

SPAM LEGISLATION IN THE UNITED STATES

DAVID E. SORKIN†

Spam—unsolicited bulk or commercial e-mail¹—began lighting up lawmakers’ radar screens in 1997. The Federal Trade Commission (“FTC”) held a public workshop on spam and other consumer privacy issues in June of that year.² Legislation that would prohibit unsolicited commercial e-mail was proposed in Congress and five state legislatures.³ No such laws were enacted that year, although one state did enact a law requiring unsolicited commercial e-mail messages to identify the sender and include instructions for declining further communications.⁴

Since 1997 there has been a torrent of legislative activity related to spam. Well over half of the states have enacted some form of spam legislation,⁵ and two states have prohibited spam outright⁶—as have various

† Associate Professor of Law, Center for Information Technology and Privacy Law, The John Marshall Law School.

1. “Spam” has traditionally been defined as either unsolicited bulk e-mail or unsolicited commercial e-mail. See David E. Sorkin, *Technical and Legal Approaches to Unsolicited Electronic Mail*, 35 U.S.F. L. Rev. 325, 328 (2001) (available at <<http://www.spamlaws.com/articles/usf>>). Less formally the term is also used to refer to any commercial or unwanted e-mail. See *id.* at 327. Recently, some marketers have sought to redefine the term to include only fraudulent e-mail (and, by implication, to exclude the unsolicited bulk commercial e-mail that they send). See *e.g.* Don Oldenburg, *Spam and a Case of Dyspepsia: Marketers and Blacklisters Face Off at FTC’s E-Mail Forum*, Wash. Post. C1 (May 3, 2003) (referring to remarks Direct Marketing Association president Robert Wientzen).

2. See Fed. Trade Commn., *Consumer Information Privacy Workshop* <<http://www.ftc.gov/bcp/privacy/wkshp97>> (June 10-13, 1997).

3. See H.R. 1748, 105th Cong. (1997); Conn. H. 6558, 1997 Reg. Sess. (Jan. 30, 1997); Mass. H. 4581, 182d Gen. Ct., Reg. Sess. (June 12, 1997); Nev. Sen. 13, 69th Reg. Sess. (Jan. 14, 1997) (subsequently enacted in different form); R.I. Sen. 1073, 1997-98 Leg. Sess. (May 9, 1997); Wis. S.B. 283, 93d Reg. Sess. (Aug. 28, 1997).

4. See 1997 Nev. Stat. 1225, codified at Nev. Rev. Stat. §§ 41.705-41.735 (1997) (amended 2003).

5. See David E. Sorkin, *Spam Laws: Summary* <<http://www.spamlaws.com/state/summary.html>> (1997) (summarizing spam-related legislation in thirty-six states).

6. See Cal. Bus. & Prof. Code Ann. § 17529.2 (Westlaw 2004); Del. Code tit. 11, § 937 (2003).

jurisdictions outside the United States, including the European Union.⁷ In 2003, the FTC held a second spam forum,⁸ and later in the year Congress enacted the *CAN-SPAM Act of 2003*,⁹ which imposes stiff penalties on fraudulent spam but pre-empts state laws that attempt to regulate nonfraudulent spam. Yet it is generally agreed that legislation has failed to solve the spam problem. There is more spam now than ever before,¹⁰ and some argue that ill-advised legislation may be making the problem even worse.¹¹

I. STATE LEGISLATION (1997-2003)

Thirty-six states enacted legislation targeting unsolicited bulk or commercial e-mail between 1997 and 2003. Most of these laws focus on deceptive practices associated with spam, such as the use of misleading subject lines, forged sender addresses, and false routing information contained in message headers. Some states also impose affirmative disclosure requirements on senders of unsolicited e-mail, and several require that a specified label appear in the subject line of unsolicited commercial messages. Most state laws also contain provisions requiring senders to honor individual “opt-out” requests, and two states prohibit nearly all unsolicited commercial e-mail (the equivalent of an “opt-in” regime). The geographic reach of the state laws varies from state to state, as do the methods of enforcement that they provide.

A. COMMON PROVISIONS OF STATE SPAM LEGISLATION

1. *Deceptive Practices*

Senders of unsolicited bulk and commercial e-mail commonly employ a variety of deceptive practices. They may falsify or obscure components of the message header, including the “from” line and the routing information (“received” lines), in order to conceal their identity and that of their clients or service providers, and thereby avoid some of the costs and other negative consequences that might otherwise result from sending spam—especially when the substantive content of the message is also fraudulent or unlawful. They also frequently use vague or mislead-

7. See Directive 2002/58/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, 2002 O.J. L 201 (July 12, 2002).

8. See Fed. Trade Commn., *FTC Spam Forum* <<http://www.ftc.gov/bcp/workshops/spam>> (Apr. 30–May 2, 2003).

9. Pub. L. No. 108-187, 117 Stat. 2699 (2003).

10. See e.g. Chris Gaither, *Congress Reaches Antispam Bill Accord*, Boston Globe D1 (Nov. 22, 2003); Saul Hansell, *Totaling Up the Bill for Spam*, N.Y. Times C1 (July 28, 2003).

11. See *infra* pt. I(B).

ing subject lines, in order to induce recipients to open their messages instead of recognizing them immediately as spam and deleting them unread.

Many states have enacted legislation that attempts to address the use of deceptive practices in spam. The following provision is typical:

No individual or entity may initiate or cause to be initiated an unsolicited electronic mail advertisement if the electronic mail advertisement (i) uses a third party's Internet domain name without permission of the third party, or otherwise misrepresents any information in identifying the point of origin or the transmission path of an electronic mail advertisement or (ii) contains false or misleading information in the subject line.¹²

Restrictions on deceptive practices tend to be directed at commercial messages, but many states impose such restrictions on noncommercial messages as well.¹³

2. *Disclosure and Labeling Requirements*

In addition to prohibiting senders of unsolicited bulk and commercial e-mail from misrepresenting their identity, some states impose an affirmative duty to disclose the sender's name and contact information. In some instances even the sender's physical postal address must be included in each message.¹⁴ These disclosure requirements seem to have two primary objectives: to combat fraud and to facilitate submission of "opt-out" requests by recipients.

Another common provision in state spam legislation is a requirement that all unsolicited commercial e-mail messages bear a subject line beginning with a standard label—usually "ADV:"—in order to facilitate efficient recognition of such messages by recipients and intermediaries, presumably including the ability to block such messages automatically before they even reach an addressee's inbox. Some states require an extended version of the label such as "ADV:ADLT" for sexually explicit advertisements.¹⁵ At least twenty-four states have enacted legislation that

12. 815 Ill. Comp. Stat. § 511/10(a) (2002).

13. See e.g. Pa. Consol. Stat. Ann. § 7661(a)(1) (LexisNexis 2003) (all unsolicited e-mail); Okla. Stat. tit. 15, § 776.1 (LexisNexis 2003) (all e-mail).

14. See e.g. Ark. Code Ann. § 4-88-603(a)(1) (Supp. 2003); Utah Code Ann. § 13-36-103(1)(a) (2003).

15. See e.g. Ark. Code Ann. § 4-88-603(a)(2) (Supp. 2003) ("ADV:ADULT"); Cal. Bus. & Prof. Code § 17538.4(g) (Westlaw 2003) (repealed 2003) ("ADV:ADLT"); Pa. Cons. Stat. § 5903(a.1) (LexisNexis 2003) ("ADV-ADULT"). Of course, the differing versions of this label required by various states are mutually inconsistent, since the label normally must appear at the beginning of the subject line. This point was raised in 2002 in a dormant Commerce Clause challenge to California's then-current law. The court characterized the inconsistency as a "minor distinction" and rejected the argument, apparently for want of

imposes some sort of labeling requirement.¹⁶

3. *Opt-Out Provisions*

Nearly all states at least implicitly recognize an “opt-out” regime for spam—i.e., absent fraud or some other violation of the law, a sender is free to solicit potential customers via e-mail until each potential customer requests that the communications cease.¹⁷ States often attempt to regulate the “opt-out” process, although with varying levels of specificity. Some states impose specific requirements concerning the method by which such requests are received, the speed with which they are processed, or the manner in which the “opt-out” right is disclosed to recipients.¹⁸

Nearly all of these “opt-out” provisions contemplate individual recipients of spam communicating their preferences to individual spammers on a one-to-one basis. An alternative considered by the New Hampshire state legislature in 1998 would have permitted Internet service providers to register with the state as “restricted solicitation” providers, and then prohibited marketers from sending spam to any subscriber of a registered provider.¹⁹ The Ohio statute adopts a technological variant of this approach, giving legal effect to a provider’s anti-spam terms that are posted on a public Web site and communicated to marketers by the provider’s e-mail server.²⁰

evidence that a sender would ever have to comply with two states’ laws simultaneously. See *Ferguson v. Friendfinders, Inc.*, 115 Cal. Rptr. 2d 258, 266 (App. 1st Dist. 2002).

16. See Sorkin, *Spam Laws: Summary*, *supra* n. 5.

17. The only exceptions—states that have adopted an “opt-in” regime—are California and Delaware. See *infra* pt. I(A)(4).

18. See *e.g.* Mich. Comp. Laws §§ 445.2503(c), (d), 2504(3) (2003).

19. See N.H. H. 1633, 155th Leg., 2d Year (Jan. 7, 1998) (available at <<http://gencourt.state.nh.us/legislation/1998/HB1633.html>>). Such an approach could become the functional equivalent of an “opt-in” regime, since nearly all Internet service providers already have strong anti-spam policies, and presumably they would all elect to register as “restricted solicitation” providers. Cf. Sorkin, *Technical and Legal Approaches to Unsolicited Electronic Mail*, *supra* n. 1, at 374 (speculating that nearly all ISPs would take advantage of a law enabling them to enforce anti-spam policies based upon constructive notice).

20. See Ohio Rev. Code Ann. § 2307.64(C) (Anderson 2004). This constructive notice provision took effect in November 2002, but it has not yet been applied, at least not in any widely-reported cases. It is possible that senders who relay e-mail through unrelated third-party servers (a common technique used by spammers) would not be affected by the provision anyway, since the notice transmitted by the receiving server would not reach them.

4. *Outright Prohibition*

Two states have enacted laws that amount to an outright prohibition on most spam. In 1999, Delaware enacted legislation criminalizing the sending of unsolicited bulk commercial e-mail:

A person is guilty of the computer crime of un-requested or unauthorized electronic mail . . . when that person, without authorization, intentionally or recklessly distributes any unsolicited bulk commercial electronic mail (commercial e-mail) to any receiving address or account under the control of any authorized user of a computer system.²¹

In 2003, California amended its law to provide that “a person or entity may not . . . [i]nitiate or advertise in an unsolicited commercial e-mail advertisement.”²² Although Delaware’s law has been in effect for some years, the state has not yet attempted to enforce it,²³ and the California law was pre-empted by federal legislation before its scheduled effective date.²⁴ Congress and several other states have considered (but thus far rejected) similar legislation.²⁵

5. *Geographic Reach*

The vast majority of spam is sent across state lines. Even if the sender and recipient happen to be located within the same state, it is likely that the message will be routed through a server located elsewhere. Moreover, senders and recipients of spam usually are unaware of (and generally unable to determine) the other party’s location. Some state laws contain explicit provisions regarding their geographic reach, although several are silent on this question, producing uncertainty as to whether a state’s law applies to a particular message.

Although Delaware’s law is substantively stronger than most, in geographic reach it is similar to the laws in many other states. If a message is sent from outside Delaware, the law applies only if the sender is aware of circumstances making it a “reasonable possibility” that the recipient is within the state.²⁶ Washington law is similar in effect but more specific: a sender is deemed to know that the recipient is within the state “if that information is available, upon request, from the registrant of the internet domain name contained in the recipient’s electronic mail address.”²⁷ California’s law, on the other hand, has a broader reach—it

21. Del. Code Ann. tit. 11, § 937 (2003).

22. Cal. Bus. & Prof. Code § 17529.2 (Westlaw 2004).

23. See Saul Hansell, *California Acts to Ban Junk E-Mail*, N.Y. Times C1 (Sept. 24, 2003).

24. See *infra* pt. II(B).

25. See *e.g. supra* n. 3 and accompanying text.

26. See Del. Code Ann. tit. 11, § 937(d).

27. See Wash. Rev. Code § 19.190.020(2) (Westlaw 2004). Of course, it is impractical for a spammer who intends to send messages to several million recipients to communicate

applies to messages sent from California or to a California resident's e-mail address, without regard to the sender's knowledge.²⁸

6. *Enforcement Mechanisms*

A variety of enforcement mechanisms can be found in state spam legislation. In some states, certain spam-related activities may be prosecuted as crimes,²⁹ although it is rare for criminal charges to be brought in the absence of behavior that also violates other laws.³⁰ Some states confer other enforcement powers upon the attorney general or other officials, although few states have been aggressive in enforcing spam laws.³¹

In many states, a private right of action is available to Internet service providers or even individual recipients of unlawful spam.³² Most of the laws provide for fixed statutory damages as an alternative to actual damages, which may be difficult to ascertain.³³ It is difficult to estimate the number of actions that have been brought under such provisions (in part because many such cases are brought by individual recipients in small claims courts), but it is likely in the thousands.

with the relevant service provider for each address on the spammer's list concerning the addressee's physical location.

28. See Cal. Bus. & Prof. Code § 17529.2; see also *id.* § 17529.1(b) (defining "California electronic mail address"). Statutes in some other states appear to have similarly broad reach. For example, the Connecticut long-arm statute provides for jurisdiction over a non-resident who uses a computer or network located within the state to transmit unsolicited bulk electronic mail. See Conn. Gen. Stat. Ann. § 52-59b(a) (West Supp. 2003); see *id.* § 53-452(f) (West 2001).

29. See e.g. Va. Code Ann. § 18.2-152.3:1 (Westlaw 2004).

30. See e.g. Mark Harrington, "Spammer" Faces Felony, *Newsday* A68 (Dec. 12, 2003); Mark Harrington, *NY Spammer Is Arrested*, *Newsday* A47 (May 15, 2003).

31. Attorney General Christine Gregoire of Washington has placed a relatively high priority on fighting fraudulent spam. State officials have brought civil charges against alleged spammers in Washington and New York and perhaps elsewhere, although the total number of such cases appears to be quite small. See e.g. Paul Festa, *CNET News.com*, *Spam Crusaders Slog It Out in Court*, <http://news.com.com/2100-1023_3-954960.html> (accessed Aug. 23, 2002).

32. See e.g. 815 Ill. Comp. Stat. § 511/10(c), (d) (2002). In addition, many state spam laws provide that violations constitute unfair or deceptive trade practices or otherwise are actionable under a separate consumer protection or consumer fraud statute. See e.g. Tex. Bus. & Com. Code Ann. § 46.007 (Westlaw 2004); Wash. Rev. Code § 19.190.030(3) (Westlaw 2004). And in some states, a person who suffers a loss as a result of a crime is entitled to bring a civil action against the offender even absent a conviction. See e.g. *Porter County Cable Co. v. Moyer*, 624 F. Supp. 1, 5 (N.D. Ind. 1983).

33. See e.g. Cal. Bus. & Prof. Code § 17529.8 (Westlaw 2004) (\$100 to \$1,000 per message); Mich. Comp. Laws § 445.2508(4) (2003) (\$500 per message); Ohio Rev. Code Ann. § 2307.64(E) (Anderson 2004) (\$100 per message); Va. Code Ann. § 18.2-152.12 (Westlaw 2004) (\$1 or \$10 per message).

B. CONSEQUENCES OF STATE LEGISLATION

1. *Effectiveness*

Commentators seem to agree that state laws have failed to stem the tide of spam, although the net impact of state legislation is not clear. Anecdotal evidence—including the extremely low rate of compliance with existing state laws recently observed by the Federal Trade Commission³⁴—suggests that most spammers are simply ignoring state laws entirely, rather than making even perfunctory attempts to comply. On the other hand, it is possible that the states' preoccupation with fraudulent aspects of spam has contributed to the legitimization of nonfraudulent spam and encouraged legitimate marketers to begin using e-mail for prospecting purposes.³⁵ As already noted, neither of the two states that prohibit spam have attempted to enforce those laws,³⁶ so there is little evidence regarding the effect of substantively stronger laws. In the European Union, laws prohibiting spam seem to have had relatively little impact, although this may merely reflect the fact that the vast majority of spam received there originates elsewhere.³⁷

2. *Constitutionality*

The constitutionality of state spam legislation has been challenged in two major cases, one in California³⁸ (under the state's 1998 law, which did not prohibit spam outright) and one in Washington.³⁹ In both instances, the state laws were challenged under the dormant Commerce Clause of the U.S. Constitution, based upon their effect upon interstate commerce. Neither challenge was successful, although both courts placed considerable emphasis on the fact that the challenged statutes merely regulated fraud or deception, suggesting that a challenge to substantively stronger state law provisions might have fared better.

34. The FTC observed that very few spammers comply with such requirements as the "ADV:" labeling schemes mandated by many states. Fed. Trade Comm'n., *False Claims in Spam 11* <<http://www.ftc.gov/reports/spam/030429spamreport.pdf>> (Apr. 30, 2003).

35. See e.g. Doug Bedell, *Spammers Given a Lift, Experts Say*, Dallas Morning News 1D (Dec. 20, 2003); Jonathan Krim, *Anti-Spam Act Signed But Some Are Skeptical*, Wash. Post A18 (Dec. 17, 2003); SA Mathieson, *Strong Arm of the Law: Can Legislation Stop the Tide of Junk Email in Europe?*, Guardian (London) 16 (July 3, 2003) (available in LEXIS, News & Business, Country & Region (excluding U.S.), United Kingdom, News, The Guardian (London)); Saul Hansell, *Microsoft Sues 15 Organizations in Broad Attack on Spam E-Mail*, N.Y. Times C3 (June 18, 2003).

36. See *supra* pt. I(A)(4).

37. See Mathieson, *supra* n. 33 (citing estimate that ninety percent of email sent to Europeans originates outside the EU).

38. See *Ferguson v. Friendfinders, Inc.*, 115 Cal. Rptr. 2d 258 (App. 1st Dist. 2002).

39. See *State v. Heckel*, 24 P.3d 404 (Wash. 2001).

II. FEDERAL LEGISLATION (2003)

After considering numerous spam-related bills over a period of several years, in December 2003 Congress enacted the *CAN-SPAM Act of 2003*,⁴⁰ much of which parallels provisions found in state spam laws. Like most state spam laws, *CAN-SPAM* implicitly recognizes an “opt-out” regime, and focuses most of its attention on fraudulent and misleading spam. *CAN-SPAM* does contain a few interesting wrinkles, including authorization of a “Do-Not-E-Mail” registry. Perhaps most significantly, *CAN-SPAM* pre-empts key provisions in state spam laws.

A. PROVISIONS OF THE CAN-SPAM Act

The *CAN-SPAM Act* applies to “commercial e-mail messages,” a term defined in the law as excluding “transactional or relationship messages” sent by a business to its customers for purposes other than marketing.⁴¹ It imposes criminal penalties for certain fraudulent acts, including falsification of routing information.⁴² Other provisions in the law prohibit deceptive subject headings, regulate “opt-out” procedures, and require the sender’s physical address to appear in every message.⁴³ It does not require subject-line labels on most spam, except for messages containing sexually explicit material, which must bear a label to be determined by the Federal Trade Commission.⁴⁴ Businesses “knowingly promoted” by messages sent in violation of the law may also be held liable.⁴⁵

Primary enforcement authority rests with the FTC and various other federal agencies, although states are also empowered to bring enforcement actions with notice to the appropriate federal agency.⁴⁶ In addition, the law creates a private right of action for Internet service providers (but not individual recipients).⁴⁷

The *CAN-SPAM Act* directs the FTC to prepare a plan for a nationwide “Do-Not-E-Mail” registry analogous to the FTC’s “Do-Not-Call” registry, and to submit a report on the plan to Congress within six months.⁴⁸ The law authorizes but does not require the FTC to implement the registry, and preliminary indications are that the FTC will de-

40. Pub. L. No. 108-187, 117 Stat. 2699 (2003).

41. See *id.* § 3, 117 Stat. at 2700-2703 (to be codified at 15 U.S.C. § 7702).

42. See *id.* § 4, 117 Stat. at 2703-2706 (to be codified at 18 U.S.C. § 1037).

43. See *id.* § 5(a), 117 Stat. at 2706-2708 (to be codified at 15 U.S.C. § 7704(a)).

44. See *id.* § 5(d), 117 Stat. at 2709-2710 (to be codified at 15 U.S.C. § 7704(d)).

45. Pub. L. No. 108-187, § 6, 117 Stat. at 2710-2711 (to be codified at 15 U.S.C. § 7705).

46. See *id.* § 7, 117 Stat. at 2711-2715 (to be codified at 15 U.S.C. § 7706).

47. See *id.* § 7(g), 117 Stat. at 2714-2715 (to be codified at 15 U.S.C. § 7706(g)).

48. See *id.* § 9, 117 Stat. at 2716 (to be codified at 15 U.S.C. § 7708).

cline to implement it absent further Congressional action.⁴⁹

Another provision in *CAN-SPAM* contemplates the creation of a reward system in which persons who assist in tracking violations of the Act become eligible to receive a bounty,⁵⁰ an idea supported by Lawrence Lessig.⁵¹ Yet another provision directs the FTC to study labeling of commercial e-mail with “ADV” or a comparable identifier.⁵²

B. EFFECTS OF CAN-SPAM ON STATE LEGISLATION

The *CAN-SPAM Act* provides that it supersedes state laws regulating commercial e-mail, although the pre-emption clause contains broad exceptions for laws regulating falsity or deception and those that are not specific to e-mail.⁵³ State laws regulating falsification of routing information and other deceptive practices therefore remain in force, while those that require “ADV:” labels, mandate various disclosures, regulate “opt-out” procedures, or prohibit spam outright generally are pre-empted.⁵⁴ The federal law has no effect on common-law rights, although the California Supreme Court’s recent decision in *Intel Corp. v. Hamidi*⁵⁵ may tend to limit the most promising theory, trespass to chattels, to the most egregious cases.

CONCLUSION

Thus far, legislation has had very little impact on spam, and the *CAN-SPAM Act of 2003* is unlikely to change that situation. Most state laws do little or nothing to halt the transmission of unsolicited messages, and spammers have generally ignored even the least onerous state law requirements. A stronger federal law might accomplish some good—for example, a “Do-Not-E-Mail” registry encompassing most Internet users, coupled with strong enforcement mechanisms—but the international dimensions of the spam problem and other factors limit the potential impact of any legal approach.⁵⁶ On the other hand, one might reasonably presume that unlike the fraudulent spammers prevalent today, legiti-

49. See Jonathan Krim, *Senate Votes 97-0 to Restrict E-Mail Ads*, Wash. Post A1 (Oct. 23, 2003).

50. See Pub. L. No. 108-187, § 11(1), 117 Stat. at 2717 (to be codified at 15 U.S.C. § 7710(1)).

51. See Declan McCullagh, *CNET News.com, A Modest Proposal to End Spam* <<http://news.com.com/2010-1071-998513.html>> (Apr. 28, 2003).

52. See Pub. L. No. 108-187, § 11(2), 117 Stat. at 2717 (to be codified at 15 U.S.C. § 7710(2)).

53. See *id.* § 8, 117 Stat. at 2716 (to be codified at 15 U.S.C. § 7707).

54. See Sen. Rpt. 108-102, at 21 (July 16, 2003).

55. 71 P.3d 296 (Cal. 2003).

56. See Sorkin, *Technical and Legal Approaches to Unsolicited Electronic Mail*, *supra* n. 1, at 380-383 (discussing limitations of legal approaches).

mate marketers will pay attention to laws that regulate their activities. A federal law focusing on fraud (as *CAN-SPAM* does) or mandating "ADV:" labels on all unsolicited commercial e-mail, therefore, might be expected to have little impact on existing spam, but could lead to a dramatic increase in the amount of spam sent by legitimate businesses.