1-1-2005

Preemption of State Spam Laws by the Federal Can-Spam Act

Roger Allen Ford
University of New Hampshire School of Law, roger.ford@law.unh.edu

Recommended Citation

Roger A. Ford, Preemption of State Spam Laws by the Federal Can-Spam Act. 72 U. CHI. LAW REV. 355 (2005).

Preemption of State Spam Laws by the Federal CAN-SPAM Act

Roger Allan Ford†

Unsolicited bulk commercial electronic mail is increasingly a problem on the internet. More than thirteen billion spam[1] messages are sent per day.[2] One study estimates that spam costs $10 billion annually in worker productivity in the United States.[3] In 2003, spam for the first time surpassed 50 percent of all email sent on the internet.[4] That same year AOL, the world's largest internet service provider (ISP), blocked 500 billion spam messages sent to its users[5]—about fifteen thousand per user, or more than forty per user per day. The total amount of spam received is even greater: millions more make it through filters to their recipients.

---

† S.B. 2002, Massachusetts Institute of Technology; J.D. Candidate 2005, The University of Chicago.

1 Though it now refers primarily to a type of email, "spam" as a pejorative term on the internet first referred to irrelevant or inappropriate mass messages posted to Usenet newsgroups. See *Spam*, Jargon File 4.4.7 (Dec 29, 2003), online at http://www.faqs.org/docs/jargon/S/spam.html (visited Nov 14, 2004) (discussing different meanings of the word "spam"). The first significant instance of Usenet spam came in 1994, when two Arizona immigration attorneys, Laurence Canter and Martha Siegel, posted advertisements for their services to more than 6,000 of the 9,000 newsgroups then in existence. See Mike Godwin, *Electronic Frontier Justice and the "Green Card" Ads*, Internet World 97 (Oct 1994) (discussing the controversy that arose around Canter and Siegel's ads). Canter was eventually disbarred, in part because of the advertising campaign. See Sharael Feist, *The Father of Modern Spam Speaks*, CNET News.com (Mar 26, 2002), online at http://news.com.com/2008-1082-868483.html (visited Nov 14, 2004).

The name itself comes from a 1970 Monty Python's Flying Circus sketch in which a waitress recites a menu containing "egg and spam; egg bacon and spam; egg bacon sausage and spam; spam bacon sausage and spam; spam egg spam spam bacon and spam; spam sausage spam spam bacon spam tomato and spam. . . ." David Crystal, *Language and the Internet* 53 (Cambridge 2001). Spam thus symbolizes the mindless, annoying repetition of mass commercial email. See id at 53–54.

There are as many definitions of spam as there are definers. One common definition refers to all commercial email. A narrower view applies the label only to *unsolicited* email, or to *bulk* email. See, for example, *Spam*, Jargon File 4.4.7 (listing six definitions of "spam"). Because of the lack of consensus on just which emails are spam, there is some inherent variance in any measure of the harms caused by spam.

2 Evan I. Schwartz, *Spam Wars*, 106 Tech Rev 32, 34 (July/Aug 2003).

3 Id.

4 Id.

5 *AOL Is Blocking Spam*, Wash Post E2 (Jan 5, 2004). See also AOL Press Release, *America Online Releases "Top 10 Spam" List of 2003* (Dec 31, 2003), online at http://media.timewarner.com/media/newmedia/cb_press_view.cfm?release_num=55253692 (visited Nov 14, 2004).

In short, internet spam is a significant problem,[6] and both the federal government and various states have attempted to curb the problem. Thirty-six states have enacted antispam laws.[7] Two have banned unsolicited spam entirely, requiring recipients to opt in to receiving such messages.[8] In part due to the uncertainty and conflict these state laws created, in 2003 Congress passed, and President Bush signed, the CAN-SPAM Act.[9] Thus far, though, these attempts to combat spam have not had a significant effect on the amount of spam sent.[10]

Technical issues make enforcement of *any* spam law difficult. Spam senders frequently use forged email headers and send email through third-party computers, often located overseas, that aren't secured against outside use. It thus becomes difficult or impossible to

---

6 The argument can be made that some specific types of unsolicited email advertisements may be beneficial. Indeed, Congress seems to hold this view. See note 32.

Whatever its problems, spam works. American consumers spent $50 billion shopping online in 2003. See *US Online Sales Hit $50bn in 2003*, BBC News (Feb 23, 2004), online at http://news.bbc.co.uk/2/hi/business/3515287.stm (visited Nov 14, 2004). Of that amount, one industry study found that consumers spent a full $11.7 billion on products purchased as a direct result of unsolicited email advertisements. See Peter A. Johnson and Lee Johnson, *The Growing Value of Legitimate Commercial E-Mail: Consumer Purchases and Savings in 2003* (Direct Marketing Association White Paper Feb 24, 2004), online at http://www.the-dma.org/cgi/registered/whitepapers/commercial_email.pdf (visited Nov 14, 2004) (examining the impact of email advertising on consumers' spending habits).

This Comment nevertheless assumes that most types of spam pose substantial problems. For a more thorough treatment of the problems spam creates for consumers, businesses, ISPs, and marketers, see Hanah Metchis and Solveig Singleton, *Spam, That Ill o' the ISP: A Reality Check for Legislators* 4–7 (Competitive Enterprise Institute May 2003), online at http://www.cei.org/gencon/025,03482.cfm (visited Nov 14, 2004).

7 See Part II and Appendix.

8 Restrictions on Unsolicited Commercial E-Mail Advertisers, 2003 Cal Legis Serv 487 (West), codified at Cal Bus & Prof Code § 17529–17529.9 (West 1997 & Supp 2004); 11 Del Code Ann §§ 937–38 (2001). See text accompanying note 49.

9 Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, Pub L 108-187, 117 Stat 2699 (2003), codified at 15 USC § 7701 et seq (Supp 2004) and 18 USC § 1037 (Supp 2004) ("CAN-SPAM").

10 See, for example, Jonathan Krim, *Spam Is Still Flowing into E-Mail Boxes: Senders Evade Federal Law Banning Junk Messages*, Wash Post E1 (Jan 6, 2004):

> At California-based Postini Inc., which provides e-mail protection and filtering for businesses, spam reached a new high [the week the Act went into effect], accounting for 84.9 percent of the roughly 1 billion pieces of e-mail it handles each week. . . . At Brightmail Inc., the leading spam-filtering company, the number has held steady at about 60 percent of the e-mail it handles. Internet account providers Earthlink and America Online said they also have seen little measurable change in spam patterns in the past couple of weeks.

MX Logic, a company that produces email security software, found that seven months after the law went into effect only *1 percent* of spam messages complied with CAN-SPAM. Howard Witt, *22-Year-Old Thrives in World of Spam: Law Fails to Stop Flood of E-Mails*, Chi Trib C1 (July 18, 2004) (citing an MX Logic study of 250,000 emails). The largest share of the world's spam continues to come from the United States. See note 129.

track down senders.[11] Senders themselves are sometimes located overseas. Even when one can track down an individual sender, it requires substantial effort due to the techniques senders use to hide their identities.[12] These technical obstacles make the cost of tracking down a relatively skilled spam sender fairly high.

Were these technical obstacles surmounted, though, the CAN-SPAM Act might nevertheless have little effect on spam, because the federal law is relatively weak—weaker on spam than some state laws, and weaker than many experts had hoped.[13] Although a strong case can be made that spam should be banned outright,[14] the CAN-SPAM

---

11 One potential solution is to target the client of the spammer—the business whose product or service is being advertised. Most spam exists to sell something. If such a sale takes place, then money must change hands, typically through a credit card transaction. It is thus fairly easy for authorities to determine the recipient of the money and track down one party responsible for the spam. The National Cyber-Forensics and Training Alliance, a nonprofit organization that cooperates with the FBI to investigate spammers, has used this strategy successfully. See Saul Hansell, *Junk E-Mail and Fraud Are Focus of Crackdown*, NY Times C1 (Aug 25, 2004). If the client is a business located outside of the United States, however, then it would be beyond the reach of U.S. law. The United States could make it illegal for credit card companies to do business with foreign businesses that violate U.S. spam laws, but both U.S. credit card companies and foreign states are likely to oppose any such action, and in any event placing the burden on credit card companies to determine whether their merchants use spam is unlikely to be politically or practically feasible.

12 One particularly worrisome development was first presented by the MyDoom computer worm, which caused more than $250 million in damage in January 2004. Andrew Stein, *Microsoft Offers MyDoom Reward: No. 1 Software Firm Offers $250,000 for Information on Creator of Worm Seen Costing Firms $250M*, CNN/Money (Jan 30, 2004), online at http://money.cnn.com/2004/01/28/technology/mydoom_costs/index.htm (visited Nov 14, 2004) (listing lost productivity and clean-up expenses as the main costs of MyDoom). The worm included its own mail server, which could send email from the infected computer without the owner's knowledge. Experts believe that the worm's development was funded by spammers as an experiment; once infected, a computer could be programmed to start sending spam messages when a certain trigger event occurred. Even if one could track down the sender, then, it would lead to an infected personal computer rather than a server operated by the spam sender. See Bill Husted, *Latest Worm Has Professional Twist: Computer Experts Blame Spammers*, Atlanta J & Const B1 (Jan 28, 2004) (describing the chances of shutting down MyDoom as "virtually zero").

13 See Stephanie Schorow, *Enlarged Spam Law Has Many Frustrated*, Boston Herald 38 (Jan 7, 2004) (quoting a representative of the Coalition Against Unsolicited Commercial Email as saying CAN-SPAM "is just a bad law. . . . [I]t fails the most basic test. It doesn't tell anybody not to spam."); Spamhaus Project, *United States Set to Legalize Spamming on January 1, 2004* (Nov 22, 2003), online at http://www.spamhaus.org/news.lasso?article=150 (visited Nov 14, 2004) (discussing the relative weakness of CAN-SPAM).

14 Perhaps the most obvious argument for banning spam is that doing so corrects a market defect. Sending spam has essentially zero marginal cost for the sender. At the same time, there are substantial costs that are borne by recipients, ISPs, and other third parties. See Metchis and Singleton, *Spam, That Ill o' the ISP* at 4–7 (cited in note 6). Because spam imposes substantially greater costs on society than on senders, an inefficiently high quantity of spam will be produced absent regulation. Similar arguments led Congress to ban unsolicited fax advertisements. See note 33.

A ban is not the only way to solve the market failure problem. Ian Ayres and Matthew Funk instead suggest that spammers be required to pay email recipients for the right to send them

Act ultimately permits some types of spam. More importantly, the Act preempts many stronger state laws, including California's law, which went into effect on January 1, 2004, the same day as the CAN-SPAM Act. It also doesn't provide for a private individual right of action against senders, leaving enforcement of the statute to government officials and ISPs. Despite these factors, however, this Comment argues that the CAN-SPAM Act, when interpreted correctly, leaves key state law provisions in force and is stronger than many antispam activists fear.

Part I of this Comment introduces the CAN-SPAM Act. It summarizes the Act's substantive limits on spam and discusses its preemption provisions. Part II discusses the various attempts by states to regulate spam. It describes the different types of provisions that states have enacted and compares them to the CAN-SPAM provisions. Part III briefly summarizes federal preemption doctrine. Part IV applies this doctrine to the CAN-SPAM Act. It first discusses which state limits on spam are preempted by the Act. It then examines the preemption provisions' effect on state laws' enforcement mechanisms. While many in the industry have assumed that the Act supersedes all state spam laws,[15] this Comment argues that the Act allows key portions of some states' laws to survive. Part V then briefly outlines some implications of this conclusion for spam control policy.

I. THE CAN-SPAM ACT

A. Substantive Provisions of the Act

After several failed attempts,[16] in 2003 Congress enacted the CAN-SPAM Act.[17] The statute applies to email messages with the "primary purpose" of "commercial advertisement or promotion of a

---

unsolicited messages, which would cause spammers to internalize the costs they impose on recipients. See Ian Ayres and Matthew Funk, *Marketing Privacy*, 20 Yale J Reg 77, 135–37 (2003) (discussing ways to ensure consumer privacy from intrusive marketing techniques).

15 For instance, one maker of email marketing software tells potential customers that "[s]ince the CAN-SPAM Act supersedes any and all State-level email laws, it will be *much* easier for you to keep up to date on [complying with anti-spam laws]." Lyris, *Frequently Asked Questions About CAN-SPAM*, online at http://www.lyris.com/CAN-SPAM (visited Nov 14, 2004) (advising clients on ways to avoid legal difficulties under CAN-SPAM).

16 For example, the Netizens Protection Act of 2001, HR 3146, 107th Cong, 1st Sess (Oct 16, 2001), would have required unsolicited emails to include the sender's name and address, and would not have preempted state spam laws. The Unsolicited Commercial Electronic Mail Act of 2001, HR 95, 107th Cong, 1st Sess (Jan 3, 2001), would have banned false email headers, prohibited use of an ISP's facilities to send spam in violation of that provider's policies, and required spam to be labeled as such. For a list of proposed laws that failed to pass, see David E. Sorkin, *Spam Laws*, online at http://spamlaws.com/federal/index.html (visited Nov 14, 2004).

17 117 Stat 2699.

commercial product or service."[18] There are no quantity requirements; its provisions apply any time an advertiser sends an email message.[19]

The Act bans some deceptive practices: it prohibits forged headers[20] and deceptive subject lines.[21] It *does not* generally prohibit false or deceptive messages, although such messages would likely be subject to state deceptive trade practices laws[22] or the Lanham Act's[23] prohibition of unfair competition. The CAN-SPAM Act also lets states enact laws specific to email that prohibit falsity or deception in commercial messages.[24]

The Act also extensively regulates the structure of spam messages and the techniques used to send them. It requires spam to contain a method for recipients to opt out of later messages[25] and to contain identifying information, including the sender's physical mailing address.[26] It also prohibits methods used to build email lists and evade detection, including harvesting addresses from web pages and Usenet newsgroups,[27] using so-called dictionary attacks to send spam to thou-

---

18 CAN-SPAM § 3(2)(a), 117 Stat at 2701. Messages sent to customers with whom the sender has a preexisting business relationship are excluded. Id § 3(17), 117 Stat at 2702. Spammers have already found one possible loophole in this definition: they can send messages with a noncommercial "primary purpose" and a commercial secondary purpose. See Jonathan Krim, *Gates Wants to Give E-Mail Users Anti-Spam Weapons*, Wash Post E1 (Jan 27, 2004) (noting one message that claims: "The primary purpose of this email is to deliver you a 'Crazy USA State Law of the Week'—The secondary purpose of this email is to let you know: Click Here to Email Advertise Your Web Site to 1,850,000 OPT-IN Email Addresses for FREE!").

19 CAN-SPAM § 4(a)(1), 117 Stat at 2703.

20 Id § 5(a)(1), 117 Stat at 2706. The headers of an email message are the parts other than the message body, including the to and from addresses, subject, date and time stamp, and information showing the path the message took before arriving in its recipient's inbox. The CAN-SPAM Act defines "header information" to be "the source, destination, and routing information attached to an electronic mail message, including the originating domain name and originating electronic mail address, and any other information that appears in the line identifying, or purporting to identify, a person initiating the message." CAN-SPAM § 3(8), 117 Stat at 2701. See also Internet Engineering Task Force Network Working Group, *Internet Message Format* § 2.2 (Apr 2001), online at http://www.ietf.org/rfc/rfc2822.txt (visited Nov 14, 2004).

21 CAN-SPAM § 5(a)(2), 117 Stat at 2706.

22 The National Conference of Commissioners on Uniform State Laws (NCCUSL) has published the Revised Uniform Deceptive Trade Practices Act (NCCUSL 1966) (recommending money damages for victims of fraud or other unfair trade practices). At least thirty-six states adopted legislation similar to the Uniform Act. William A. Lovett, *State Deceptive Trade Practice Legislation*, 46 Tulane L Rev 724 (1972) (listing states that have made "deceptive acts or practices" unlawful). See, for example, 6 Del Code Ann § 2532 et seq (2004) (setting a $10,000 cap on money damages for deceptive trade practices); 815 ILCS 510/1–7 (West 2004) (adopting the Uniform Act). See also Jonathan A. Sheldon, *Unfair and Deceptive Acts and Practices* (National Consumer Law Center 5th ed 2001) (detailing states' deceptive practices acts).

23 15 USC § 1125 (2000).

24 See Part IV.A.

25 CAN-SPAM § 5(a)(3)(A), 117 Stat at 2707.

26 Id § 5(a)(5)(B)(iii), 117 Stat at 2708.

27 Id § 5(b)(1), 117 Stat at 2708.

sands of possible email addresses,[28] automatically creating multiple email accounts for the purpose of sending spam messages,[29] and transmitting messages through third-party computers without authorization.[30] Finally, the Act authorizes (but does not require) the Federal Trade Commission (FTC) to establish a "do not email" registry, similar to the "do not call" list for telemarketing.[31]

The law is thus relatively comprehensive: it includes nearly every *type* of antispam measure that the state laws include, short of an outright ban on spam. Ultimately, though, it falls short of what many antispam activists believe is needed to combat spam:[32] the law permits

---

28 Id. A dictionary attack consists of sending mail to email addresses generated from a word list, such as a list of all the words in a dictionary. For example, an advertiser could send a message to a@domain.com, aardvark@domain.com, abacus@domain.com, and so forth, working her way through the list. For an even more effective address list, a spammer would also use a list of common usernames, such as combinations of first and last names. Anyone who has an email address on the resulting list will get the spam message, even if that email address is not otherwise known to the public. This method is massively overinclusive—most of the resulting email addresses will lead nowhere—but the economics of spam make it worthwhile. See Michelle Delio, *Hotmail: A Spammer's Paradise?*, Wired News (Jan 9, 2003), online at http://www.wired.com/news/infostructure/0,1377,57132,00.html (visited Nov 14, 2004).

29 CAN-SPAM § 5(b)(2), 117 Stat at 2709.

30 Id § 5(b)(3), 117 Stat at 2709.

31 Id § 9, 117 Stat at 2716. The "do not call" list permits individuals to register as not wishing to receive telemarketing calls on their home and wireless telephones. The registry is established by 47 CFR § 64.1200(c)(2) (2003) (setting a five-year do-not-call period for registrees). The Tenth Circuit rejected First Amendment and other challenges to the regulation in *Mainstream Marketing Services, Inc v FTC*, 358 F3d 1228 (2004), cert denied, 125 S Ct 47 (2004) (holding that the do-not-call list was valid because it advanced the government's interest in safeguarding personal privacy).

The Tenth Circuit relied in part on *Rowan v United States Post Office Department*, 397 US 728 (1970) (upholding the right of a homeowner to reject receipt of certain materials through the mail), in upholding the do-not-call list. *Mainstream Marketing Services*, 358 F3d at 1237. The plaintiff in *Rowan* challenged a law that permitted recipients of sexual advertisements via mail to opt out of receiving further advertisements from the same senders. The Court dismissed the challenge, reasoning:

> The Court has traditionally respected the right of a householder to bar, by order or notice, solicitors, hawkers, and peddlers from his property. . . . To hold less would tend to license a form of trespass and would make hardly more sense than to say that a radio or television viewer may not twist the dial to cut off an offensive or boring communication and thus bar its entering his home.

Rowan, 397 US at 737. See also note 33.

32 See, for example, Schorow, *Enlarged Spam Law*, Boston Herald at 38 (cited in note 13); Spamhaus Project, *United States Set to Legalize Spamming* (cited in note 13). Indeed, one common joke in antispam circles called the law the YOU-CAN-SPAM Act. Id.

The best explanation for the Act's relative weakness is that Congress does not appear to consider all spam to be bad. The Senate committee that recommended passing the Act distinguished between seemingly legitimate spam and fraudulent or misleading spam:

> Unlike direct mail delivered through the post office to consumers, [unsolicited commercial e-mail] can reach millions of individuals at little to no cost and almost instantaneously. Noting its effectiveness, the Direct Marketing Association has reported that 37 percent of con-

spam within certain parameters, while many experts had argued that only a complete ban on bulk unsolicited commercial email would effectively curb the spam problem.[33] In addition, many of the Act's specific provisions fall short of some states' parallel restrictions.[34]

The Act includes criminal provisions[35] and permits civil enforcement by state and federal agencies,[36] by state attorneys general,[37] and by ISPs.[38] Private citizens and businesses receiving spam messages that violate the Act are not granted any enforcement power. Thus far, state and federal authorities have taken only limited action under the law. In April 2004, four people were arrested and charged with, among

---

> sumers it surveyed have bought something as a result of receiving unsolicited e-mail from marketers. However, in addition to legitimate businesses that wish to use commercial e-mail as another channel for marketing products or services, spam has become a favored mechanism of those who seek to defraud consumers and make a living by preying on unsuspecting e-mail users and those new to the Internet. As a result, Americans using e-mail, whether new users or those who have used it for decades, are finding their e-mail in-boxes deluged with unsolicited, and in most instances unwanted, promotions and advertisements that increasingly contain fraudulent and other objectionable content.

CAN-SPAM Act of 2003, S Rep No 108-102, 108th Cong, 1st Sess 2 (2003), reprinted in 2004 USCCAN 2348, 2349.

33 There is precedent for a complete ban. In the analogous case of unsolicited advertisements sent by fax, Congress chose a complete ban. See Telephone Consumer Protection Act of 1991, Pub L No 102-243, 105 Stat 2394, codified as amended at 47 USC § 227 (2000) (TCPA) (banning most junk faxes and permitting recipients to sue the sender for the greater of actual damages or $500). In 2003 the Eighth Circuit upheld the TCPA against a First Amendment challenge. *Missouri v American Blast Fax, Inc*, 323 F3d 649 (8th Cir 2003). The court held that the government has a substantial interest in preventing the cost shifting and interference with recipients' fax machines associated with junk faxes, and that the ban was in proportion to that interest and was narrowly tailored to that interest. See id at 656–58.

A similar argument might apply to spam. Most end users pay for their internet connection, and so a significant portion of the cost of spam is shifted to users. Likewise, the torrent of spam interferes with recipients' ability to use email productively. The argument is yet more forceful with ISPs, which incur substantial bandwidth and filtering costs as a result of spam. If lesser measures are not successful—and all signs so far indicate that they are not—then a ban could be the least restrictive means of achieving a substantial government objective.

Some spam opponents have argued that the junk fax ban can be used to sue email spammers as well. See, for example, Paul Festa, *Spam Law a Matter of Fax?*, CNET News.com (Mar 26, 2003), online at http://news.com.com/2100-1028-994076.html (visited Nov 14, 2004). At least one court has rejected this argument. See *Aronson v Bright-Teeth Now, LLC*, 2003 Pa Super 187, 824 A2d 320, 321–22 (2003) (reasoning that a personal computer does not meet the definition of fax machine under the TCPA). See also David E. Sorkin, *Unsolicited Commercial E-Mail and the Telephone Consumer Protection Act of 1991*, 45 Buff L Rev 1001 (1997) (concluding that although a spam message might technically meet the wording of the law, Congress clearly did not intend for the anti–junk fax law to apply to email).

34 See Part II.

35 CAN-SPAM § 4(a), 117 Stat at 2705.

36 Id § 7(a)–(d), 117 Stat at 2711–12.

37 Id § 7(f), 117 Stat at 2712–14.

38 Id § 7(g), 117 Stat at 2714–15.

other crimes, violating the CAN-SPAM Act.[39] A few ISPs have also filed lawsuits.[40]

The Act's ISP enforcement provision, in particular, could be a strong tool against spam. It provides for statutory damages of up to $100 per false or misleading message received, up to $1 million total.[41] If the defendant violated the law "willfully and knowingly," then the plaintiff can recover treble damages.[42] The Act also allows courts discretion to award attorneys' fees.[43] Accordingly, a large ISP like AOL, which receives billions of spam messages per year,[44] could take action against some of the largest senders; this could deter other senders. Enforcement by spam recipients presents a collective action problem that ISPs might be in the best position to solve. ISPs face substantial costs from spam, and they have the resources to track down senders and take them to court. ISPs also have incentives to do so, since they can compete for customers on the basis of how much spam they receive.[45]

B. The Act's Preemption Provision

Section 8(b)(1) of the Act addresses preemption of state laws. It states:

> This Act supersedes any statute, regulation, or rule of a State or political subdivision of a State that expressly regulates the use of electronic mail to send commercial messages, except to the extent

---

39 See Hiawatha Bray, *Federal Antispam Law to Be Put to Its First Test*, Boston Globe A1 (Apr 29, 2004) (describing federal charges against four Michigan men who allegedly used email to sell fraudulent weight-loss products).

40 See Saul Hansell, *4 Big Internet Providers File Suits to Stop Leading Senders of Spam*, NY Times A1 (Mar 10, 2004) (describing lawsuits by AOL, EarthLink, Microsoft, and Yahoo against alleged spammers, including a "former leader of a neo-Nazi organization who turned to selling penis enlargement pills"). See also *Handyman Celebrity's Web Site Sued for Sending Spam*, Natl J Tech Daily, AM Ed (Mar 5, 2004) (reporting that a small ISP sued the operator and marketer of BobVila.com for allegedly sending email ads to consumers who had opted out of the site's email list).

41 CAN-SPAM § 7(g)(3)(A)–(B), 117 Stat at 2715.

42 Id § 7(g)(3)(C), 117 Stat at 2715.

43 Id § 7(g)(4), 117 Stat at 2715.

44 See note 5 and accompanying text.

45 Another potential solution to the collective action problem would be allowing class action lawsuits against spam senders. This mechanism is not available under the CAN-SPAM Act, but could be permitted by a state law. ISPs themselves face their own collective action problem: any action an ISP takes that successfully reduces the level of spam for the entire internet would pass the vast majority of its benefits onto other ISPs and their customers. We should accordingly expect ISPs to take too few actions under any law governing spam. But see Hansell, *4 Big Internet Providers File Suits to Stop Leading Senders of Spam*, NY Times at A1 (cited in note 40). The obvious solutions to the collective action problem are government enforcement, enforcement by coalitions of ISPs or industry organizations, and enforcement by consumer groups. CAN-SPAM embraces the first two tactics, CAN-SPAM § 7, 117 Stat at 2712–15, but ignores the third.

> that any such statute, regulation, or rule prohibits falsity or deception in any portion of a commercial electronic mail message or information attached thereto.[46]

The provision has two parts. The portion up to "except" defines the outer boundary of preempted state laws: any state law "that expressly regulates the use of electronic mail to send commercial messages" is at least potentially preempted, while any that does not is not. The latter portion of the provision—the savings clause—protects state laws that otherwise would be preempted if they fall into certain categories.

The hard question in determining the scope of the entire provision is the scope of its savings clause. Section 8(b)(1) expressly preserves state laws that prohibit "falsity or deception in any portion of a commercial electronic mail message or information attached thereto." This clause could be interpreted in multiple ways, and how it is interpreted will have a substantial effect on states' ability to target spam. The section's effect on state law enforcement methods is also unclear.

The provision clearly preempts a substantial portion of state spam laws. For instance, the broadest provision of California's law, which went into effect January 1, 2004, and would have banned sending any commercial email advertisement without the recipient's direct consent,[47] is clearly preempted. California's statute expressly regulates the use of electronic mail, and it goes far beyond prohibiting falsity or deception. At the same time, many more narrowly drawn state laws survive, and it is these provisions that must be effective against spam.

In analyzing the effects of the preemption provision, then, it is helpful to know what kinds of laws have been passed to deal with commercial electronic mail.

II. STATE REGULATION OF SPAM

By the time the CAN-SPAM Act went into effect, thirty-six states had enacted some sort of law explicitly regulating commercial email.[48] These laws vary widely in scope, from simply requiring that vendors label the spam they send to banning all spam messages sent without explicit consent. This Part details the categories of substantive rules that states have enacted.

Opt-in provisions. Opt-in provisions require that a recipient specifically choose to receive messages. These provisions are the

---

46 CAN-SPAM § 8(b)(1), 117 Stat at 2716.

47 Cal Bus & Prof Code § 17529.2.

48 For an invaluable reference for all state and federal spam laws, I am indebted to David E. Sorkin, *Spam Laws* (cited in note 16).

strongest antispam laws and have been enacted by two states.[49] They are clearly preempted by the CAN-SPAM Act, as they "expressly regulate[] the use of electronic mail to send commercial messages" without falling into the exception for laws prohibiting falsity or deception.[50]

Opt-out provisions. Opt-out provisions require that spam senders include a mechanism allowing email users to opt out of later messages and require senders to comply with these requests. Typical opt-out mechanisms include a reply email address, a toll-free telephone number, or a web form. These provisions are key parts of most antispam laws, and they exist in twenty-one states, though different states require different opt-out mechanisms. The CAN-SPAM Act's opt-out provision is relatively weak compared to some of the state provisions, which it preempts.

Bans on false or misleading subject lines, false routing information, and the use of false third-party return addresses or domain names. These are the other key provisions in most antispam laws. Thirty-two states ban at least one type of false or misleading information in spam; twenty ban all three. These provisions are explicitly saved from preemption (and largely duplicated) by the CAN-SPAM Act, as they are state laws against "falsity or deception in any portion of a commercial electronic mail message or information attached thereto."[51]

Subject-line labeling requirements. Twenty-two states require spam labels at the beginning of the subject line, typically with a label like "ADV" (for advertisement) for all spam messages or "ADV:ADLT" for adult messages.[52] Labels would permit easy filtering of spam messages from a user's inbox, but the CAN-SPAM Act preempts state laws that require such labeling. The Act itself has no labeling requirement, instead requiring "clear and conspicuous identification that the message is an advertisement or solicitation," though not necessarily in the subject line.[53] This provision's lack of specificity makes it much harder to filter messages based on the required identification: under CAN-SPAM, email recipients cannot block all spam by telling their software to block all messages containing "ADV" in the

---

49 See Cal Bus & Prof Code § 17529.2; 11 Del Code Ann §§ 937–38. This and the subsequent counts are based on the author's compilation. For a full list of states having each type of provision, see Appendix. The spam laws themselves can be found at Sorkin, *Spam Laws* (cited in note 16).

50 CAN-SPAM § 8(b)(1), 117 Stat at 2716.

51 Id.

52 See, for example, Alaska Stat § 45.50.479(a) (Michie 2003) (requiring "ADV:ADLT" for spam containing "explicit sexual material"). Four states require labeling only spam with adult content. Six states require a single label for all spam, adult and otherwise. Twelve states require labels for all spam, and more specific labels for spam with adult content. See Appendix.

53 CAN-SPAM § 5(a)(5)(A)(i), 117 Stat at 2708.

header. Although the Act has no labeling requirement, it does grant the FTC rulemaking authority to implement the Act.[54] The FTC recently announced a requirement that sexually explicit spam be labeled "SEXUALLY-EXPLICIT" in the subject line.[55]

Contact information requirements. Fifteen states require that spam messages contain some contact information for the sender: a name, email address, mailing address, or phone number. These provisions vary greatly in what is required. The CAN-SPAM Act preempts these provisions but requires that messages contain a physical postal address.[56]

Bans on selling software that can be used to falsify routing information. Fifteen states ban the sale of software designed to falsify routing information or return addresses. The CAN-SPAM Act preempts only state laws that "expressly regulate[] the use of electronic mail to send commercial messages."[57] Because these provisions apply to the software, and the act of selling it, rather than to email, they should be unaffected by the Act.[58] They are also relatively powerless: they prohibit the upstream act of selling the software, which won't prevent senders from using it.

Bans on violating ISP policies. Nine states prohibit, to one degree or another, violations of an ISP's terms of service.[59] These provisions are intended to give the force of law to an ISP's prohibitions on sending spam. Their effectiveness in controlling spam is not clear for several reasons. First, few states have these provisions. Second, they apply only if an ISP prohibits sending spam. Not all ISPs will necessarily do so: while widespread adoption of such policies could lead to spammer-friendly internet access selling for a premium, thus discouraging some spam by increasing the costs of sending it, even such elevated prices would nevertheless be less than the social harm from spam, leaving an inefficiently high level of spam. Finally, these laws don't apply to spam sent from overseas or through hijacked computers, sources that account for a substantial portion of spam. These

---

54 Id § 13, 117 Stat at 2717.

55 Federal Trade Commission, Label for E-Mail Messages Containing Sexually Oriented Material, 69 Fed Reg 21024 (2004) (final rule) (creating 16 CFR § 316.1). See also Marilyn Geewax, *Feds: Smutty Spam Must Carry New Label*, Atlanta J & Const D1 (Apr 14, 2004) (noting an FTC estimate that 17 percent of pornographic emails contain graphic images "that appear whether or not the user wants to see them").

56 CAN-SPAM § 5(a)(5)(A)(iii), 117 Stat at 2708.

57 Id § 8(b)(1), 117 Stat at 2716.

58 See Part IV.A.

59 For an example of an ISP's service terms, see EarthLink, Inc, *EarthLink Internet Service Agreement* § 3 (Oct 1, 2004), online at http://www.earthlink.net/about/policies/dial (visited Nov 14, 2004) ("Using a dial-up account for high volume or commercial use (e.g., revenue generation, advertising, etc.) is prohibited.").

laws are unaffected by the CAN-SPAM Act because they do not "expressly regulate[] the use of electronic mail to send commercial messages."[60]

States enforce all of these various substantive limits in a variety of ways, from government or ISP enforcement actions (which have parallels in the CAN-SPAM Act), to private lawsuits by spam recipients (which are not mentioned in the Act), and criminal penalties (which exist in the Act, but only in limited form).[61] The preemption effect of the CAN-SPAM Act on these state-level enforcement provisions is unclear; the Act's preemption provisions explicitly address only substantive limits. In Part IV.B, I argue that, despite the seemingly broad language of its preemption provisions, the Act has no limit on state enforcement provisions that differ from the federal limits.

III. A BRIEF TOUR OF FEDERAL PREEMPTION DOCTRINE

The United States Constitution establishes that when valid federal and state laws conflict, the federal law has force.[62] Federal law preempts state law in two primary ways.[63] First, Congress can preempt state laws explicitly, with an express preemption clause. Second, even absent any clear direction from Congress, a federal law may implicitly preempt state laws. The Supreme Court has found two broad categories of implicit preemption: when the federal regulation is "so pervasive as to make reasonable the inference that Congress left no room for the States to supplement it,"[64] a category known as field preemption; and when the state law conflicts with or "stands as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress,"[65] a category known as conflict preemption. Laurence

---

60 CAN-SPAM § 8(b)(1), 117 Stat at 2716.

61 For a state-by-state summary of state enforcement methods, see Appendix.

62 US Const Art VI, cl 2 ("This Constitution, and the Laws of the United States which shall be made in Pursuance thereof . . . shall be the supreme Law of the Land."). See also *McCulloch v Maryland*, 17 US (4 Wheat) 316, 406 (1819) ("The government of the United States . . . though limited in its powers, is supreme; and its laws, when made in pursuance of the constitution, form the supreme law of the land, 'any thing in the constitution or laws of any State to the contrary notwithstanding.'"); *Gibbons v Ogden*, 22 US (9 Wheat) 1, 211 (1824) (holding that "acts of the State Legislatures . . . [that] interfere with, or are contrary to the laws of Congress" are nullities because "[i]n every such case, the act of Congress . . . is supreme; and the law of the State, though enacted in the exercise of powers not controverted, must yield to it").

63 On federal preemption generally, see Erwin Chemerinsky, *Constitutional Law: Principles and Policies* § 5.2 at 376–401 (Aspen 2d ed 2002); Laurence H. Tribe, 1 *American Constitutional Law* § 6-28 at 1172–79 (Foundation 3d ed 2000).

64 *Rice v Santa Fe Elevator Corp*, 331 US 218, 230 (1963) (holding that Congress intended a federal law regulating grain warehouses to supersede state warehouse regulations).

65 *Hines v Davidowitz*, 312 US 52, 67–74 (1941) (holding that federal immigration law preempted a Pennsylvania law requiring registration of legal aliens because the state law may

Tribe characterizes these two types of preemption as jurisdictional and substantive, respectively.[66] In the former case Congress intends to be the sole regulator, even when the state and federal laws would otherwise be entirely consistent, while in the latter case the state is substantively interfering with the federal purpose.

A. Express Preemption

The clearest preemption cases are those interpreting express preemption clauses. In those instances, determining the scope of the preemption clause is a straightforward matter of statutory construction. Even when Congress has explicitly preempted state laws, though, the scope of that preemption is rarely clear. As Erwin Chemerinsky has noted, "provisions in federal statutes expressly preempting state and local laws inevitably require interpretation as to their scope and effect."[67]

For instance, the Public Health Cigarette Smoking Act of 1969 provided: "No requirement or prohibition based on smoking and health shall be imposed under State law with respect to the advertising or promotion of any cigarettes" meeting the law's labeling requirements.[68] The Supreme Court in *Cipollone v Liggett Group, Inc*[69] held that this reasonably straightforward provision preempted application of state tort law to cigarette manufacturers but left in place a claim for breach of express warranties.[70] The Court reasoned that the warranty obligations were created by contract, not by state law, and so were not within the scope of the state law that Congress had intended to preempt.[71]

The Court in *Cipollone* applied its longstanding assumption that, because the states' general police powers are so well established, any intention by Congress to supplant that authority must be shown by the "clear and manifest purpose of Congress."[72] Indeed, the Court is reluctant to infer preemption in ambiguous cases, but instead rests on the presumption that "Congress did not intend to displace state law."[73] Congress has the ability to make its intention to preempt clear, and so

---

have resulted in "inquisitorial practices and police surveillances that might . . . affect our international relations").

66 Tribe, 1 *American Constitutional Law* § 6-28 at 1177 (cited in note 63).

67 Chemerinsky, *Constitutional Law* § 5.2.2 at 383 (cited in note 63).

68 Pub L No 91-222, 84 Stat 87, 88, codified at 15 USC § 1334 (2000).

69 505 US 504 (1992).

70 Id at 526 (Stevens plurality).

71 Id at 525–26.

72 Id at 516 (majority), quoting *Rice*, 331 US at 230.

73 *Maryland v Louisiana*, 451 US 725, 746 (1981) (holding that federal law preempted a Louisiana tax on natural gas).

when there is no explicit preemption clause it is reasonable to assume that Congress did not intend to preempt.

However, in another tobacco case, *Lorillard Tobacco Co v Reilly*,[74] the Court interpreted the same provision at issue in *Cippollone* to preempt a Massachusetts law banning outdoor cigarette advertising near schools. The Court reasoned that Congress had in several ways attempted to protect the public from the danger of minors smoking and had vested the authority to regulate advertising in the FTC.[75] While the preemption clause was the direct authority to find preemption, the Court arguably went further and invoked field preemption, inferring congressional intent to regulate comprehensively from amendments expanding the federal advertising regulation and from the scope of the regulations.[76] The dissent argued that the Massachusetts law regulated only the location of the advertisement, not its content, and therefore the law didn't constitute a requirement or prohibition based on smoking and health.[77]

Lorillard illustrates that applying preemption clauses requires ordinary statutory interpretation, but it also shows that the categories of preemption can overlap: a statute could expressly preempt a category of state laws, and yet also implicitly preempt state laws more broadly.[78] Understanding the preemptive effect of a federal law thus requires determining the result under both explicit and implicit preemption analysis.

B. Field Preemption

The Court has struck down state laws when Congress has evidenced a desire to occupy the entire field of regulation. The classic field preemption case is *Rice v Santa Fe Elevator Corp*,[79] which held that states cannot regulate grain elevators licensed by the federal government. The Court reasoned that by replacing a system of dual regulation with one in which grain elevators needed only federal licensing,

---

74 533 US 525 (2001).

75 Id at 547–49.

76 Id at 547–48.

77 Id at 595–98 (Stevens dissenting).

78 As Laurence Tribe notes:

> These three categories of preemption are anything but analytically air-tight. For example, even when Congress declares its preemptive intent in express language, deciding exactly *what* it meant to preempt often resembles an exercise in implied preemption analysis. So too, implied preemption analysis is inescapably tied to the presumption that Congress did not intend to allow state obstructions of federal policy, the existence of which is a central inquiry in conflict preemption analysis.

Tribe, 1 *American Constitutional Law* § 6-28 at 1177 (cited in note 63).

79 331 US 218 (1963).

Congress intended to eliminate state requirements on those grain elevators, despite its failure to say so explicitly.[80] Congress, the Court concluded, intended to occupy the field of grain elevator regulation for federally licensed elevators, and so any state regulation was preempted.[81]

Likewise, in *City of Burbank v Lockheed Air Terminal, Inc*,[82] the Court held that the Federal Aviation Act preempted local aircraft noise regulations. The Court explained, "It is the pervasive nature of the scheme of federal regulation of aircraft noise that leads us to conclude that there is preemption."[83] Such a pervasive scheme of federal regulation seems to be a threshold requirement to find field preemption, but the law is far from clear: the Court has declined to find preemption even in some cases of substantial federal regulation.[84]

C. Conflict Preemption

Finally, the Court has held that a state law is preempted if it "stands as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress."[85] The simplest case arises when the state and federal laws conflict such that one could not simultaneously comply with both the state and federal laws, as in *McDermott v Wisconsin*.[86] Federal law required that cans of syrup be sold in their original packaging,[87] while Wisconsin law required that they be sold only in state-approved packaging.[88] Because a retailer could not comply with both laws, the state law was preempted.[89]

A more difficult determination is whether a state law obstructs the accomplishment of a federal objective when the two laws do not directly conflict.[90] Two determinations must be made in such cases:

---

80 Id at 234–36.

81 Id at 235–36.

82 411 US 624 (1973).

83 Id at 633.

84 See Chemerinsky, *Constitutional Law* § 5.2.3 at 388–91 (cited in note 63) (discussing cases involving blood donation, music piracy, and welfare, where the Court declined to find preemption).

85 *Hines*, 312 US at 67. See also Chemerinsky, *Constitutional Law* § 5.2.5 at 394–98 (cited in note 63).

86 228 US 115 (1913).

87 Id at 130.

88 Id at 124–27.

89 Id at 132–34.

90 A prototypical case is *Nash v Florida Industrial Commission*, 389 US 235 (1967), which held that a state law that denied unemployment benefits to those who filed a complaint with the National Labor Relations Board (NLRB) was preempted by the federal statute establishing the NLRB. A purpose of the federal statute was to encourage such filings, and a state law that penalized them stood as an obstacle to that purpose.

what the purpose of the federal law is, and whether the state law hinders that purpose. The question often arises in cases of federal laws setting safety or environmental standards, when the Court must determine whether Congress's goal is to provide comprehensive, uniform, nationwide standards or simply to provide minimum standards. In the former case, stricter state laws conflict with the federal purpose and are thus preempted, while in the latter case the two laws are compatible.[91] These cases often turn, then, on the court's characterization of the federal purpose. As Chemerinsky has noted:

> If a court wants to avoid preemption, it can narrowly construe the federal objective and interpret the state goal as different from or consistent with the federal purpose. But if a court wants to find preemption, it can broadly view the federal purpose and preempt a vast array of state laws.[92]

To determine the preemptive effect of the CAN-SPAM Act, then, this Comment analyzes both the impact of the express preemption clause and the impact of the Act according to implicit preemption doctrine, both with respect to field preemption and conflict preemption. The Act's express preemption clause clearly preempts many, perhaps most, state spam laws.[93] At the same time, the clause presents some puzzles of interpretation. These questions are the focus of Part IV.

IV. APPLYING THE PREEMPTION CLAUSE OF THE CAN-SPAM ACT

A state law that limits spam presents two potential questions of effect. First, the state law's substantive provisions might fall within the scope of the CAN-SPAM Act's preemption clause (and not be saved by the savings clause). Second, even if a state law regulated the kind of conduct that the CAN-SPAM Act explicitly permits states to regulate, the Act might nevertheless limit the enforcement mechanisms available to a state. This Part addresses these two issues in turn, and then considers some implications of the preemption clause's scope.

---

91 Compare *Gade v National Solid Wastes Management Association*, 505 US 88 (1992) (holding that an Illinois law protecting workers who handled hazardous waste was preempted by the Occupational Safety and Health Act (OSHA), in part because OSHA had procedures for state regulations to supplant federal ones on approval from the federal government), with *Pacific Gas & Electric Co v State Energy Resources Conservation and Development Commission*, 461 US 190 (1983) (holding that a California moratorium on the construction of nuclear power plants was not preempted because its motivation was economics, not safety).

92 Chemerinsky, *Constitutional Law* § 5.2.5 at 398 (cited in note 63).

93 See Part I.B.

A. Effect of the Preemption Clause on Substantive State Spam Laws

The CAN-SPAM Act "supersedes any statute, regulation, or rule . . . that expressly regulates the use of electronic mail to send commercial messages, except to the extent that any such statute, regulation, or rule prohibits falsity or deception in any portion of a commercial electronic mail message or information attached thereto."[94] This language, while seemingly clear, leaves some questions unanswered. First, which laws "expressly regulate[] the use of electronic mail to send commercial messages"? Second, when do such laws "prohibit[] falsity or deception in any portion of a commercial electronic mail message or information attached thereto"? Section 8(b) preempts a category of state laws, but carves out a subset that is exempt from preemption. The first question, then, determines the outer boundaries of the preemption clause, while the second determines the scope of its savings clause.

The answer to the first question seems clear. Laws that expressly regulate "the use of electronic mail to send commercial messages" will expressly mention electronic mail. General laws that apply more broadly than to spam—general bans on deceptive trade practices, for instance—remain unaffected. Likewise, the preemption clause is limited to laws that apply to "commercial" email. Were a state to pass a law regulating all email, commercial or otherwise, it would not be affected by the CAN-SPAM Act (though it would potentially face other constitutional hurdles).

Perhaps more interestingly, the preemption clause applies only to laws that regulate the *use* of electronic mail, not to ancillary activities related to email. Laws that might be narrowly tailored to combating spam, but *not* by regulating its use, fall outside the scope of the preemption clause and therefore are not preempted.

Good examples of this kind of law are state laws that ban the sale of software designed to be used in spamming—to falsify email routing information, for example. Fourteen states have such laws.[95] Connecticut's provision is typical: it prohibits selling or distributing software that is "primarily designed or produced for the purpose of facilitating or enabling the falsification of electronic mail transmission information or other routing information" or is marketed for that purpose.[96] This law does not regulate the *use* of electronic mail any more than a ban on possessing burglary tools regulates the act of breaking into a

---

94 CAN-SPAM § 8(b)(1), 117 Stat at 2716.

95 See text accompanying notes 57–58.

96 Conn Gen Stat Ann § 53-451(c)–(d) (West 2001) (providing criminal penalties up to a class D felony for violations of the statute).

home. The provision therefore does not fall within the scope of the CAN-SPAM Act's preemption clause.

Determining whether a state law "expressly regulates the use of electronic mail to send commercial messages," and thus is (presumptively) preempted by § 8(b), is then a fairly straightforward matter: the law must (1) expressly apply to email (2) that is commercial in nature, and must (3) regulate the *use* of email, not just relate in some way to email. Unless it meets these three criteria, the law is outside the scope of the preemption clause and is therefore unaffected by the CAN-SPAM Act.[97]

Even if a state law does meet these criteria, and thus falls into the scope of the preemption clause, it still survives if it meets the requirements of the savings clause. State laws meeting the three criteria are preempted, except to the extent that they "prohibit[] falsity or deception in any portion of a commercial electronic mail message or information attached thereto."[98]

Congress's primary concern in creating an exception for laws prohibiting "falsity or deception" was to allow states to regulate the use of spam for fraudulent purposes.[99] Though Congress wanted to avoid the problem of conflicting state standards with respect to things like spam formatting, where both "legitimate" and illegitimate commercial email would be affected, it felt no such qualms about fraudulent spam, stating that "[s]tatutes that prohibit fraud and deception in email do not raise the same concern [of inconsistency], because they target behavior that a legitimate business trying to comply with relevant laws would not be engaging in anyway."[100]

The choice, then, is between interpreting the savings clause narrowly, so that it applies only to laws aimed directly at consumer fraud, or more broadly, so that that it applies to any falsity or deception in spam messages. The former interpretation is more consistent with Congress's intent, while the latter is more consistent with the text of the preemption clause.

States have targeted three main areas of falsity or deception in spam: false routing information, false or misleading subject lines, and

---

97 Substantive state limits on spam are still subject to implicit preemption, but they probably would escape preemption under such an analysis. First, the CAN-SPAM Act is not the kind of comprehensive scheme of federal regulation that invokes field preemption. See Part IV.B.2. Second, the Act's preemption clause seems well tailored to capture any state law that conflicts with Congress's objectives. Any law that survives the preemption clause does so largely because it is consistent with those objectives.

98 CAN-SPAM § 8(b)(1), 117 Stat at 2716.

99 See S Rep No 108-102 at 21–22 (cited in note 32).

100 Id.

false return addresses or domain names.[101] Use of falsified routing information to hide the sender's origin is probably not the type of consumer fraud Congress was concerned about. Nevertheless, such behavior is not what "a legitimate business trying to comply with relevant laws" would engage in, and so the inconsistency concern doesn't apply. Congress's intent is even consistent with a state law banning falsity or misleading information in the body of a spam message, but such a law would be broader than any state has gone.

Other potential state laws that arguably target "falsity or deception" in spam might not target the kinds of fraudulent acts Congress was concerned about. For instance, a state could ban the "cloaking" techniques that many spam senders use to get their messages past spam filters.[102] These techniques hardly represent the kind of consumer fraud Congress was worried about. Cloaking techniques are designed to fool spam filters, not consumers; a consumer who viewed such a spam message and bought an advertised product would have been fully aware of the message's nature. These messages are deceptive to a spam filter, but are not necessarily deceptive to the recipient.

The narrow interpretation of the savings clause would hold a law banning cloaking techniques to be preempted, because it is not aimed at the kind of consumer fraud that was Congress's primary concern. At the same time, though, there is no reason for "a legitimate business trying to comply with relevant laws" to use these techniques; they're simply attempts to get one's advertisement to consumers who have taken active steps (or whose ISPs have taken steps) to avoid those ads.[103] It doesn't accomplish any purpose of Congress to hold such a law preempted.

---

101 See text accompanying note 51.

102 Common techniques include putting spaces inside words that would otherwise trip filters ("F R E E"), see *An In-Depth Look at Current Trends in Spamming Techniques*, Security Park (Mar 2, 2004), online at http://www.securitypark.co.uk/article.asp?articleid=22070&CategoryID=33 (visited Nov 14, 2004) (describing the technique as "lost in space"); substituting characters for letters ("\/!A6RA"), see Mitch Wagner, *Spammers' Technology Secrets! Exposed!*, InternetWeek (Feb 13, 2003), online at http://www.internetweek.com/story/showArticle.jhtml?articleID=6900020 (visited Nov 14, 2004) (discussing various spamming techniques); inserting nonsense HTML ("mill‹!-- xe64 -->ionaire") that isn't displayed on the recipient's computer, see id; and using HTML character codes to represent letters (turning "V i a g r a" into "Viagra" on screen), see Leon Erlanger, *Spam War*, PC Mag (Mar 2, 2004) (describing spammers' increasing sophistication). The façade of randomness and innocent words conceals words that would otherwise trip a spam filter.

103 One could argue that attempts to get around filters are not illegitimate. The act of deceiving a filter is not illegal, and techniques used to defeat filters do not mislead consumers. It seems unlikely, however, that Congress believed that argument. The CAN-SPAM Act requires that spam recipients be able to opt out of future messages, CAN-SPAM § 5(a)(3)(A)(i), 117 Stat

Though Congress framed its concern in terms of consumer fraud, its primary concern in enacting the preemption clause was inconsistency in state laws that would make it hard for "legitimate" users of commercial email to operate. Since no legitimate use requires deception, courts should adopt the broad reading of the savings clause so as not to hinder states' ability to regulate illegitimate spam email.

B. State Enforcement Provisions

Another difficulty in applying § 8(b) is determining its effect on state laws that ban falsity or deception in spam (and so are not preempted) but use enforcement mechanisms that differ from the CAN-SPAM Act's enforcement provisions.[104] Two such measures are state criminal penalties and state laws giving recipients of spam a private right of action against spam senders.

For example, Washington State's antispam law prohibits sending commercial email that "(a) [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 of a commercial electronic mail message; or (b) [c]ontains false or misleading information in the subject line."[105] This statute bans commercial email with some false or deceptive content, and accordingly would be preserved under § 8(b)(1). At the same time, though, the statute is enforced by a private right of action against senders violating the law, with minimum damages of $500 per violation for consumers and $1,000 per violation for ISPs.[106]

It may be the case that one of Congress's objectives was to limit spam enforcement, possibly to protect marketers against the threat of thousands of individual lawsuits or class actions. The Act could implicitly limit all antispam enforcement to those limited enforcement measures included in the CAN-SPAM Act, or alternatively to enforcement methods of the same types.[107] Interpreting the preemption clause as an implicit limitation on state enforcement mechanisms, so as to strike the Washington state enforcement measures, might then be

---

at 2707, and Congress would presumably want to likewise honor consumers' efforts to avoid viewing spam messages.

104 See text accompanying notes 35–45.

105 Wash Rev Code Ann § 19.190.020 (West Supp 2004).

106 Id § 19.190.040.

107 Such a division of substantive provisions and remedies would be unusual, but not unprecedented. For example, the Telephone Consumer Protection Act provides for a private cause of action by the recipient of an illegal marketing call but avoids the judicial costs of such lawsuits by only permitting these cases to be brought in state courts under state law. See 47 USC § 227(b)(3). CAN-SPAM's legislative history is silent on the issue of state enforcement of state antispam provisions. See S Rep No 108-102 (cited in note 32).

truest to this intent. At the same time, striking it down could leave the law with no enforcement mechanism. Such a result is unlikely to be what Congress intended: an enforcement mechanism is fundamentally linked to the substantive provision it enforces, and if Congress really wanted to keep only the substantive half it likely would have been more explicit.

Enforcement mechanisms present a more plausible case for implicit preemption than substantive provisions do: even if Congress did not explicitly preempt state law enforcement techniques, it might have intended to limit the *kinds* of enforcement available for use against spam to those compatible with the federal objective or the federal regulatory scheme. Because a state law can be preempted either due to express preemption or implied preemption, we must look to both kinds of preemption analysis.

1. Express preemption of enforcement mechanisms.

The best reading of the text of the Act's preemption provision is that it applies only to substantive limitations on the use of email for commercial purposes.[108] The Act is mostly focused on determining which kinds of spam are permitted and which are banned. Congress was careful to invalidate state laws that go beyond the substance of the Act, such as the California and Delaware statutes that require opt-in schemes for all spam.[109] Congress was presumably less concerned about how surviving state provisions are enforced, since the Act's preemption clause makes no mention of enforcement.

The text of the Act is consistent with a reading of the statute as being focused on state substantive provisions rather than state enforcement provisions. Section 8(b)(1) specifically saves from preemption "any [state] statute, regulation, or rule [that] prohibits falsity or deception in any portion of a commercial electronic mail message or information attached thereto."[110] This is very broad language that was designed to save state laws that are consistent with the Act's provisions and permit what Congress considered to be legitimate advertising. Congress wanted to avoid both incompatible state limitations and an outright ban, both of which would prevent any commercial email from being legally sent, while ensuring that a law that was more narrowly aimed at preventing consumer fraud was saved.[111]

---

108 See Part IV.A.

109 Cal Bus & Prof Code § 17529.2; 11 Del Code Ann §§ 937–38.

110 CAN-SPAM § 8(b)(1), 117 Stat at 2716.

111 The Senate Committee on Commerce, Science, and Transportation noted in its report on the Act:

Congress did not express the same degree of concern about methods of enforcement. Enforcement provisions have no direct effect on the substantive rules advertisers live by, and while stronger enforcement provisions might be more efficient to administer, and thus result in less rule breaking, the existence of stronger enforcement provisions won't deter what Congress considers to be appropriate spam. Enforcement differences also do not present the same concern that Congress cited about inconsistency of state laws.[112] If one state requires that adult spam be labeled with "adv:adult,"[113] and another requires "ADV:ADLT,"[114] then it becomes impossible to send law-abiding spam messages without knowing the destination of every message (or even what states each message will travel through). If one state enforces its spam laws by allowing recipients to sue,[115] though, while another relies on the state attorney general,[116] no conflict is created. As long as the substantive limits are consistent, a legitimate advertiser using email has no need to worry.

Although the CAN-SPAM Act limits its enforcement to ISPs and government agencies, this could simply represent a judgment that private actions are not sufficiently important to justify federal court time. A state could easily come to the opposite conclusion, and there is little reason not to support that decision, especially since that state will foot the bill for the use of its court system.

Finally, courts have long been reluctant to infer preemption where Congress has been vague.[117] The ultimate authority in determining the scope of a preemption clause is Congress, but because the re-

---

> [A] State law requiring some or all commercial e-mail to carry specific types of labels, or to follow a certain format or contain specified content, would be preempted. . . . Given the inherently interstate nature of e-mail communications, the Committee believes that this bill's creation of one national standard is a proper exercise of the Congress's power to regulate interstate commerce that is essential to resolving the significant harms from spam faced by American consumers, organizations, and businesses throughout the United States. This is particularly true because, in contrast to telephone numbers, e-mail addresses do not reveal the State where the holder is located. As a result, a sender of e-mail has no easy way to determine with which State law to comply.

S Rep No 108-102 at 21–22 (cited in note 32).

112 Id.

113 See, for example, Ark Code Ann § 4-88-603(a)(2) (Michie 2001) (requiring the label to be included in the first nine characters of the subject line).

114 See, for example, Alaska Stat § 45.50.479(a).

115 See, for example, Colo Rev Stat Ann § 6-2.5-104(1)(a)–(b) (West 2002) (allowing both recipients and ISPs to sue).

116 See, for example, Iowa Code Ann § 714E.2 (West 2003) (allowing the attorney general to seek injunctive relief and civil penalties).

117 See *Maryland v Louisiana*, 451 US 725, 746 (1981) (discussing the presumption that "Congress did not intend to displace state law"); Tribe, 1 *American Constitutional Law* § 6-28 at 1176 (cited in note 63).

sult of such a clause is to override the sovereignty of the states, the Supreme Court demands clear guidance from Congress before reaching that result. Here, Congress has been anything but clear: the text of the preemption clause, which is limited to discussing substantive rules, does not support preemption of enforcement provisions. Neither does Congress's intent, which was to limit the inconsistency in state laws and limit those laws to banning things that a "legitimate" spam sender would not do. Holding illegitimate senders accountable in different ways does not contradict that goal.

2. Implied preemption of enforcement mechanisms.

Even if Congress did not expressly preempt state causes of action against spam senders when it passed the CAN-SPAM Act, those causes of action might nevertheless be preempted according to one of the theories of implied preemption, either because Congress has evidenced a desire to occupy the entire field of spam regulation (field preemption) or because the state laws stand as an obstacle to the accomplishment of a federal objective (conflict preemption).

Field preemption is a poor fit for the CAN-SPAM Act. A pervasive scheme of federal regulation is almost a threshold requirement for finding field preemption: the Court seems to use such a pervasive scheme as a rough test for whether Congress intends to occupy a field of regulation.[118] The CAN-SPAM Act probably does not qualify as such a scheme. Though it applies to all commercial email affecting interstate or foreign commerce and authorizes some regulation by the FTC, this regulation is far from comprehensive: its only significant administrative component authorizes, but does not require, the FTC to set up a "do not email" registry.[119]

More importantly, the cases where the Supreme Court has found field preemption involve areas of law where Congress is ambiguous about preemption and where a finding that Congress intended to occupy the entire field is plausible. Here, Congress was explicit: it prevented states from enacting laws varying in substance from the CAN-SPAM Act, but it specifically left states with the ability to enforce essentially parallel provisions. This shows that rather than intending to occupy the field, Congress specifically intended to *divide* regulation between the federal government and the states. Congress has also expressed this intent in other ways: the Act gives state government agencies enforcement powers under federal law, alongside

---

118 See Part III.B.

119 CAN-SPAM § 9, 117 Stat at 2716.

federal agencies and ISPs.[120] Field preemption, accordingly, does not apply to the CAN-SPAM Act.

Conflict preemption—whether state spam laws "stand[] as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress"[121]—is a somewhat closer question. It's easy to imagine a state spam law that stands as such an obstacle. California's law is one: its strongest provision bans all unsolicited commercial email advertisements and requires prior consent or a business relationship for a company to send any such message.[122] It also provides harsh liquidated damages for any violation: $1000 per email message, up to a total of $1 million.[123] The former provision is clearly an obstacle to one of Congress's objectives in passing the CAN-SPAM Act: Congress aimed to create an environment where "legitimate" marketers could make use of email,[124] and the California law makes that impossible.

At the same time, the California enforcement provision—the severe liquidated damages provision—probably is not, when separated from the California substantive provisions, an obstacle to the objectives of the CAN-SPAM Act. The damages provision applies to a number of violations, from the ban on sending any spam without consent, to a ban on harvesting addresses from the internet for use in spamming.[125] Some of these violations are clearly beyond the intention of Congress and are explicitly preempted; others are explicitly saved from preemption. Those provisions that are not preempted are those that permit techniques used by "legitimate" email marketers and are thus consistent with Congress's intent.

Allowing a consumer to sue over such a violation, or to obtain a large liquidated damages amount, doesn't change that calculation: if the substantive provision is something Congress intended to permit, then the law is (explicitly) preempted; and if it is not, then a state enforcement provision cannot make that enforcement contrary to Congress's intent. Rather than impeding operation of the federal system, state enforcement assists the federal system by dividing the workload among federal courts, federal agencies, and state courts.

Indeed, Congress was careful in drafting the Act's preemption clause to ensure that no state law could escape preemption under that

---

120 Id § 7(b)(6), 117 Stat at 2712 (state insurance authorities); id § 7(f), 117 Stat at 2712 (state attorneys general and agencies generally).

121 *Hines v Davidowitz*, 312 US 52, 67 (1941).

122 Cal Bus & Prof Code § 17529.2.

123 Id § 17529.8(a)(1).

124 See note 32.

125 Cal Bus & Prof Code § 17529.4(a).

clause while nevertheless interfering with Congress's goals. Congress wanted to ensure that email was available as an advertising method to "legitimate" advertisers, and it designed the CAN-SPAM Act to permit that use. The preemption clause leaves in place only state laws that do not interfere with that goal—state statutes that are not preempted under conflict preemption analysis. Leaving state enforcement provisions in place is the best way to accomplish that intention.

V. SOME POLICY IMPLICATIONS

The scope of its preemption clause will determine, in part, the CAN-SPAM Act's overall effectiveness. As explained in Part I, the Act is broad in scope and prohibits many of the worst aspects of spam. It contains at least some restrictions in nearly every potential area of regulation the states have identified, short of banning spam outright or limiting it to recipients who have opted to receive messages. In other areas, however, the Act's restrictions are weaker than those enacted by the states, and the Act ultimately ignores several ways to fight spam. The set of tools available to fight spam will depend, then, on the extent to which the Act permits these state laws to remain in force: a narrow interpretation of the Act's savings clause will hinder states' efforts to fight spam, while a broader interpretation could give states stronger tools.

This is particularly important because the Act's restrictions are probably not the optimal way to reduce the volume of spam. By preempting substantial portions of most state spam laws, Congress has cut off the states' ability to experiment and determine the most effective or cost-efficient antispam measures. Given that neither the CAN-SPAM Act nor the state laws before it have been very effective in fighting spam,[126] giving states flexibility to find better laws could lead to more effective antispam measures.[127]

There are also several extralegal obstacles to effective spam control that the CAN-SPAM Act leaves unchanged.[128] Despite the technical obstacles and the law's weaknesses, though, the CAN-SPAM Act might nevertheless be a significant boost in the fight against spam. Recent studies show that the vast majority of spam comes from serv-

---

126 See note 10 and accompanying text.

127 At the same time, spam is fundamentally a national (and international) problem, and too many inconsistent state laws might hamper the federal government's ability to tackle the issue. Conflicting state laws also make it much more difficult for legitimate marketers to take advantage of email. Congress was concerned about this effect on legitimate marketers. See note 32.

128 See notes 11–12 and accompanying text.

ers located in the United States.[129] More importantly, most of that spam comes from a small number of servers—200 or fewer.[130] This concentration of senders represents an opportunity to make a major dent in the world's spam problem, since the cost of fighting 200 senders is substantially smaller than the cost of fighting millions of small-time operators. Interpreting the CAN-SPAM Act as broadly as possible, then, while permitting enforcement of broader state laws as well, could actually have a substantial effect on the world's spam problem.

Unfortunately, the CAN-SPAM Act's enforcement provisions, while relatively strong, are limited to ISPs and the government.[131] For those parties, the Act's enforcement approach is fine as far as it goes. It is, however, unnecessarily limited. ISPs have incentives to prevent spam senders from targeting their customers, but lawsuits are expensive, and the incentives probably result in too little ISP enforcement.[132] Likewise, government agencies are unlikely to have the resources or motivation to track down more than a handful of senders, due to the large volume of senders and the use of various methods to obscure the identity of those senders. ISPs and government agencies are not the only parties harmed by spam, and by limiting enforcement to them, Congress neglects probably the most effective potential enforcers: individuals and businesses who receive spam and are likely the group most hurt by it.

A large company that provides internet access to its employees for use in their work could face substantial costs in avoiding spam; all consumers and companies that receive spam almost certainly face aggregate costs—from filtering or from time wasted wading through

---

129 See Gregg Keizer, *Spam: Born in the USA*, InformationWeek TechWeb News (Aug 12, 2004), online at http://www.informationweek.com/story/showArticle.jhtml?articleID=28700163 (visited Nov 14, 2004) (reporting on a survey by message-filtering vendor CipherTrust, which found that 86 percent of the world's spam comes from the United States); CipherTrust, *CipherTrust Spam Statistics*, online at http://www.ciphertrust.com/resources/statistics/spam_sources.html (visited Nov 14, 2004) (listing the top seventeen spam-producing nations, of which the United States is the first). But see Sophos, Press Release, *Sophos Reveals Latest "Dirty Dozen" Spam Producing Countries* (Aug 24, 2004), online at http://www.sophos.com/spaminfo/articles/dirtydozenaug04.html (visited Nov 14, 2004) (reporting that only 43 percent of spam in one study originated in the United States).

130 See Spamhaus, *Register of Known Spam Operations*, online at http://www.spamhaus.org/rokso (visited Nov 14, 2004) (listing 200 spam operators who have been kicked off of at least three ISPs for "serious spam offenses"); Keiser, *Spam: Born in the USA*, InformationWeek TechWeb News (cited in note 129) (estimating that most spam comes from fewer than 200 U.S.-based IP addresses).

131 See text accompanying notes 35–45.

132 See note 45. The Act does provide for the discretionary award of attorneys' fees to ISPs. CAN-SPAM § 7(g)(4), 117 Stat at 2715. Many spam senders, however, are likely to be judgment proof. In any event, a substantial portion of the costs of enforcing the Act are likely to be technical, and thus not covered by the fees provision.

spam—greater than those faced by ISPs.[133] Additionally, any cost borne by ISPs is presumably passed on to customers; ISPs therefore may not have the incentives to take the right level of action against senders. In short, the CAN-SPAM Act relies on governmental and ISP third parties to vindicate consumers' rights, but those parties' incentives to do so are unclear at best. The prospect of defending lawsuits brought by consumers and businesses nationwide would surely encourage advertisers to obey the law. Interpreting the Act to permit such state law enforcement provisions is most consistent with Congress's intent in passing the CAN-SPAM Act.

CONCLUSION

When it passed the CAN-SPAM Act in 2003, Congress replaced a patchwork system of inconsistent, incomplete state spam regulations with a uniform nationwide system that prohibits forged headers and deceptive subject lines in commercial email, requires identification information and opt-out mechanisms, and prohibits many methods used to obtain email addresses and send messages without being traced. Despite this, neither the CAN-SPAM Act nor its predecessor state laws have entirely stopped spam or even obviously reduced it in quantity.

Despite its billing as a law designed to reduce the spam problem, the CAN-SPAM Act essentially legalizes and regulates spam messages in the United States. Nevertheless, the Act's preemption provisions, which preempt most stronger state spam laws, still allow some that go beyond the federal provisions. These potential state laws include both additional substantive provisions and enforcement mechanisms. Interpreting the CAN-SPAM Act's preemption provisions to permit enforcement of compatible state laws could be a substantial boost in the fight against spam.

---

[133] Arguably, the Act gives a large company that provides internet service to its employees a right of action. The Act gives "provider[s] of Internet access service" the right to sue spammers. CAN-SPAM § 7(g), 117 Stat at 2714–15. The Act defines "Internet access service" as "a service that enables users to access content, information, electronic mail, or other services offered over the Internet, [possibly including] access to proprietary content, information, and other services as part of a package of services offered to consumers." Id § 3(11), 117 Stat at 2702 (referring to the definition provided in 47 USC § 231(e)(4) (2000)). A large provider of internet service is providing "a service that enables users to access content, information, electronic mail, or other services offered over the Internet," even if it is not a paid service offered to consumers. This interpretation, however, is fairly clearly not what Congress intended, and its success in court is far from certain.

APPENDIX: STATE SPAM LAWS[134]

	no statute	attorneys must label spam	opt-in for all spam	subject-line label	subject-line label (adult content)	opt-out required	ban on false routing info	ban on false/misleading subject line	ban on false/third-party domain name	must contain sender's email address	must contain sender's name	must contain sender's mailing address	must contain sender's domain name	geographic jurisdictional limitations	illegal to harvest addresses	false routing software banned	illegal to violate ISP spam policy	attorney general enforcement	recipient right of action	ISP right of action	liquidated damages	criminal provisions	injunctive relief
Alabama	•																						
Alaska					•																		
Arizona				•		•	•	•	•					•				•	•	•	•		
Arkansas					•	•	•	•	•		•	•	•			•		•	•	•	•	•	
California			•				•	•	•						•		•	•	•	•	•		
Colorado				•		•	•		•	•				•					•	•	•		
Connecticut							•									•	•	•	•	•	•	•	
Delaware			•				•							•		•			•			•	•
Florida		•					•	•	•							•			•	•	•		•
Georgia	•																						

[134] This compilation of state spam laws is based on the information provided by David E. Sorkin, *Spam Laws* (cited in note 16). The categorization by type in this Appendix is by the author. State statutes can be found at Alaska Stat § 45.50.479 (Michie 2003); Ariz Rev Stat § 44-1372 (2003); Ark Code Ann §§ 4-88-601 to -607, 5-41-201 to -206 (Michie 2003); Cal Bus & Prof Code §§ 17529, 17538 (West 2003); Colo Rev Stat §§ 6-2.5-101 to -105, 13-6-105, 13-6-403 (2000); Gen Stat Conn §§ 53-451 to -453, 52-59b (2003); 11 Del Code Ann §§ 931, 937–41 (2000); Fla Stat Ann § 668.60 et seq (West 2004); Idaho Code § 48-603E (2000); 720 ILCS 5/16D-1 to -7 (West 2003); 815 ILCS 511/1, 5, 10, 15, 505/2Z, 7 (West 2003); Ind Code §§ 24-5-22-1 to -10 (2003); Iowa Code § 714E.1–2 (2000); Kan Stat Ann §§ 50-6, 107 (2003); La Rev Stat Ann §§ 14:73.1, 14:73.6, 14:106.A(7), 51:1741.1–3 (West 2003); 10 Me Rev Stat Ann § 1497 (West 2003); Md Comm Code Ann §§ 14-3001 to -3003 (2002); Mich Comp Laws § 445.2501–08 (2003); Minn Stat §§ 325F.694–95, 325F.70 (2003); Mo Rev Stat §§ 407.100, 407.1120, 407.1123, 407.1126, 407.1129, 407.1132, 407.1135, 407.1138, 407.1141 (2003); Nev Rev Stat §§ 41.705–35, 205.492–513 (2003); NM Stat Ann §§ 57-12-11, -23 to -24 (Michie 2003); NC Gen Stat §§ 1-75.4, 1-539.2A, 14-453, 14-458 (2000); ND Cent Code §§ 51-27-01 to -09 (2003); Ohio Rev Code Ann § 2307.64 (Anderson 2004); 15 Okla Stat §§ 756.1, 776.1–7 (2003); Or Rev Stat § 646.607–08 (2003); 2003 Or Laws 910; 18 Pa Cons Stat §§ 5903, 7661 (2000); 73 Pa Cons Stat § 2250.1–8 (2002); RI Gen Laws §§ 11-52-1 to -8, 6-47-1 to -3 (2000); SD Cod Laws §§ 37-24-6, -36 to -40 (Michie 2004); Tenn Code Ann §§ 47-18-2501 to -2502 (2003); Tex Bus & Comm Code Ann §§ 46.001–11 (West 2003); Va Code Ann §§ 8.01-328.1, 18.2-152.2, 18.2-152.3:1, 18.2-152.4, 18.2-152.12 (Michie 2003); Wash Rev Code §§ 19.190.010–50 (2000); W Va Code §§ 46A-6G-1 to -5 (2000); Wis Stat § 944.25 (2001); Wyo Stat §§ 40-12-401 to -404 (2003). Restrictions on attorney email are mandated by state bar rules in Florida and Louisiana, and by a state supreme court rule in Kentucky. See Fla Rules Prof Conduct, 4-7.6(c)(3); La Rules Prof Conduct 7.2(b)(iii)(B); Ky S Ct Rule 3.130(7.09)(3).

	no statute	attorneys must label spam	opt-in for all spam	subject-line label	subject-line label (adult content)	opt-out required	ban on false routing info	ban on false/misleading subject line	ban on false/third-party domain name	must contain sender's email address	must contain sender's name	must contain sender's mailing address	must contain sender's domain name	geographic jurisdictional limitations	illegal to harvest addresses	false routing software banned	illegal to violate ISP spam policy	attorney general enforcement	recipient right of action	ISP right of action	liquidated damages	criminal provisions	injunctive relief
Hawaii	•																						
Idaho						•	•		•	•									•		•		
Illinois				•	•	•	•	•	•					•		•		•	•	•	•	•	
Indiana				•	•	•	•	•	•					•				•	•	•			
Iowa						•	•		•	•				•				•	•	•	•		•
Kansas				•	•	•	•	•	•	•	•			•		•		•	•	•	•		
Kentucky	•	•																					
Louisiana		•		•	•	•	•	•	•	•						•	•		•	•		•	
Maine				•	•	•	•		•	•	•							•	•	•	•		•
Maryland							•	•	•					•					•	•	•		
Massachusetts	•																						
Michigan				•		•	•		•	•	•	•	•	•		•		•	•	•	•	•	
Minnesota				•	•	•	•	•	•					•				•	•	•	•		•
Mississippi	•																						
Missouri				•		•		•										•	•	•	•		•
Montana	•																						
Nebraska	•																						
Nevada				•		•	•	•	•	•	•	•			•	•		•	•		•	•	•
New Hampshire	•																						
New Jersey	•																						
New Mexico				•	•	•												•	•	•	•		•
New York	•																						
North Carolina							•										•		•	•	•	•	
North Dakota				•	•	•	•	•	•					•					•	•	•		
Ohio						•	•			•	•	•					•		•	•	•	•	•
Oklahoma				•	•	•	•	•	•							•		•	•	•	•		•
Oregon				•			•	•	•									•	•	•	•		•
Pennsylvania					•	•	•	•	•	•						•		•	•	•	•	•	•
Rhode Island						•	•		•					•		•	•		•	•	•	•	
South Carolina	•																						
South Dakota				•	•		•	•	•					•					•	•	•		•

	no statute	attorneys must label spam	opt-in for all spam	subject-line label	subject-line label (adult content)	opt-out required	ban on false routing info	ban on false/misleading subject line	ban on false/third-party domain name	must contain sender's email address	must contain sender's name	must contain sender's mailing address	must contain sender's domain name	geographic jurisdictional limitations	illegal to harvest addresses	false routing software banned	illegal to violate ISP spam policy	attorney general enforcement	recipient right of action	ISP right of action	liquidated damages	criminal provisions	injunctive relief
Tennessee				•	•	•								•		•	•		•	•	•		
Texas				•	•	•	•	•	•	•								•	•	•	•	•	•
Utah	•																						
Vermont	•																						
Virginia							•									•	•	•	•	•	•	•	
Washington							•	•	•					•				•	•	•	•		
West Virginia							•	•	•	•	•			•		•	•		•	•	•		•
Wisconsin					•																	•	
Wyoming							•	•	•					•				•					