgar v. MITE Corp.*,[121] the Supreme Court considered an Illinois statute that regulated tender offers for certain companies.[122] The statute applied to any company of which Illinois residents owned ten percent of the stock, even if the company was not located or incorporated in Illinois.[123] The Court held that the statute violated the dormant Commerce Clause, a plurality holding that a regulation having the "practical effect" of regulating transactions that take place extraterritorially (i.e., across state lines) exceeds the "inherent limits of the State's power," regardless of the legislators' intentions.[124] The Court defined the "extraterritoriality doctrine"[125] as follows: "The Commerce Clause . . . precludes the application of a state statute to commerce that

115. Maine v. Taylor, 477 U.S. 131 (1986) (outlining the discriminatory effect test).

116. For a law that was held valid despite its being found discriminatory, see *id.* (upholding Maine's ban on the import of baitfish because Maine had no other way to prevent the spread of parasites and the adulteration of its native fish species).

117. CAL. BUS. & PROF. CODE § 17538.4(a) (West Supp. 2000).

118. *Id.* § 17538.4(d).

119. The Bowen Bill requires only that the sender conduct business in California and that the spam started from a server in California. These requirements might be needed for personal jurisdiction reasons. If the requirements favor anyone, they are more likely to favor out-of-state spammers than in-state spammers.

120. Note that it may cost more for an out-of-state spammer to operate a toll-free phone number for spam recipients to use, as is an option in the Bowen Bill. CAL. BUS. & PROF. CODE § 17538.4(a)(2) (West Supp. 2000). However, the spammer can avoid this cost by allowing the recipient to complain via e-mail. Thus, the Bowen Bill might discriminate against out-of-state spammers, but in an insignificant way.

121. 457 U.S. 624 (1982).

122. *Id.* at 626-27.

123. *Id.* at 627.

124. *Id.* at 642-43.

125. Some commentators have suggested that the holdings in the extraterritoriality cases were based on something other than dormant Commerce Clause concerns. *See* Gaylord, *supra* note 64 (requirement of a nexus between state interests and regulated enterprises).

takes place wholly outside of the State's borders, whether or not the commerce has effects within the state."[126]

In *Healy v. Beer Institute*,[127] the Court used the extraterritoriality doctrine to hold that a Connecticut law facially violated the dormant Commerce Clause.[128] The law required out-of-state beer shippers to affirm that their prices were no higher than the prices charged in the bordering states at the time of the affirmation.[129] The Court reiterated the extraterritorial doctrine of *Edgar*[130] and added that the practical effect of a statute includes both

> the consequences of the statute itself [and] how the challenged statute may interact with the legitimate regulatory regimes of other States[, including] what effect would arise if not one, but many or every, State adopted similar . . . inconsistent legislation arising from the projection of one state regulatory regime into the jurisdiction of another State.[131]

Lastly, the intent of the legislature does not affect the validity of the statute.[132]

The Bowen Bill appears to comply with the extraterritoriality doctrine because it applies only to spam originating from servers located in California. However, *Healy* requires that courts also consider the practical effects of the statute, including what would happen if many states adopted similar, yet inconsistent, legislation.[133] The possibility of conflicting obligations exists because the Bowen Bill can apply to e-mail which travels through other states, even if the message originated in California and was sent to a California resident. This may occur in either of two ways. First, the e-mail may simply be routed through other states on its way from the

---

126. *Edgar*, 457 U.S. at 642-43.
127. 491 U.S. 324 (1989).
128. *Id.* at 340.
129. *Id.* at 335.
130. *Id.* at 336 (quoting *Edgar*, 457 U.S. at 642-43).
131. *Id.* at 337.
132. [A] statute that directly controls commerce occurring wholly outside the boundaries of a State exceeds the inherent limits of that State's authority, and is invalid regardless of whether the statute's extraterritorial reach was intended by the legislature. The critical inquiry is whether the practical effect of the regulation is to control conduct beyond the boundaries of the State.

Id. at 336.

133. This consideration is just another form of the "conflicting obligations problem" discussed earlier. *See supra* Part II.A.2.

sender to the recipient.[134] Second, the California resident could access the e-mail remotely from another state. Either way, the requirements of the Bowen Bill would still be met. In these situations, therefore, the e-mail could be subject to both California's law and the potentially inconsistent law of the state through which the e-mail traveled. Thus, the Bowen Bill may run afoul of the extraterritoriality doctrine.[135]

2. Excessively Burdening Interstate Commerce

Even if a law regulates evenhandedly and does not directly discriminate, it may still violate the dormant Commerce Clause if it places an excessive burden on interstate commerce.[136] In order to determine whether a state law excessively burdens interstate commerce, courts balance the local benefits conferred by the law against the burdens imposed on interstate commerce.[137] In *Pike v. Bruce Church, Inc.*,[138] the Court considered an Arizona statute that prohibited interstate shipment of cantaloupes not packed in regular compact arrangements in closed standard containers.[139] The Court held that the statute violated the dormant Commerce Clause, stating that even if a law "regulates evenhandedly to effectuate a legitimate local public interest," it will still be invalidated if it imposes a burden on interstate commerce which is "clearly excessive in relation to the putative local benefits."[140] In general, the balancing test weighs local needs against national needs. In the process, the court determines whether the area sought to be regulated should be regulated on a local or national level.[141] The Court has held that states may regulate those interests that are so local in nature as to demand diverse regulation, while Congress has exclusive domain over those aspects of interstate commerce that are so national in character as to demand uniform treatment.[142]

---

134. *See supra* note 101 and accompanying text.

135. The Bowen Bill might pass this test if amended so that it applies only to spam that never leaves the state of California. However, due to the indeterminacy involved in routing e-mail, two e-mail messages that travel between the same sender and recipient could travel through different states or stay within California. Thus, spam sent on one day may be legal under the amended Bill (because it traveled outside of California), while spam sent on another day may be illegal (because it stayed within California and therefore is subject to the amended Bowen Bill).

136. In this situation, the law could be seen as "indirectly" discriminating against interstate commerce. Kassel v. Consolidated Freightways Corp., 450 U.S. 662 (1981).

137. Pike v. Bruce Church, Inc., 397 U.S. 137, 142 (1970).

138. 397 U.S. 137 (1970).

139. *Id.* at 138.

140. *Id.* at 142.

141. *See infra* Part III.B.2.b.

142. Cooley v. Bd. of Wardens, 53 U.S. (12 How.) 299, 319 (1851).

a) Local Benefits

Many factors are considered on each side of the scale in the *Pike* balancing test. First, the court examines the legitimacy of the state's interest.[143] If the area benefited is an area of traditional local concern (such as a police power), then it is more likely that the law will be held valid.[144] Thus, regulations designed to protect public health or safety probably will not be overturned unless their justifications are "illusory."[145]

With respect to the Bowen Bill, the state interest is mainly economic: California wants to protect its citizens and businesses from the monetary costs associated with spam.[146] In addition, California wants to decrease the inconveniences of receiving spam. This factor would probably weigh in favor of the statute's validity.

Next, the court considers the effectiveness of the statute. If the law is unlikely to bring about the desired beneficial effect (e.g., because of the difficulty of enforcement), then the benefit factor will be small and will probably not outweigh the burden on interstate commerce.[147] Also, the law is more likely be declared unconstitutional if a reasonable alternative would cause "less of an impact" on interstate commerce.[148]

In this case, the Bowen Bill may be ineffective due to difficulties in enforcement. If the spammer spoofs information in the e-mail, it may be difficult for the state to find the spammer in order to prosecute him. On the other hand, it is unlikely that better alternatives exist, such as statutes that would regulate spam while placing less of a burden on interstate commerce. Thus, overall, the local benefit side of the scale is not tipped very far (if at all) in favor of finding the Bowen Bill to be constitutional.

b) Burden on Interstate Commerce

After determining the local benefit at stake, the court assesses the burden on interstate commerce, especially the possibility of inconsistent obligations.[149] This situation arises most often when the state seeks to address

143. *Pike*, 397 U.S. at 142.

144. *See, e.g.*, Kassel v. Consolidated Freightways Corp., 450 U.S. 662, 670 (1981).

145. *Id.*

146. Note that consumer protection against fraud is a traditional state police power. Thus, the scale may tip towards approving consumer protection laws that regulate spam by prohibiting spoofing. In *Lipsitz*, for example, a law prohibiting spoofing survived because it only "tangentially" burdened interstate commerce. People v. Lipsitz, 663 N.Y.S.2d 468, 475 (Sup. Ct. 1997).

147. Am. Libraries Ass'n v. Pataki, 969 F. Supp. 160, 178 (S.D.N.Y. 1997).

148. *Pike*, 397 U.S. at 142.

149. *See supra* Part II.A.2.

a national problem, because state regulation of national interests may impose inconsistent obligations on interstate actors. Therefore, national interests must be regulated in a uniform way, which usually can be done only at the federal level. Courts have "long held that state regulation of those aspects of commerce that by their unique nature demand cohesive national treatment is offensive to the Commerce Clause."[150] This factor has been determinative in cases involving transportation, communications, and taxes,[151] for all are areas involving national interests.

In order to determine when an aspect of interstate commerce demands uniform treatment, courts consider the hypothetical effect of every state enacting conflicting laws concerning the subject at issue.[152] If such regulations would excessively burden interstate commerce, then uniform treatment is required and the state law is struck down.

State regulation of instruments of interstate commerce usually places a large burden on interstate commerce, because instruments of interstate commerce are national in scope and are therefore very vulnerable to inconsistent state laws. Thus, if the Internet is an instrument of interstate commerce, then the burdens that state Internet regulation place on interstate commerce will likely outweigh any local benefits of the regulation. For example, in *Pataki*, the court stated that "[h]aphazard and uncoordinated state regulation can only frustrate the growth of cyberspace."[153] The court also found that the Internet "requires a cohesive national scheme of regulation so that users are reasonably able to determine their obligations."[154] Thus, the court concluded that the Internet is "susceptible to regulation only on a national level."[155] This line of reasoning suggests that virtually all state laws regulating the Internet would violate the dormant Commerce Clause.[156]

---

150. *Am. Libraries Ass'n*, 969 F. Supp. at 169.

151. *See, e.g.*, S. Pac. Co. v. Arizona *ex rel.* Sullivan, 325 U.S. 761 (1945) (holding that an Arizona statute that limited the length of trains within the state was unconstitutional). The court held that there are parts of "national commerce which, because of the need of national uniformity, demand that their regulation, if any, be prescribed by a single authority." *Id.* at 767.

152. Wabash, St. Louis & Pac. Ry. Co. v. Illinois, 118 U.S. 557, 575-76 (1886).

153. *Am. Libraries Ass'n*, 969 F. Supp. at 183.

154. *Id.* at 182.

155. *Id.* at 181.

156. *Id.* at 182; *see supra* note 103; Hameline & Miles, *supra* note 102, at 21; Burk, *supra* note 37, at 1123-34; Reynolds, *supra* note 99, at 537-42; Blake, *supra* note 25, at 141.

As discussed above,[157] the Bowen Bill can apply to spam that travels through states other than California. Therefore, one piece of e-mail likely can be subject to inconsistent laws. Thus, the burden that the Bowen Bill places on interstate commerce probably outweighs its local benefits, and the Bill therefore violates the dormant Commerce Clause.

IV. CONCLUSION

The costs that spam imposes on ISPs and recipients increase daily. Private responses to the problem, such as ISP use policies and the MAPS RBL, are inadequate. Legislation is a better choice, since the process is public and legislators are politically accountable. However, state spam legislation is subject to dormant Commerce Clause limits, and some statutes, such as the Bowen Bill, have been held to violate the dormant Commerce Clause. Because spam is sent interstate via the Internet, it must be regulated in a uniform way at the national level.[158]

So far, approximately seventeen federal spam bills have been introduced into Congress,[159] all of which have failed to become law.[160] Currently, only one federal spam bill is pending, the Unsolicited Commercial Electronic Mail Act of 2001 ("UCEMA").[161] UCEMA aims "[t]o protect individuals, families, and Internet service providers from unsolicited and unwanted electronic mail."[162] It is a reintroduction of the Unsolicited

157. *See supra* note 134 and accompanying text.

158. *See* Bassinger, *supra* note 37, at 926; Derek D. Simmons, Comment, *No Seconds on Spam: A Legislative Prescription to Harness Unsolicited Commercial E-mail*, 3 J. SMALL & EMERGING BUS. L. 389, 409 (1999); Topping, *supra* note 64, at 237; Michael W. Carroll, *Garbage In: Emerging Media and Regulation of Unsolicited Commercial Solicitations*, 11 BERKELEY TECH. L.J. 233, 276 (1996); *see also* Gary S. Moorefield, Note, *SPAM—It's not Just for Breakfast Anymore: Federal Legislation and the Fight to Free the Internet From Unsolicited Commercial E-Mail*, 5 B.U. J. SCI. & TECH. L. 10 para. 35 (1999) (proposing a new federal law).

159. *See* Spam Laws, *at* http://www.spamlaws.com/federal/index.html (last visited Jan. 25, 2001) (current bills); Pending Federal Bills, *at* http://www.jmls.edu/cyber/statutes/email/fedtable.html (July 17, 1998) (past bills); *see also* Ochoa, *supra* note 49, at 459 n.4 ("Eight bills were introduced in the 105th Congress, none of which became law.").

160. *Id.*

161. Unsolicited Commercial Electronic Mail Act of 2001, H.R. 95, 107th Cong. (2001).

162. *Id.*

Commercial Electronic Mail Act of 2000,[163] which was passed by the House but died in the Senate.[164]

UCEMA contains many provisions common to state spam laws. First, it requires that spam be labeled as such and include opt-out instructions.[165] UCEMA also prohibits spoofing.[166] Lastly, UCEMA would give ISP use policies the force of law.[167] Specifically, if an ISP's use policy is clearly posted on a web site at the domain name included in the recipient's e-mail address, or is made available by a standard method approved by the Federal Trade Commission, then it would be illegal to use the ISP's facilities in violation of the ISP's use policy.

UCEMA has been referred to House Committees. Thus, Congress is aware of the spam problem and is trying to provide a solution. It remains to be seen whether a federal spam regulation will ever become law.

---

163. Unsolicited Commercial Electronic Mail Act of 2000, H.R. 3113, 106th Cong. (1999).

164. Patrick Ross, *Technology Bills Fall Short in Congress*, CNET NEWS.COM, Oct. 20, 2000, *at* http://news.cnet.com/news/0-1004-200-3244298.html.

165. H.R. 95 § 5(a)(3). This is very similar to section 17538.4 of California's Business and Professions Code.

166. H.R. 95 § 4. This is very similar to section 17538.45 of California's Business and Professions Code.

167. H.R. 95 § 5(b).