Sabra-Anne Kelin
L&T Writing Seminar
Fall 2000

State Spam Laws and the Dormant Commerce Clause

I. Introduction

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 email. E sends emails to all of C's employees at their business email addresses. The email introduces some of C's employment practices and asks the employees to share their experiences. C sues E for sending unsolicited emails to its employees. The cause of action is for trespass to chattels, the chattels being C's network of email 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 Sacramento judge granted Intel a permanent injunction against Hamidi and his nonprofit organization Former And Current Employees of Intel (FACE Intel).[3] The injunction barred Hamidi and FACE Intel from sending unsolicited email to addresses on Intel's computer systems.[4] Hamidi appealed the order on July 2, 1999.[5]

The Intel/Hamidi controversy is just one of many problems created by the increased use of (and sensitivity to) unsolicited email.[6] The private sector has tried to control unsolicited email, but so far the proposed solutions are unacceptable. As for the public sector, state anti-spam legislation might be a viable alternative. [7] However, in the past year, two state laws regulating unsolicited email have been held unconstitutional

---

[1] Intel v. Hamidi, 15 IER Cases (BNA) 464, 1999 WL 450944, (Cal. (App. Dep't?) Super. Ct. Apr. 28, 1999) – **NOT ALLOWED TO CITE**.
[2] *Intel*, Motion for Summary Judgment Tentative Ruling, Apr. 28, 1999, available at http://cyber.law.harvard.edu/msvh/hamidi/tentativesjruling.html.
[3] *Intel*, Order for Entry of Final Judgment, June 16, 1999, available at http://cyber.law.harvard.edu/msvh/hamidi/finalorder.html.
[4] *Id*.
[5] *Intel*, Notice of Appeal, July 2, 1999, available at http://eon.law.harvard.edu/openlaw/intelvhamidi/appealnotice.html. For more information on the Intel v. Hamidi case, visit FACE Intel (http://www.faceintel.com/) and Harvard Law School's The Berkman Center for Internet & Society – Intel v. Hamidi (http://eon.law.harvard.edu/openlaw/intelvhamidi/).
[6] *See infra*.
[7] *See infra* Part III.

based on violation of the Dormant Commerce Clause.[8] This casenote surveys the problem of unsolicited email and examines its possible solutions. Due to the constitutionality issues surrounding state legislation, this casenote recommends the passage of federal legislation to address the problem of unsolicited email.

II. Email and the Rise of Spam

Approximately 116.5 million Americans have used the Internet.[9] Although the Internet comprises many telecommunications technologies (such as the World Wide Web, telnet, and Internet Relay Chat), the most widely used technology is electronic mail ("email").[10] As of July 1999, approximately five billion emails were sent worldwide every day, while about 1.4 trillion were sent annually.[11] Those numbers are expected to increase to 14.9 billion and four trillion, respectively, by 2002.[12]

Email is similar to conventional (paper-based) mail. They can both be used to send either a personalized message to one person (such as a birthday greeting) or an impersonal message to many people at the same time (such as an advertisement). Sending "bulk mail" (impersonal messages with many recipients) is an easy way to reach a large audience. Bulk mail is frequently commercial in nature, consisting of advertisements or solicitations for charitable donations. Since bulk mail is often unwanted by its recipients,[13] it is sometimes referred to as "junk mail." Bulk emails are commonly

---

[8] *See infra* Part III.B.3-4.
[9] U.S. DEP'T OF COMMERCE, FALLING THROUGH THE NET: TOWARD DIGITAL INCLUSION 33 (2000), http://search.ntia.doc.gov/pdf/fttn00.pdf.
[10] *Id*. at 47. About 80%of Internet users have used electronic mail. *Id*.
[11] Talk given by Michael Serbinis (Critical Path) at Spam Summit 2000. http://www.spamsummit.com/presentations/serbinis/tsld006.html
[12] *Id*.
[13] A survey of over 1,000 Internet users reported that 43% of users hate bulk email, and 25% consider it bothersome; 68.5% of respondents reported that junk email is not useful at all. Barry D. Bowen,

referred to as "unsolicited bulk email" (UBE), "unsolicited commercial email" (UCE), junk email, or spam.[14] People who send spam are called "spammers."

Recently, advertisers have begun to take advantage of the low cost of sending bulk email.[15] A 1998 study estimated that approximately thirteen billion pieces of junk email are sent each year.[16] A recent study found that over 90% of users receive spam at least once a week, while almost 50% of users receive spam six or more times per week.[17] As the number of bulk emails sent has grown, so has the burden imposed by these emails on ISPs and recipients. A recent study estimated that over one billion dollars is lost each year because of spam.[18]

ISPs suffer most of this loss.[19] Spam causes the ISPs to lose customers[20] and spend extra money on staffing (due to increased traffic and user complaints) and

---

Controlling Unsolicited Bulk E-mail, Sun World, Aug. 1997, at 1, available at http://www.sunworld.com/sunworldonline/swol-08-1997/swol-08-junkemail.html.

[14] Note that bulk email can be either commercial (such as an advertisement) or non-commercial (such as a joke or chain letter). Both types are equally costly to ISPs and recipients (see supra notes 19 to 24 and accompanying text). However, the spam controversy generally focuses on commercial bulk email, since that is the most common type of bulk email.

Some states have passed statutes that regulate all unsolicited emails, whether they are 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 casenote will assume that spam is always commercial in nature.

[15] It is much less expensive to send bulk mail via email than it is via conventional mail. With conventional mail, each additional piece of mail sent requires both another paper copy and additional postage. With email, however, the only cost to the sender is typing one more email address into the recipient list. This cost differential arises because the cost of bulk email is shifted to other parties, such as the sender's Internet Service Provider (ISP), the recipient's ISP, and the recipient herself. The additional costs imposed on the ISPs and the recipient are never borne by the sender. Junk E-mail: Hearings Before the Senate Subcommittee on Communications of the Senate Committee on Commerce, Science and transportation, 105th Congress (1998), available at 1998 WL 12761269 (testimony of Deirdre Mulligan, Staff Counsel, The Center for Democracy and Technology).

[16] Jon Swartz, Reputed King of Junk E-mail Says He's Through Spamming, S.F. Chron., June 4, 1998, at D3.

[17] Talk given by John Leo (AT&T WorldNet Service) at Spam Summit 2000. http://www.spamsummit.com/presentations/leo/tsld015.html.

[18] Talk given by Michael Serbinis (Critical Path) at Spam Summit 2000. http://www.spamsummit.com/presentations/serbinis/tsld007.html

[19] Spam can cost ISPs hundreds of thousands of dollars per year. Bowen article at 4.

hardware (to obtain more storage and bandwidth).[21] Spam also causes outages and brownouts.[22] In response to these losses, ISPs have sued spammers for damages.[23] Costs imposed by spam on the recipient include money spent for Internet access time to download the spam and time spent to read and delete the spam.[24]

III. Private and Legislative Responses to Spam

As shown by Part II, *supra*, the spam problem is both widespread and costly. In response to this problem, many different types of approaches have been used to cut down on spam. The private sector responded to spam first, followed by the public sector.[25] Part III.A provides an overview of the private sector's response to spam, including norms, technology, and organizations. Part III.B describes state legislative responses to spam, including general approaches to anti-spam legislation and specific anti-spam laws.

---

[20] ISPs lose 7.2% of their new customers every year to spam, according to a 1999 survey conducted by GartnerGroup. Talk given by John Leo (AT&T WorldNet Service) at Spam Summit 2000. http://www.spamsummit.com/presentations/leo/tsld004.html

[21] http://www.spamsummit.com/presentations/serbinis/tsld007.html and http://www.spamsummit.com/presentations/serbinis/tsld011.html

[22] *Id*.

[23] Many ISPs have sued Cyber Promotions, a spammer. See CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015 (S.D. Ohio 1997) and American Online, Inc. v. Cyber Promotions, Inc., 948 F. Supp. 436 (E.D. Pa. 1996).

[24] **CITE**

[25] Although spam has only recently become a widespread problem (*see supra* note 16 and accompanying text), the private sector recognized that unwanted emails were a potential problem back 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 ftp://ftp.internic.net/rfc/rfc706.txt; P. Denning, *Electronic junk*, Communications of the ACM, vol. 3, issue 25, 163-165 (Mar. 1982).

A. Private Responses to Spam

The private responses to spam consist primarily of enforcement of social norms[26] of the Internet. Just like societal norms, Internet norms are largely unwritten. However, since most users of the Internet do not like unsolicited email,[27] commentators have argued that sending spam violates Internet norms,[28] sometimes referred to as "netiquette."[29] Although the actual rules of netiquette are vague, a recent Canadian court held a spammer liable based on violation of these rules.[30] Thus, violation of netiquette can sometimes have a legal effect.

ISPs and private organizations are the primary actors in the private-sector spam area. [31] Part III.A.1 describes the role of these actors, while Part III.A.2 analyzes the results of their actions.

1. How ISPs and Organizations Control Spam

ISPs control spam via their use policies. When a user signs up with an ISP, she frequently has to agree to follow the ISP's terms of use. Recently, ISPs have begun to include Internet norms in their use policies.[32] While some of these use policies use the

[26] "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, available at http://www.temple.edu/lawschool/dpost/blackohle.html.
[27] *See supra* note 13.
[28] **CITE**.
[29] "Netiquette" is a combination of the words "net" (for Internet) and "etiquette."
[30] 1267623 Ontario Inc. et al. v. Nexx Online Inc., Ont. Sup. Ct. Just., June 14, 1999, 1999 Ont. Sup. C.J. LEXIS 465
[31] At least one commentator has suggested that private self-regulation is the best way to regulate the Internet. See Blake article (lack of physical situs) at 157.
[32] For example, America Online's (AOL's) Unsolicited Bulk E-mail Policy explicitly does not authorize use of AOL's computers and network to "accept, transmit or distribute unsolicited bulk e-mail sent from the Internet to AOL members." (http://www.aol.com/info/bulkemail.html). Yahoo's Terms of Service

vague term "netiquette" to indicate acceptable behavior,[33] some policies explicitly disallow using the ISP to send spam.[34]

Because sending spam involves two ISPs — the sender's ISP and the recipient's ISP, an ISP's use policy can be used to combat spam in two ways: to prevent an ISP's subscriber from sending spam via that ISP, and to prevent an outside user from sending spam to that ISP's subscribers. The first way obtains its legal power from the contract that the subscriber signed with the ISP.[35] The second method, blocking incoming email does not have this same legal power because the outside user has no contract with the ISP.[36]

In order to control spam, an ISP uses filtering software. The filtering software detects whether a particular email message is spam. Once spam is detected, it can be 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 method allows the recipient to choose whether to read or delete the spam. Either ISPs or

---

prohibit the user from 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." (http://docs.yahoo.com/info/terms/, Section 6(g))

[33] NYTimes Kaplan article at http://www.nytimes.com/library/tech/99/07/cyber/cyberlaw/16law.html. The Canadian case in note 30 involved an ISP policy that required users to conform to netiquette. **CITE**.

[34] *See id*. and supra note 32.

[35] For example, the contract might specify that if a subscriber breaks the ISP's rules, the subscriber is barred from using the ISP.

[36] However, some states have passed laws that give ISP policies the force of law. In general, these laws allow the ISP to sue the outsider for trespass to chattels (the chattels being the ISP's computer systems). *See, e.g.*, CAL. BUS. & PROF. CODE § 17538.45 (discussed *infra* in Part III.B.2.a). *See also* Dan L. Burk, Article: 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, NYTimes, July 28, 2000, http://www.nytimes.com/library/tech/00/07/cyber/cyberlaw/28law.html.

individual recipients can use message-filtering software. One example of a spam-filtering product made for ISPs is Brightmail's Anti-Spam.[37]

Many anti-spam consumer organizations have arisen in response to spam.[38] The most vocal and active U.S. organizations include the Coalition Against Unsolicited Commercial Email (CAUCE),[39] SueSpammers.org,[40] and Junk Busters.[41] These organizations share knowledge about recent spam legislation and cases and how to combat spam personally and via legislative and lobbying activities.

Mail Abuse Prevention System (MAPS) is a private organization that 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."[42] MAPS distributes the RBL to ISPs so that they can block email coming into their networks from blacklisted networks. In order to produce

[37] http://www.brightmail.com/isp/anti-spam/. Common ways of detecting spam include examining the subject line and body of the email 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 (emails which are not spam but are treated like spam) and false negatives (emails which are spam but are not caught by the system). Blocking some non-spam emails and allowing some spam emails to go through are the major drawbacks of using filtering software. **CITE** o'reilly spam book.

[38] Foreign anti-spam organizations include the European Coalition Against Unsolicited Commercial Email (EuroCAUCE) (http://www.euro.cauce.org/en/), the Coalition Against Unsolicited Bulk Email, Australia (CAUBE.au) (http://www.caube.org.au/), and CAUCE India (http://www.india.cauce.org/).

The spam industry has recently started regulating itself. On September 14, 2000, fifteen companies announced their intent to form a coalition to design email standards to limit unsolicited email. Jennifer DiSabatino, E-mail marketers form alliance for antispam protocols, Computerworld, Sep. 15, 2000. (accessed via web page) Members of this coalition, the Responsible Electronic Communications Alliance (RECA), http://www.responsibleemail.org/, include DoubleClick, Inc., and Yesmail.com. DiSabatino article, note **Error! Bookmark not defined.**.

[39] http://www.cauce.org/

[40] http://www.suespammers.org/

[41] http://www.junkbusters.com/

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

the RBL, MAPS uses its own definition of spamming. According to the RBL, acceptable email solicitations must include a double-opt-in system.[43]

2. Results of Spam Control by ISPs and Organizations

Using ISP policies to prevent outside users from sending spam to ISPs' subscribers imposes a large burden on spammers. This burden is so large that it may outweigh the cost benefits[44] of spamming entirely, causing the spammer to abandon his activities.[45] While this is the goal of many people,[46] it is important to examine why and how this burden comes about.

By definition, spammers send the same email to many different recipients. Each of these recipients belongs to an ISP. While users tend to belong to the largest ISPs, in reality there are thousands of ISPs in the United States alone.[47] Thus, it is possible that one piece of spam will arrive at many different recipient ISPs.

To comply with the use policy of each recipient's ISP, a spammer must first obtain the policy of each ISP and learn the requirements it places on incoming emails. Next, the spammer must modify the spam so that it complies with each ISP's policy. Since each ISP can have a different use policy, it is very difficult for one email to comply

[43] The first opt in occurs when a new subscriber asks to receive mailings via submitting her email 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 that new mailing-list subscriptions be verified. Nick Nicholas, Basic Mailing List Management Principles for Preventing Abuse, http://mail-abuse.org/manage.html (last revised July 20, 1999).
[44] *See supra* notes **Error! Bookmark not defined.** to **Error! Bookmark not defined.** and accompanying text.
[45] **CITE**
[46] Note that some types of unsolicited email 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.
[47] In 1999, there were 5,775 ISPs in the United States. That number is expected to increase to 7,785 in 2000. Cahners In-Stat Group, *Press Release: National ISPs Stand to Gain Most in Growing U.S. Market* (Sep. 25, 2000), http://www.instat.com/pr/2000/is0004sp_pr.htm.

with every ISP's policy. In particular, it is possible that ISP policies will directly conflict with one another. 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 email cannot literally 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.[48] If ISP use policies do in fact conflict, any email sender might be unable to send one version of an email to recipients at two different ISPs while complying with both ISPs' use policies. Thus, conflicting obligations may silence mass emailers, whether commercial or not, creating a potentially unacceptable chilling effect on speech.

Turning now to the MAPS system of spam control, while the RBL has successfully reduced the amount of spam received by its subscribers, it has been heavily criticized.[49] First, critics argue that single-opt-in systems are a valid way of obtaining permission from users to send them bulk email.[50] Since MAPS requires a double-opt-in system, bulk emailers who do obtain single-opt-in permission are nonetheless placed on the RBL. [51] This disagreement over the definition of "spam" is important, since the widespread usage of the RBL results in MAPS' definition being applied to the entire Internet.

---

[48] The problem of conflicting obligations will be revisited in Part IV.B.2.b.ii, which discusses this problem with respect to state laws.
[49] *See* Post, *supra* note 26; **CITE**. For MAPS' response to these criticisms, see the *MAPS RBL Rationale* by Paul Vixie, http://mail-abuse.org/rbl/rationale.html (last revised July 19, 2000).
[50] **CITE**.
[51] For example, a federal district court recently sustained a temporary injunction barring MAPS from adding Yesmail.com to the RBL. **CITE** (federal district court case from chicago) Yesmail and MAPS have since come to an agreement whereby Yesmail will change its email policies and MAPS will remove Yesmail from the RBL. **CITE**

Critics also argue that MAPS' methods are grossly overbroad:[52] If one user sends spam from an ISP, then all users of that ISP are placed on the RBL. Thus, people who are not spammers are frequently blocked by the RBL. Since the RBL is a completely private enterprise, there is little incentive 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 emails.

Finally, many ISPs use the RBL to filter their email, but because MAPS is a private organization, the public has little (if any) input into how it runs, including whom 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' email addresses on the RBL. Moreover, MAPS could choose to censor these users based on, for example, their public expression of a viewpoint with MAPS disagrees.[53] This scenario demonstrates the need for oversight and a public voice in spam regulation.

The next section discusses the legislative approaches to spam. Legislation seems like a promising way to control spam, since the process is public, the implementers of the system would be accountable, and the rules would have a real effect because they have the force of law.[54]

B. Legislative Responses to Spam

Many spam laws have been passed in an attempt to decrease spam in order to reduce its burden on ISPs and recipients. These laws have been enacted in both the

[52] **CITE**.
[53] *Cf.* **CITE** (discussing filtering software that blocks websites which criticize the maker of the software or the software itself).

United States and in foreign countries.[55] Part III.B.1 describes the general categories of spam laws, while Part III.B.2 examines some actual spam laws. In particular, Part III.B.2 closely examines the spam laws of Washington and California.

Each state may enact a different spam law and, like different ISP use policies, the various laws may impose conflicting obligations. Thus, a mass emailer might be subject to inconsistent state obligations. Also, it might be unclear which state law to apply to a particular email, since the email may have originated in one state, traveled through many other states, and arrived in yet another state. These problems will be discussed further in Parts IV and V, *infra*.

1. Categories of Spam Laws

Spam laws can be categorized based on how they address the spam problem.[56] Emails contain many pieces of information that tell the recipient about the sender. One piece of information is the return address, which specifies who sent the email. Another piece is the header, which specifies the route the email has taken through the Internet to get from the sender to the recipient.[57] Most anti-spam laws work by regulating the information conveyed in these identifiers. Part III.B.1.a provides an overview of laws that explicitly regulate spam, while Part III.B.1.b demonstrates how consumer protection statutes can be used to combat spam.[58]

---

[54] 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 US laws.
[55] For information on anti-spam activities in foreign countries, see http://www.spamlaws.com/eu.html (EU) and http://www.spamlaws.com/world.html (other countries). **ARTICLE** on european spam laws/cases.
[56] Ochoa article at 461.
[57] Ochoa article at 462.
[58] *Id*. Various other types of statutes have been passed which make it easier to cut down on spam. One approach is to outlaw software that facilitates the sending of spam. (*See, e.g.*, VA. CODE ANN. § 18.2-

a. Laws That Explicitly Regulate Spam

Some laws seek to regulate spam as such. The first hurdle such regulations must overcome is to accurately define unsolicited commercial email. A common statutory definition of "unsolicited" can be found in a North Carolina statute: "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."[59] 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."[60]

Once a specific piece of email has been identified as spam, the law attempts to control it in some way. For example, some laws require senders to label spam by putting the phrase "ADV:" in the subject line of spam emails.[61] These laws often allow ISPs and recipients to sue spammers for damages.[62]

b. Consumer Protection Statutes

152.4(b) (1999). This type of statute may be unconstitutional based on First Amendment grounds because sometimes software is speech. *See, e.g.*, Junger v. Daley, 2000 WL 343566, *4 (6th Cir. 2000); Bernstein v. United States Dept. of Justice, 176 F.3d 1132 (9th Cir. 1999)). Another approach is to explicitly give courts long-arm jurisdiction (i.e., personal jurisdiction over out-of-state actors) so that out-of-state spammers can be prosecuted. (*See, e.g.*, Okla. Stat., Tit. 15, 776.3 (1999).) 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 46a-6G-3(4) (1999)) or attempts to prevent spam (*see, e.g.*, W. Va. Code 46a-6G-3(1) – (3) (1999)). Lastly, state laws differ as to who may sue spammers. Possible plaintiffs include ISPs, recipients of spam, and state attorney generals. (Ochoa article at 464.) Violations of spam statutes may be either civil or criminal offenses, depending on the state. (Ochoa article at 464.)

[59] N.C. GEN. STAT. § 14-453 (10) (1993).

[60] *Id*. § 14-453 (1b) (1999).

[61] *See, e.g.*, CAL. BUS. & PROF. CODE § 17538.4 (2000), discussed *infra*; **CITE**.

[62] *See, e.g.*, CAL. BUS. & PROF. CODE § 17538.45 (2000), discussed *infra*; **CITE**.

Consumer protection statutes require that advertisers not mislead buyers with false information. Spammers may violate these statutes by deliberately putting false information in their spam to keep their identities secret. In this way, they can avoid complaints and lawsuits from recipients and ISPs. For instance, spammers modify their messages to contain misleading information, such as 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 email not alter, misrepresent, or obfuscate the return address or header information.[63] These laws do not prevent spam, but they do help because they 1) help recipients identify spam via relevant subject lines; 2) make emails 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 emails with false return addresses.[64] The court held the spammer liable under a state consumer fraud statute and granted an injunction against the spammer.[65]

2. State Anti-Spam Laws

[63] **CITE**.
[64] People v. Lipsitz, 663 N.Y.S.2d 468 (Sup. Ct. 1997).
[65] *Id.* at 468.

Nevada introduced the first state anti-spam bill in January 1997.[66] As of September 2000, **NUMBER** states had passed spam laws.[67] Many commentators have hypothesized on the constitutionality of these state spam laws,[68] citing issues such as the First Amendment[69] and the Dormant Commerce Clause (hereinafter, "DCC").[70]

Although, in the past, some cases have addressed the problem of Internet content regulation and the DCC,[71] only recently have any state spam laws been held unconstitutional under the DCC. The next two sections discuss the Washington and California spam laws that were held to violate the DCC.

a. Washington Anti-Spam Law

On June 11, 1998, Washington's Unsolicited Electronic Mail Act (UEMA)[72] took effect,[73] thereby making Washington the first state to effect a spam regulation.[74] The UEMA applies to email sent from a computer in Washington or to an email address that belongs to a Washington resident.[75] The Act explicitly prohibits spoofing[76] and also

[66] NEV. REV. STAT. 41.3 (1998) (introduced Jan. 1997, enacted July 1997, effective July 1, 1998).
[67] For a good overview of state spam laws, see Ochoa article.
[68] *See* Dan L. Burk, *Federalism in Cyberspace*, 28 CONN. L. REV. 1095 (1996); Kenneth D. Bassinger, Note, *Dormant Commerce Clause Limits on State Regulation of the Internet: The Transportation Analogy*, 21 GA. L. REV. 889 (1998).
[69] For an overview of the subject, see Joshua A. Marcus, Note: *Commercial Speech on the Internet: Spam and the First Amendment*, 16 CARDOZO ARTS & ENT. L.J. 245 (1998).
[70] Other problems with state spam statutes include obtaining personal jurisdiction over the spammer. *See generally* Blake article (lack of physical situs).
[71] See American 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) based on DCC grounds); Johnson, 4 F. Supp. 2d at 1029 (New Mexico) (enjoining action under an Internet content-related statute based on DCC 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 (suggesting that the IDL can escape DCC problems by restricting its application to conduct occurring only in New York); Gaylord article – letting DCC lie (suggesting that the extraterritoriality principle relied on will soon no longer be valid).
[72] WASH. REV. CODE § 19.190 (**YEAR**).
[73] Ochoa article at 461, n.12.
[74] *Id*.
[75] § 19.190.020(1).

provides that spoofing violates Washington's consumer protection act.[77] ISPs can recover damages of $1,000 or actual damages (whichever is greater) and recipients can recover damages of $500 or actual damages (whichever is greater).[78] Lastly, the UEMA immunizes from liability an ISP that blocks in good faith the receipt or transmission through its servers of email that violates the Act.[79]

On March 10, 2000, a Kings Country trial court held that the UEMA violates the DCC.[80] In a brief opinion, the court held that the UEMA "violate[d] the Federal Interstate Commerce Clause of the United States Constitution [and was] unduly restrictive and burdensome."[81] On April 6, 2000, the Attorney General appealed the decision.[82]

b. California Anti-Spam Laws

Three new spam laws took effect in California on January 1, 1999.[83] A trial court has already ruled that one of these laws, section 17538.4 of the Business & Professions Code, [84] violates the DCC.[85] Courts have not yet considered the other two laws.

Section 502 of the Penal Code,[86] originally added by California's "Comprehensive Computer Data Access and Fraud Act," was amended to prohibit

---

[76] Specifically, it is illegal to send unsolicited commercial email that "[u]ses a third party's internet domain name without permission of the third party, or otherwise misrepresents or obscures any information in identifying the point of origin or the transmission path" or "[c]ontains false or misleading information in the subject line." *Id*.
[77] § 19.190.030.
[78] § 19.190.040.
[79] § 19.190.050.
[80] Washington v. Heckel, Wash. Super. Ct. (Kings Cty.), No. 98-2-25480-7SEA.
[81] *Heckel*, Judge's order on civil motion granting defendant's summary judgment, March 10, 2000.
[82] Attorney General of Washington, News Release*: AG's Office Files Notice of Appeal in Anti-Spam E-mail Lawsuit*, http://www.wa.gov/ago/releases/rel_spam_040600.html.
[83] David Kramer, California's New Anti-Spam Laws, Wilson Sonsini Goodrich & Rosati Library, http://www.wsgr.com/library/libfileshtm.asp?file=spam.htm.
[84] *See infra*.
[85] Ferguson v. Friendfinder, Inc., Cal. Super. Ct. (S.F.), No. 307309.
[86] CAL. PENAL CODE § 502 (1999).

spoofing[87] if the spoofing causes damage to one or more computers.[88] Violators of the statute are subject to criminal prosecution.[89] Penalties depend on the damages that the violation causes.[90] Additionally, victims may bring a civil suit against an offender convicted under Section 502.[91] In this manner, parties whose domain names have been spoofed by spammers can be compensated.

Section 17538.45 of the Business & Professions Code,[92] also known as the "Miller bill," was added to give an ISP the right to sue people who use its network to send spam.[93] The Miller bill allows an email service provider,[94] such as an ISP, to sue someone who sends unsolicited commercial email[95] either from the ISP or to an ISP subscriber. Thus, the ISP can sue both registered users of the ISP and outsiders.[96] If the suit is successful,[97] the ISP can recover damages from network clogs or crashes.[98]

---

[87] The statute defines spoofing as the unauthorized use of another party's domain name in connection with the sending of electronic mail messages. § 502(c)(9).
[88] *Id.*
[89] § 502(d).
[90] § 502(d)(4).
[91] § 502(e).
[92] CAL. BUS. & PROF. CODE § 17538.45 (2000).
[93] For commentary on this statute, see David T. Bartels, *Review of Selected 1998 California Legislation: Business Associates and Professions: Canning Spam: California Bans Unsolicited Commercial E-mail*, 30 MCGEORGE L. REV. 420, 430 (suggesting that the statute does not violate the Dormant Commerce Clause).
[94] The statute defines "email 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." § 17538.45(a)(3).
[95] The statue defines "commercial email" 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." § 17538.45(a)(1). "Unsolicited" is defined as "addressed to a recipient with whom the initiator does not have an existing relationship" and "is not sent at the request of or with the express consent of the recipient." § 17538.45(a)(2).
[96] This possibility was discussed in Part III.A.1, *supra*.
[97] In order for the ISP to succeed in its claim, it 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.
[98] Specifically, the ISP can recover $50 per spam email sent (up to $25,000 per day) or actual damages, whichever is greater. § 17538.45(f)(2).

Section 17538.4 of the Business & Professions Code,[99] California's "junk fax" law, was amended to allow spamming, but only if the spam[100] messages meet two requirements. First, the subject line of a spam message must begin with the characters "ADV:".[101] If the spam advertises adult goods,[102] the subject line must begin with the characters "ADV:ADLT".[103] Second, the body of a spam message must contain a toll-free phone number or email address that the recipient can use to notify the sender not to send her any more spam.[104] Violations of the statute are punishable as a misdemeanor.[105] The statute does not give ISPs or spam recipients a private cause of action against spammers.

[99] CAL. BUS. & PROF. CODE § 17538.4 (2000).
[100] 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 or with the express consent of, the recipient." § 17538.4(e).
[101] "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." § 17538.4(g).
[102] Approximately 11% of spam has adult content. Talk given by Michael Serbinis (Critical Path) at Spam Summit 2000. http://www.spamsummit.com/presentations/serbinis/tsld007.html
[103] "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." § 17538.4(g).
[104] § 17538.4(a)(2).
[105] CAL. BUS. & PROF. CODE § 17534 (**YEAR**).

On June 2, 2000, a San Francisco trial court held that section 17538.4 violates the DCC.[106] In a short opinion, the judge found that the statute "unconstitutionally subject[ed] interstate use of the Internet to inconsistent regulations, therefore violating the DCC of the United States Constitution."[107] The constitutionality of section 17538.4 will be discussed in Part V, *infra*.

IV. The Dormant Commerce Clause: A Judicially-Created Restriction on State Regulation of Interstate Commerce

As mentioned in Part III.B.2, *supra*, state spam laws in Washington and California have recently been held to violate the DCC. In order to understand these decisions, Part IV introduces the DCC and outlines the major doctrines and tests that are used when applying the DCC to a state statute.

A. Introduction

Over the years, the Supreme Court has held that the DCC prohibits states from regulating interstate commerce.[108] However, this prohibition is not explicitly present in the Constitution. Instead, the DCC stems from the negative implication of the Commerce Clause. The Commerce Clause states that "Congress shall have Power . . . [t]o regulate

[106] Ferguson v. Friendfinder, Inc., Cal. Super. Ct. (S.F.), No. 307309.
[107] *Ferguson*, Judge's order sustaining defendants' demurrer without leave to amend, June 2, 2000.
[108] "[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." 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).

At this point, it is important to note that some commentators doubt the legitimacy of the DCC. *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, *Comment, The Dormant Commerce Clause: On Its Last Leg*, 57 ALB. L. REV. 1215, 1243 (1994).

Commerce . . . among the several States."[109] Because Congress has the power to regulate interstate commerce, states cannot pass laws that interfere with interstate commerce.[110] Many different types of state laws have been struck down because they affect interstate commerce.[111]

The DCC first arose in dicta in *Gibbons v. Odgen*,[112] 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."[113] However, the Court did not officially acknowledge the negative aspect of the Commerce Clause until *Willson v. Black Bird Creek Marsh Co.*[114] In *Willson*, Marshall noted that state legislation might fail if it were "repugnant to the power to regulate commerce in its dormant state."[115]

Such legislation did fail in the *Passenger Cases*.[116] In that case, the Court held (5-4) that statutes imposing bond requirements and taxes on immigrants arriving at state ports were unconstitutional. However, the DCC's role in the ruling is unclear. Only three of the eight separate opinions clearly relied on the DCC for their results.

It is important to note that the DCC is not an absolute bar on certain types of state legislation. Congress can always explicitly authorize a state to act in a particular area otherwise precluded by the DCC.[117] Congress' ability to authorize state regulations stems

---

[109] U.S. CONST. art. I § 8 cl. 3.
[110] *See* Cooley v. Board of Wardens, 53 U.S. (12 How.) 299, 317-19 (1851); Willson v. Black Bird Creek Marsh Co., 27 U.S. (2 Pet.) 245 (1829); Gibbons v. Ogden, 22 U.S. (9 Wheat.) 1, 5-6 (1824).
[111] *See, e.g.,* Dean Milk Co. v. City of Madison, 340 U.S. 349 (1951) (produce regulations); Southern Pac. Co. v. Arizona *ex rel.* Sullivan, 325 U.S. 761 (1945) (railroad regulations).
[112] Gibbons v. Ogden, 22 U.S. (9 Wheat.) 1 (1824).
[113] *Id*. at 199-200.
[114] Willson v. Black Bird Creek Marsh Co., 27 U.S. (2 Pet.) 245 (1829).
[115] *Id*. at 252.
[116] Passenger Cases, 48 U.S. (7 How.) 283 (1849).
[117] Laurence H. Tribe, American Constitutional Law, § 6-**SECTION** (3d ed. **YEAR**); Reynolds article at 542 n.20.

from Congress' power to regulate interstate commerce under the Commerce Clause. Thus, instead of imposing its own law, Congress can instead allow the states to regulate certain activities.

B. The DCC Prohibits State Regulations that Discriminate Against or Excessively Burden Interstate Commerce

In its modern form, the DCC prohibits states from discriminating against or unduly burdening interstate commerce.[118] The Court clearly articulated the test for whether a state statute violates the DCC in *Oregon Waste Systems v. Department of Environmental Quality*.[119] In that case, the Court analyzed an Oregon statute that imposed a surcharge on the disposal within Oregon of solid waste generated outside of Oregon. "The first step in analyzing any law subject to judicial scrutiny under the negative Commerce Clause [(DCC)] is to determine whether it regulates evenhandedly with only incidental effect on interstate commerce, or discriminates against interstate commerce."[120] The Court held that the surcharge imposed by the statute was discriminatory on its face, since the fee depended on whether the waste was generated out-of-state.[121] Thus, the Court held that the statute violated the DCC. [122]

[118] *See infra*. As a preliminary matter, the DCC applies only to statutes that regulate activities that are within Congress' Commerce Power. The Commerce Power encompasses "interstate commerce itself" (such as items shipped across state lines) and "that which affects interstate commerce" (such as shipping and transportation mechanisms; also known as "instruments of interstate commerce"). Gibbons v. Ogden, 22 U.S. (9 Wheat.) 1, **PINCITE** (1824).
[119] Oregon Waste Systems v. Department of Environmental Quality, 511 U.S. 93 (1994).
[120] *Id*. at 99.
[121] *Id*.
[122] *Id*. at 108.

Thus, under *Oregon Waste Systems*, a court will first determine whether the spam statute discriminates against interstate commerce.[123] If it regulates evenhandedly, then the court analyzes the effect the law has on interstate commerce.[124] If the law excessively burdens interstate commerce, then it may violate the DCC despite its evenhandedness.[125]

a. Discriminating Against Interstate Commerce and the Extraterritoriality Doctrine

"Discrimination" in this context means "differential treatment of in-state and out-of-state economic interests that benefits the former and burdens the latter."[126] State statutes that facially discriminate against interstate commerce trigger strict scrutiny and are usually invalid.[127] The statute will be held invalid unless the state can show that it has no other way to advance a legitimate local interest.[128]

A state also directly discriminates against interstate commerce by attempting to project its law into other states. In *Edgar v. MITE*,[129] the Court considered an Illinois statute that regulated tender offers for certain companies.[130] 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.[131] The Court held that the statute violated the DCC, a plurality holding that a regulation having the "practical effect" of regulating transactions which take place extraterritorially (i.e., across state lines) exceeds the

[123] *See infra* Part IV.B.1.
[124] *See infra* Part IV.B.2.
[125] **CITE**.
[126] *Oregon*, 511 U.S. at 99.
[127] Maine v. Taylor, 477 U.S. 131 (1986) (outlining the discriminatory effect test).
[128] For a law that was held valid despite its being found discriminatory, see C&A Carbone, Inc. v. Town of Clarkstown, 511 U.S. 383, 392 (1994).
[129] Edgar v. MITE, 457 U.S. 624 (1982).
[130] *Id*. at 626-27.
[131] *Id*. at 627.

"inherent limits of the State's power," regardless of the legislators' intentions.[132] The Court defined the "extraterritoriality doctrine"[133] as such: "The Commerce Clause . . . precludes the application of a state statute to commerce that takes place wholly outside of the State's borders, whether or not the commerce has effects within the state."[134]

In *Healy v. Beer Institute*, [135] the Court used the extraterritoriality doctrine to hold that a Connecticut law violated the DCC "per se."[136] 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.[137] Most importantly, the Court synthesized the holdings of previous extraterritoriality cases, stating that "the Commerce Clause . . . precludes the application of a state statute to commerce that takes place wholly outside of the State's borders, whether or not the commerce has effects within the state."[138] Also, 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."[139] Lastly, the intent of the legislature does not affect the validity of the statute.[140]

---

[132] *Id.* at 642-43.
[133] Some commentators have suggested that the holdings in the extraterritoriality cases were based on something other than DCC concerns. See Gaylord article - letting DCC lie (requirement of a nexus between state interests and regulated enterprises).
[134] *Edgar* at 642-43.
[135] Healy v. Beer Institute, 491 U.S. 324 (1989).
[136] *Healy*, 491 U.S. at **PINCITE**.
[137] *Id*. at 335.
[138] *Id*. at 336 (internal citations and quotation marks omitted).
[139] *Id*. at 337 (internal citations and quotation marks omitted).
[140] "[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

b. Excessively Burdening Interstate Commerce

Even if a law regulates evenhandedly and does not directly discriminate, it may still violate the DCC if it places an excessive burden on interstate commerce.[141] In this situation, the law could be seen as "indirectly" discriminating against interstate commerce.

In order to determine whether a state law places an excessive burden on interstate commerce, courts balance the local benefits conferred by the law against the burdens imposed on interstate commerce.[142] In *Pike v. Bruce Church*,[143] the Court considered an Arizona statute that prohibited interstate shipment of cantaloupes not packed in regular compact arrangements in closed standard containers.[144] The Court held that the statute violated that DCC, 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."[145]

In general, the balancing test weights 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.[146] In *Cooley v. Board of Wardens*,[147] the Court held that states are permitted to regulate those interests that are so local in nature as to demand

---

to control conduct beyond the boundaries of the State." *Id*. at 337 (internal citations and quotation marks omitted).
[141] Kassel v. Consolidated Freightways Corp. of Del., 450 U.S. 662 (1981).
[142] Pike v. Bruce Church, Inc., 397 U.S. 137, 142 (1970).
[143] 397 U.S. 137 (1970).
[144] *Id*. at 138.
[145] *Id*. at 142.
[146] *See infra* Part IV.B.2.b.ii.
[147] Cooley v. Board of Wardens of the Port of Philadelphia, 53 U.S. (12 How.) 299 (1851).

diverse regulation, while Congress has exclusive domain over those aspects of interstate commerce that are so national in character as to demand uniform treatment.[148]

i. 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.[149] 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.[150] Thus, regulations designed to protect public health or safety will probably not be overturned unless their justifications are "illusory."[151]

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.[152] Also, it is more likely that the law will be declared unconstitutional if a reasonable alternative to the legislation exists that would cause "less of an impact" on interstate commerce.[153]

ii. Burden on Interstate Commerce

After determining the local benefit at stake, the court assesses the burden on interstate commerce, especially the possibility of imposing inconsistent obligations.[154]

---

[148] Cooley at 319.
[149] *Pike* at 142.
[150] *See, e.g.,* Kassel v. Consolidated Freightways Corp., 450 U.S. 662, 670 (1981).
[151] *Id*.
[152] *Pataki* at 178.
[153] *Pike* at 142.
[154] *See supra* Part III.A.2.

This problem arises most often when the area sought to be regulated is national in scope, because when states regulate national interests they may impose inconsistent obligations on interstate actors. Therefore, national interests must be regulated in a uniform way, which usually can be done only at a federal level. Thus, 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."[155] This factor has been determinative in cases involving transportation, communications, and taxes[156] — all are areas involving national interests.

In order to determine when an aspect of interstate commerce demands uniform treatment, the court considers the hypothetical effect of every state enacting conflicting laws concerning the subject matter of the case.[157] If such regulations would excessively burden that aspect of interstate commerce, then uniform treatment is required and the state law is struck down.

V. Analysis

Courts in both Washington and California have found that certain state spam statutes violate the DCC. Unfortunately, neither opinion revealed the court's reasoning. Part V.A attempts to fill that gap by carefully applying the DCC to the California statute held unconstitutional in *Ferguson v. Friendfinder*. Part V.B concludes that federal laws, not state laws, should be used to regulate spam.

[155] Wabash, St. Louis & Pac. Ry. Co. v. Illinois, 118 U.S. 557, 577 (1886).
[156] *See, e.g.,* Southern Pac. Co. v. Arizona *ex rel.* Sullivan, 325 U.S. 761 (1945) (holding that an Arizona statute, which limited the length of trains within the state, was unconstitutional). The court held that there

A. State Spam Laws Violate the DCC by Imposing Inconsistent Obligations on Interstate Spam

As discussed in Part III.B.2, *supra*, a trial court found that section 17538.4 of the California Business and Professions Code violated the DCC. This section draws upon this and other cases to determine whether the statute actually violated the DCC. The analysis below follows the DCC analysis outlined in Part IV.B.2, *supra*.

As a preliminary matter, Section 17538.4 ("the Section") can violate the DCC only if the area it regulates, spam, falls within the broad sweep of Congress' Commerce Clause power. There can be little doubt that sending spam qualifies as interstate commerce (IC) or an instrument of IC. Many courts have held that Internet communication, specifically emailing images through the Internet, qualifies as IC.[158] Assuming that spam is commercial in nature, spam that crosses state lines is IC also. Note that even if both the sender and recipient of spam are in the same state, the spam may still cross state lines before it reaches its destination and thus qualify as IC.[159]

Concerning instruments of IC, many courts and commentators have argued that the Internet itself is an instrument of IC.[160] If they are correct, then Congress has the power to regulate the Internet and thereby the power to regulate spam.[161] Their arguments rely on the similarities between the Internet and traditional instruments of IC, such as

---

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." Southern Pac. at 767.

[157] *Wabash* at **PINCITE**.

[158] 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 (1st Cir. 1997); United States v. Thomas, 74 F.3d 701, 706-09 (6th Cir. 1996).

[159] *Pataki* at 171. In fact, the judge in Pataki stated that "no [intrastate] communications exist". *Id*.

[160] *See Pataki* at 173; H. Joseph Hameline and William Miles, *The Dormant Commerce Clause Meets the Internet*, B.B.J., Oct. 1997, at 21; Blake article (lack of physical situs) at 8; Burk article at 1125-26. *See generally* Bassinger, *supra* note 68.

[161] Some critics worry that declaring that the Internet is an instrument of IC will result in the states' inability to regulate the Internet at all.

highways and railroads. Namely, both are mechanisms that are used to transport commercial items across state lines.[162]

The leading case in this area is *ALA v. Pataki*.[163] In *Pataki*, the court used the DCC to strike down a New York law that prohibited sexual contact over the Internet between adults and minors.[164] In reaching this conclusion, the court found 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."[165] Other cases where an Internet content regulation failed DCC scrutiny include *ACLU v. Johnson*[166] and *Cyberspace Communications v. Engler*.[167]

Recall that the Commerce Power allows Congress to regulate instruments that are part of a nationwide transportation network.[168] This power even stretches to portions of the instruments that are located entirely within one state.[169] Thus, if the Internet is an instrument of IC, then Congress can regulate parts of the Internet that are contained within one state. These parts would include cables and servers that comprise the nationwide network of the Internet.

Thus, a judge can rule that spam regulation comes within the Commerce Power either because spam is IC or because the Internet is an instrument of IC. Because spam regulation is within the Commerce Power, it is subject to DCC limits. The rest of the

---

[162] The Internet is a "conduit for transporting digitized information goods such as software, data, music, graphics, and videos . . . ." Burk article at 1125-1126.
[163] Am. Library Ass'n v. Pataki, 969 F. Supp. 160 (S.D.N.Y. 1997).
[164] *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.
[165] *Id.* at 161.
[166] 4 F. Supp. 2d 1029 (D.N.M. 1998); *aff'd by* Am. Civil Liberties Union v. Johnson, 194 F.3d 1149 (10th Cir. 1999) (**PARENTHETICAL**).
[167] 55 F. Supp. 2d 737 (E.D.Mich. 1999) (**PARENTHETICAL**).
[168] *See* Part IV.B.1, *supra*.
[169] *Id*.

analysis addresses whether Section 17538.4 in fact violates the DCC. It can violate the DCC in one of two ways: by discriminating against IC or by excessively burdening IC.

2. Discriminating Against Interstate Commerce

A statute discriminates against IC either by favoring in-state over out-of-state economic interests or by projecting itself into other states. In the realm of spam laws, differential treatment would involve allowing spam that originated *inside* the recipient's state while prohibiting spam that originated *outside* the recipient's state. Section 17538.4 states that "[n]o person or entity conducting business in this state"[170] may send spam to "a California resident via an electronic mail service provider's service or equipment located in this state."[171] Since the Section applies equally to spam that originates either outside or inside of California,[172] it does not provide differential treatment of spammers.[173]

The second type of discrimination against IC involves the extraterritoriality doctrine,[174] as summarized in *Healy v. Beer Institute*.[175] The extraterritoriality doctrine forbids states from regulating commerce that occurs wholly outside of the state's borders. On its face, Section 17538.4 appears to pass this test because it applies only to spam that originated from servers located in California. However, *Healy* requires the courts to also

[170] CAL. BUS. & PROF. CODE § 17538.4(a) (2000).
[171] § 17538.4(d).
[172] The only requirements are that the sender conducts 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.
[173] 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 Section 17538.4. § 17538.4(a)(2). However, the spammer can avoid this cost by allowing the recipient to complain via email. Thus, the Section might discriminate against out-of-state spammers in an insignificant way.
[174] *See supra* Part IV.B.2.a.
[175] **CITE** to Healy.

consider the practical effects of the statute, including what would happen if many states adopted similar, yet inconsistent, legislation.

This consideration is just another form of the "conflicting obligations problem"[176] discussed earlier. The problem exists here because the Section can apply to email 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 email may simply be routed through other states on its way from the sender to the recipient.[177] Second, the California resident could access the email remotely from another state. Either way, the requirements of the Section would still be met. In these situations, therefore, the email could be subject to both California's law and the potentially inconsistent law of the state through which the email traveled. Thus, Section 17538.4 may run afoul of the extraterritoriality doctrine.[178]

3. Excessively Burdening Interstate Commerce

The second way in which a state statute can violate the DCC is by excessively burdening IC. This analysis uses the *Pike* test, which balances the local benefits afforded by the statute with the burden that the statute places on IC.[179]

a. Local Benefits

[176] *See supra* Part III.A.2.
[177] *See supra* note 159 and accompanying text.
[178] One way for Section 17538.4 to pass this test is to amend the Section so that it applies only to spam that never leaves the state of California. However, due the indeterminacy involved in routing emails, two emails 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 Section (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 Section 17538.4).
[179] *See supra* Part IV.B.2.b.

The local benefits afforded by the state must further a legitimate state interest. In this context, legitimate state interests usually revolve around areas of local concern, such as the police powers over public health and safety. With respect to Section 17538.4, the state interest is economic.[180] California wants to protect its citizens and businesses from the costs associated with receiving spam. Traditionally, economic interests that benefit the state itself at the expense of interstate commerce have not been held to be legitimate.[181] In this case, however, the statute is economically benefiting California's citizens and businesses, not California itself. Thus, it is unclear whether this factor would weigh in favor of the statute being valid.

The other concern here is whether the statute is effective in achieving the desired result and whether better alternatives exist. In this case, Section 17538.4 may not be very effective due to difficulties in enforcement. If the spammer spoofs information in the email, 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 IC. Thus, overall, the local benefit side of the scale is not tipped very far (if at all) in favor of finding Section 17538.4 to be constitutional.

b. Burden on Interstate Commerce

[180] Note that consumer protection against fraud is a traditional state police power. Thus, the scale would be tipped in favor of approving consumer protection laws that regulate spam by prohibiting spoofing. In *Lipsitz*, for example, a law that prohibited spoofing escaped DCC invalidation because it only "tangentially" burdened interstate commerce. *Lipsitz* at 471.
[181] **CITE**.

In short, the burden placed on IC is the problem of conflicting obligations. As this problem has been discussed at length in other parts of this casenote,[182] that discussion will not be repeated here. It is important to realize, however, that state regulation of instruments of IC usually places a large burden on IC. This is because instruments of IC are national in scope and are therefore very vulnerable to inconsistent state laws. Thus, if the Internet is held to be an instrument of IC, the burdens that state Internet regulation place on IC are highly likely to outweigh any local benefits that are afforded by the regulation.

For example, in *Pataki*, the court stated that "[h]aphazard and uncoordinated state regulation can only frustrate the growth of cyberspace."[183] The court also found that the Internet "requires a cohesive national scheme of regulation so that users are reasonably able to determine their obligations."[184] Thus, the court concluded that the Internet is "susceptible to regulation only on a national level."[185] This line of reasoning suggests that virtually all state laws regulating the Internet would violate the DCC.[186]

As discussed in Part V.A.2, *supra*, Section 17538.4 can apply to spam that travels through states other than California. Because of this, it is likely that one piece of email can be subjected to inconsistent laws. Thus, the burden that the Section places in IC outweighs the Section's local benefits.

---

[182] *See supra* Parts III.A.2, IV.B.2.b.ii, and V.A.2.
[183] *Pataki* at 181.
[184] *Id.* at 182.
[185] *Id.* at 183.
[186] *Id.* at 170. See supra note 161. *Accord*, H. Joseph Hameline and William Miles, *The Dormant Commerce Clause Meets the Internet*, B.B.J., Oct. 1997, at 21; Burk at 1123-34; Glenn Harlan Reynolds, *Virtual Reality and "Virtual Welters": A Note on the Commerce Clause Implications of Regulating Cyberporn*, 82 VA. L. REV. 535, 537-42 (1996); 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, 141 (1998).

B. Using Federal Legislation to Control Spam

If the Internet is held to be an instrument of IC, then, in the absence of Congressional authorization, all state laws that regulate the Internet will violate the DCC. The only way to protect the Internet from inconsistent laws is to regulate the Internet at the national level. Thus, Congress (and not the states) should pass laws to regulate spam and other aspects of the Internet.[187]

So far, a total of approximately seventeen federal spam bills have been introduced into Congress,[188] all of which have failed to become law.[189] About ten federal spam bills are pending.[190] One of these is the Unsolicited Commercial Electronic Mail Act of 2000 (H.R. 3113) ("UCEMA"). UCEMA's goal is "[t]o protect individuals, families, and Internet service providers from unsolicited and unwanted electronic mail."[191]

UCEMA contains many provisions common to state spam laws. First, it requires that spam be labeled as such and include opt-out instructions.[192] UCEMA also prohibits spoofing.[193] Lastly, UCEMA would give ISP use policies the force of law.[194] Specifically, if an ISP's use policy is clearly posted on a web site at the domain name included in the recipient's email address, or is made available by an FTC-approved[195]

---

[187] *Accord*, **ARTICLES**.
[188] *See* http://www.spamlaws.com/federal/index.html (current bills); http://www.jmls.edu/cyber/statutes/email/fedtable.html (past bills). *See also* Max P. Ochoa, Case Note: Legislative Note: *Recent State Laws Regulating Unsolicited Electronic Mail*, 16 COMPUTER & HIGH TECH. L.J. 459, 459 n.4 ("Eight bills were introduced in the 105th Congress, none of which became law").
[189] *Id*.
[190] For a list of pending federal spam legislation, see http://www.spamlaws.com/federal/index.html.
[191] UCEMA, title of bill.
[192] This is very similar to Section 17538.4 of California's Business and Professions Code.
[193] This is very similar to Section 17538.45 of California's Business and Professions Code.
[194] *Id*.
[195] Federal Trade Commission

standard method, then it would be illegal to use the ISP's facilities in violation of the ISP's use policy.

The House passed UCEMA on July 18, 2000. Currently, the Senate Committee on Commerce, Science, and Transportation is reviewing UCEMA. Thus, Congress is aware of the spam problem and is trying to provide a solution. It remains to be seen whether a federal spam law will ever get passed.

VI. Conclusion

The costs that spam imposes on ISPs and recipients are increasing 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 the implementers are accountable for their actions. State spam legislation is subject to DCC limits. Some statutes, such as Section 17538.4 of the California Business and Professions Code, have been struck down because they violate the DCC. Because spam is sent interstate via the Internet, it must be regulated in a uniform way at a national level. Thus, spam should be regulated via federal laws, not via state laws.