Spring 2004

A State-By-State Comparison Of Spam Laws

Arminda B. Bepko

MEDIA LAW & POLICY

A STATE-BY-STATE COMPARISON OF SPAM LAWS

Arminda B. Bepko*

I. INTRODUCTION

Weight loss advertisements, low interest home loans, books, videos, and plane tickets are just a few items marketed on the Internet by e-mail.[1] When recipients want and expect this type of e-mail, there is no problem. However, much of the mass e-mail sent is neither wanted nor expected by consumers. Experts estimate that in 2002, the average American e-mail account received 2,200 unsolicited bulk e-mail messages.[2] The sheer volume of unsolicited commercial e-mail or spam as it is commonly known,[3] has forced Internet service providers (ISPs) and many individual consumers to seek remedies limiting the amount received. Current approaches include: 1) technology that filters out bulk e-mail so it may never reach an e-mail account;[4] 2) legal remedies in which states make certain types of spam criminal or create a civil cause of action; and 3) industry self-regulation under which senders of bulk e-

---

*J.D., New York Law School 2004. B.A., Kalamazoo College. Clerk, Hon. Harold Baer, Southern District of New York. Associate, Cleary, Gottlieb, Steen & Hamilton. The author would like to thank Professor Beth Simone Noveck for her valuable assistance in writing this Note. Thanks also to Professor Michael Botein. All mistakes are my own.

[1] Jennifer 8.Lee, *Consumer Strategies; From Filtering to Forwarding: Ways to Fight Junk E-mail*, N.Y. TIMES, June 27, 2002, at G5. Countless examples of these kinds of solicitations are on file with the author.

[2] *Senators Aim to Force Spammers Out into the Light,* THE HOUSTON CHRON., April 11, 2003. The British government believes that spam accounts for 40% of the global e-mail traffic. This article uses data available from Jupiter Research.

[3] There are several explanations for the origin of the word "spam." The most popular is that it comes from a Monty Python skit that depicted a restaurant in which every meal contained Spam, a meat product containing pork shoulder and ham. In the skit, the word is repeated over and over the same way that the unsolicited e-mail keeps appearing in e-mail boxes. An alternative explanation is that the meat in the skit is not palatable to many people just as very few people can appreciate masses of bulk e-mail. *See* David T. Bartels, *Canning Spam: California Bans Unsolicited Commercial E-Mail,* 30 MCGEORGE L. REV. 420, at 420 (1999).

[4] Some systems employ black hole lists which stop certain domain names or servers from reaching their destination addresses. Organizations like Mail Abuse Prevention System (MAPS) offer this service to help stop the flow of unsolicited commercial e-mail. MAPS, *available at* http://mail-abuse.org/ (last visited Jan. 11, 2004). Others use white lists where only pre-approved addresses will be able to reach a particular account. All others are blocked. *Anti-Spam Group to Meet in San Francisco*, LOS ANGELES TIMES, Mar. 17, 2003, at 3.

mail have set their own parameters in response to consumer complaints.[5]

However, these current approaches are inadequate to remedy all the various complaints associated with this type of marketing. Current remedies can be either too narrow or too broad in application; the end result is unsatisfied consumers and ineffective e-mail marketers. For instance, filters may be effective in blocking unwanted mail, yet they may also create more problems by inadvertently blocking mail that is welcome or expected.[6]

On the other hand, current legal remedies may allow for too much spam if they are weak in either proscription or application, making this approach an undesirable solution on its own. The federal government was initially slow to address the problem.[7] Passing a federal law, the Can-Spam Act of 2003, while preempting the patchwork of inconsistent state legislation, may complicate the issues while creating even more problems of enforcement.[8] It also may not be effective on an international scale.[9] Spam is most often sent nationally or internationally so it is unclear if any foreign spammers would have reason or incentive to

---

[5] Organizations like the Direct Marketing Association which use unsolicited commercial e-mail as a means of advertising, suggest guidelines for online marketing as well as a "Do Not E-mail List" for consumers that only participating e-mail marketers are obliged to follow. This in addition to consumer information about e-mail solicitations can be found at Direct Marketing Association (DMA), *available at* http://www.the-dma.org/ (last visited Jan. 11, 2004).

[6] Matt Richtel, *In Spam Fight, the Opposite of a Filter,* N.Y. TIMES, Dec. 9, 2002, at C8.

[7] Dianne Plunkett Latham, *Electronic Commerce in the 21st Century; Article Spam Remedies,* 27 WM. MITCHELL L. REV. 1649, 1658.

[8] Pub. L. No. 108-187, 117 Stat. 2699 (2003). *See also* Doug Bedell, *Study Finds Law Fails to Cut Spam; Volume of Unwanted E-mails Has Actually Increased*, DALLAS MORNING NEWS, Mar. 18, 2004, at 1D; Carrie Kirby, *Spam Keeps Coming Despite the New Law*, THE SAN FRANCISCO CHRONICLE, Jan. 19, 2004, at E1. *See, e.g.,* A.R.S. § 13-3506.01 (2002); CAL BUS. & PROF. CODE § 17538.4 (2002); CONN. GEN. STAT. § 53-451 (2001); 11 DEL. CODE ANN. § 937 (2001); FLA. STAT. § 847.0138 (2002); O.C.G.A. § 16-9-93.1 (2002); IDAHO CODE § 48-603E (2002); 815 ILCS 511/1 (2003); BURNS IND. CODE ANN. § 24-5-19-1 (2002); IOWA CODE § 714E.1 (2002); LA. R.S. 14:73.1 (2003); MCLS § 750.411s (2002); MINN. STAT. § 325F.694 (2002); MISS. CODE ANN. § 97-29-45 (2002); § 407.1120 R.S.MO. (2002); NRS § 41.705 (2002); 15 OKL. ST. § 776.1 (2003); R.I. GEN. LAWS § 6-47-1 (2002); S.D. CODIFIED LAWS § 37-24-37 (2002); TENN. CODE ANN. § 47-18-1602 (2002); UTAH CODE ANN. § 13-11-4 (2003); VA. CODE ANN. § 18.2-152.1 (2002); REV. CODE WASH. (ARCW) § 19.190.005 (2002); W. VA. CODE § 46A-6G-1 (2003); WIS. STAT. § 944.25 (2002).

[9] Jonathan Bick, *Congress Has Come to Control Spam, Not to Bury It*, LEGAL TIMES, Feb. 16, 2004, at 17. *See also MX Logic Finds Only 3 Percent of Unsolicited Commercial E-mail Complied with Can-Spam Act in February, Representing No Improvement Over January*, BUSINESS WIRE, Mar. 4, 2004.

comply with current laws.[10]

Those who seek to prosecute spammers under existing laws have been successful when they can actually identify the spammer.[11] Finding spammers can be difficult because many falsify their point of origin or routing information so as not to be identified.[12] ISPs have more incentive to sue egregious spammers, because their systems are increasingly burdened by the amount of spam sent. Plus, litigation is a costly and time consuming exercise most individuals would not consider. It is perhaps easier to ignore spam or use existing consumer protections despite the inconvenience consumers continue to experience.[13] Meanwhile, the amount of spam sent has increased to the point of being considered the scourge of the information age.[14]

Most technical remedies are created to filter all spam regardless of content and are generally designed to reduce the quantity. Some states take this approach by drafting legislation to regulate the way spam is sent while others objecting to the content of the e-mail instead choose to focus on the subject matter.[15] Problems with substance are further divided between e-mail that is in some way fraudulent and that which contains offensive or sexually explicit material.[16]

Depending on what aspect they seek to regulate, different approaches in state laws have led to a mixture of constraints, each state addressing a different aspect of the problem, thus imposing inconsistent

---

[10] Stanley A. Miller II, *Getting Spam Under Control; Experts Say New Law Opens Door For More Abuse*, MILWAUKEE JOURNAL SENTINEL, Mar. 2, 2004, at 4E; Saul Hansell, *4 Big Internet Providers File Suits To Stop Leading Senders of Spam*, N.Y. TIMES, Mar. 11, 2004, at A1.

[11] *See generally* America Online, Inc. v. LCGM, Inc., 46 F.Supp.2d 444, at 447, 448. In this case, America Online sought an injunction against a spammer. The defendant admitted to hijacking domain names to send spam making recipients question whether AOL endorsed the pornographic websites. AOL sued LCGM under trademark infringement and dilution laws and existing consumer and computer crime laws. *See also* Hotmail Corp. v. Van$ Money Pie, Inc., 1998 U.S. Dist. LEXIS 10729, at 21, 22. Here, the Court enjoined Van$ Money Pie from sending e-mail using the 'hotmail' domain name. Hotmail claimed the defendant falsely designated the origin of the e-mail and violated the Computer Fraud and Abuse Act.

[12] Latham, *supra* note 7, at 1655-56.

[13] Lee, *supra* note 1, at G5.

[14] SPAMMING: HEARING BEFORE THE SUBCOMM. ON COMMUNICATIONS OF THE SENATE COMM. ON COMMERCE, SCI. & TRANSP., 105TH Cong. 2 (1998) (prepared statement of Sen. Burns), *available at* 1998 WL 12761267.

[15] David E. Sorkin, *Technical and Legal Approaches to Unsolicited Electronic Mail*, 35 U.S.F.L. REV. 325, 326-27.

[16] *Id.* at 363.

laws. Current laws should be made consistent either by states adopting uniform laws or by passage of a more comprehensive federal law that supercedes existing state laws. Where legislation ends, technology and industry self-regulation provide further measures to allow or limit the amount of spam each consumer chooses to receive. Technology will continue to improve filtering systems that will only recognize legitimate mail.[17] The end result will be a more successful and reliable method of advertising.

Part II of this Note defines the different types of spam and discusses the various incentives and challenges each type poses. It goes on to examine all current state laws and to point out inconsistencies and problems likely to be faced with compliance. Part III analyzes the benefits and problems of each remedy attempting to deal with spam on its own. Part IV addresses how legislation, technology and industry self-regulation can act in concert to effectuate a more legitimate way of doing business on the Internet. This Note draws the conclusion in Part V that the blending of either uniform state law or federal legislation and industry self regulation will help to ameliorate most of the problems associated with spam and will serve to make it a more successful and reliable method of marketing.

II. TOO MUCH SPAM CAUSES INTERNET HEARTBURN

Unsolicited commercial e-mail can be either an effective marketing tool or an annoying and persistent problem for consumers as well as ISPs depending on its future regulation. There are some benefits to this type of direct marketing. Marketers profit because the cost of sending bulk e-mail is low and still allows for reaching a mass audience. While faxes and postal mail cost the solicitor the price of a phone call or stamp, e-mail is much less expensive to send in bulk. A spammer could send fifty million e-mail messages at a cost of approximately $100. By contrast, sending the same number of messages by first-class mail, at thirty-seven cents per envelope, would cost approximately $18.5 million in postage alone.[18] Even if a marketer sees a relatively small number of responses to a bulk e-mail, it can still be extremely effective. Because it is comparatively inexpensive to send electronic solicitations in bulk, a spammer needs only a few responses to make a profit.

---

[17] Organizations like Mailblocks have created services that will ask incoming e-mail to respond by demonstrating a person sent the e-mail, not merely an automated mass-mailing machine; the system will then forward the e-mail to its recipient. John Markoff, *Start-up Finds Technology Slump Works in its Favor,* N.Y. TIMES, Mar. 24, 2003, at C4.

[18] United States Postal Service, *available at* http://pe.usps.gov (last visited Jan. 11, 2004). Bulk mail rates can be used if the sender pays an annual fee, pre-sorts and pre-stamps the envelopes.

Consumers benefit by accessing information they would not otherwise have. They regularly take advantage of e-mail advertising to buy a host of products and services such as books, movies, software, compact discs, airline tickets and vacation packages.

However, because of the relative ease with which bulk e-mail can be sent, many consumers are inundated by e-mail they did not request and did not wish to receive. The sheer volume creates a burden for consumers and ISPs in increased expenses and bandwidth.[19] There are also high costs associated with remedying spam; some consumers have been forced to abandon e-mail accounts because they run out of space while others spend time reading and deleting the e-mail.[20] ISPs' systems are burdened by the amount of e-mail traffic created. Spam uses additional bandwidth forcing ISPs to try expensive and not always effective technical solutions. For instance, spam blocking filters may be over or under inclusive in the type of spam it catches. Legitimate e-mail may be blocked or unwanted spam may get through. In addition, the content of the e-mail can be harmful when it is fraudulent, offensive or inappropriate for children. The end result is a general lack of confidence in this method of marketing. However, presumably some people must be responding positively to spam; otherwise there would be no incentive to send it.

The three current remedies employed to respond to consumer and ISP complaints are 1) technical (blocking software and services); 2) legal (federal and state laws); and 3) industry self-regulation (where marketers decide their own code of conduct). Technical solutions block all bulk e-mail from reaching users' accounts by monitoring the number of recipients and subject lines of e-mail. Questionable e-mail is usually e-mail sent to large numbers of accounts or has a subject that suggests it is an advertisement. It is either blocked entirely from a user's account, or it may be sent into a junk folder where the recipient can choose whether it is valuable or if the sender should be further blocked from the account.

Industry self-regulation is practiced by various organizations, although there is no uniform system to follow. Generally, these businesses follow a similar ethical approach as other types of

---

[19] Sorkin, *supra* note 14, at 336.

[20] The Telecommunications Research and Action Center (TRAC) is a nonprofit consumer group that launched a campaign against spam in August 2002. A website was established to help consumers send complaints to the Federal Trade Commission detailing the harms incurred as a result of spam. Telecommunications Research and Action Center, *available at* http://trac.policy.net/banspam/ (last visited Jan. 11, 2004).

marketing.[21] The idea is to make consumers aware of their products or services by e-mail while giving an opportunity to decline future solicitations.

A. The Federal Government Passes the Plate

As far as regulation governing the dissemination and filtering of spam, the federal government has been slow to act.[22] Congress initially adopted a "wait and see" attitude regarding federal spam legislation with the hope that technology and "e-etiquette" would cause a self-censorship among e-mail marketers.[23] When Congress first addressed this issue, the two bills introduced in the House of Representatives had trouble defining spam.[24] Rep. Bob Goodlatte proposed legislation in 2001 seeking to protect consumers from fraudulent (false or misleading) spam.[25] That same year Rep. Heather Wilson introduced the Unsolicited Commercial Electronic E-mail Act of 2001.[26] Its focus was to protect individuals, families and Internet service providers from unsolicited and unwanted e-mail.[27] Wilson's bill not only focused on fraudulent e-mail, but also sexually explicit e-mail and the dangers posed to child recipients. Neither of these bills was active after the end of 2001.

This past year, federal legislation was finally enacted.[28] Senator Conrad Burns first introduced the CAN-SPAM Act of 2001 in the 106th Congress and then reintroduced it in the 107th and 108th with some alterations. Its most recent incarnation, the CAN-SPAM Act of 2003 was

---

[21] The Direct Marketing Association (DMA) lists what it considers ethical business practices for marketers in its organization and makes suggestions for all online marketers. Direct Marketing Association, *supra* note 7, *available at* www.the-dma.org/guidelines/ (last visited Jan. 11, 2004).

[22] Latham, *supra* note 7, at 1658. *See* H.R. 1017, 107th Cong. (2002); H.R. 2515, 106th Cong. (2001). Just prior to publication of this Note, a federal law was passed (the CAN-SPAM Act of 2003) and signed into public law. S. Res. 877, 108th Cong. (2003)(enacted).

[23] CAN-SPAM Act of 2003, Pub. L. No. 108-187, 117 Stat. 2699 (2003). *See* Memorandum on Electronic Commerce, 33 WEEKLY COMP. PRES. DOC. 1006 (July 1, 1997). *See also* The Framework for Global Electronic Commerce, *available at* http://www.technology.gov/digeconomy/framewrk.htm. Stating that in order to effectuate the goal of people using the Internet to buy and sell products and services, governments should encourage industry self-regulation wherever appropriate. This was before spam became so pervasive and a source of consumer complaint.

[24] H.R. 1017, 107th Cong. (2002); H.R. 2515, 106th Cong. (2001).

[25] H.R. 1017, 107th Cong. (2002).

[26] H.R. 2515, 106th Cong. (2001).

[27] *Id.*

[28] CAN-SPAM Act of 2003, Pub. L. No. 108-187, 117 Stat. 2699 (2003).

signed into public law at the beginning of the year.[29] The law uses the model of best state practices by focusing on regulating fraudulent spam.[30] Specifically, the Act seeks "to prohibit senders of unsolicited commercial electronic mail from disguising the source of their messages, and to give consumers the choice to cease receiving a sender's unsolicited commercial electronic mail messages."[31]

B. States Take A Bite Out of Spam

Prior to passage of federal legislation, states rapidly passed spam laws over the past few years.[32] While they may have some deterrent value, state laws on their own lack uniformity and may have trouble reaching spammers not residing in the state from which the e-mail was sent.[33] Some laws make sending certain types of spam criminal and some create a private cause of action for the recipient. Apart from the reality that litigation is costly and time consuming, damages to recipients may be difficult to measure.[34] Spamming must be egregious and unrelenting to be worth the trouble of finding a spammer and bringing her to court. Also, current state laws are subject to scrutiny under the commerce clause, after passage of the federal Act.[35]

---

[29] S. Res. 877, 108th Cong. (2003)(enacted).
[30] CAN-SPAM Act of 2003, Pub. L. No. 108-187, 117 Stat. 2699 (2003).
[31] *Id.*
[32] ARIZ. REV. STAT. § 13-3506.01 (2003); CAL. BUS. & PROF. CODE § 17538.45 (Deering 2003); CAL. BUS. & PROF. CODE § 17529 (Deering 2003); COLO. REV. STAT. § 6-2.5-102 (2003); CONN. GEN. STAT. ANN. § 53-451 (West 2003); 11 DEL. CODE ANN. TIT. 11, § 937 (2003); FLA. STAT. ANN. § 847.0138 (West 2003); GA. CODE ANN. § 16-9-93.1 (2002); IDAHO CODE § 48-603E (Michie 2003); 815 ILL. COMP. STAT. ANN. 511/1 (West 2003); IND. CODE ANN. § 24-5-19-1 (Michie 2003); IOWA CODE § 714E.1 (2003); LA. REV. STAT. ANN. 14:73.1 (West 2003); ME. REV. STAT. ANN. TIT. 17-A, § 431 (West 2003); MD. CODE ANN., [COM. LAW] § 14-3001 (2002); MICH. COMP. LAWS § 750.411S (2003); MINN. STAT. § 325F.694 (2003); MISS. CODE ANN. § 97-29-45 (2004); MO. ANN. STAT. § 407.1120 (West 2003); NEB. REV. STAT. ANN. § 86-271 (Michie 2003); NEV. REV. STAT. ANN. § 41.705 (Michie 2004); OKLA. STAT. ANN. TIT. 15, § 776.1 (West 2003); R.I. GEN. LAWS § 6-47-1 (2003); S.D. CODIFIED LAWS § 37-24-37 (Michie 2003); TENN. CODE ANN. § 47-18-1602 (2003); UTAH CODE ANN. § 13-11-4 (2003); VA. CODE ANN. § 18.2-152.1 (2003); WASH. REV. CODE ANN. § 19.190.005 (West 2003); W. VA. CODE ANN. § 46A-6G-1 (2003); WIS. STAT. § 944.25 (2003).
[33] *See generally* State v. Heckel, 24 P.3d 404 (2001). This case involved a spammer sued under Washington spam laws for sending unsolicited e-mails from Oregon. A jurisdictional challenge was one of the defenses offered.
[34] People pay for their Internet service in different ways. Not all pay by the amount of time used. Apart from the worth of a user's time, it is difficult to measure how much time and resources ISPs expend trying to deal with spam.
[35] *Heckel*, 24 P.3d 404. The defendant in this case challenged the validity of the Washington spam law under the dormant commerce clause of the Constitution.

Before the federal law, 27 states enacted specific legislation addressing spam.[36] These spam laws created restrictions based on either e-mail that is in some way fraudulent or that which is merely annoying.[37] These restrictions served to define the type of spam subject to legislation and to limit the amount sent.[38] Most states with spam laws define spam as commercial e-mail that is unsolicited or unauthorized.[39]

By focusing on commercial advertising, fraudulent speech in particular, questions of constitutional compliance and freedom of speech

---

The case has yet to go to the federal level and may be moot under the new federal law.

[36] ARIZ. REV. STAT. § 13-3506.01 (2003); CAL. BUS. & PROF. CODE § 17538.45 (Deering 2003); CAL. BUS. & PROF. CODE § 17529 (Deering 2003); COLO. REV. STAT. § 6-2.5-102 (2003); CONN. GEN. STAT. ANN. § 53-451 (West 2003); 11 DEL. CODE ANN. TIT. 11, § 937 (2003); FLA. STAT. ANN. § 847.0138 (West 2003); GA. CODE ANN. § 16-9-93.1 (2002); IDAHO CODE § 48-603E (Michie 2003); 815 ILL. COMP. STAT. ANN. 511/1 (West 2003); IND. CODE ANN. § 24-5-19-1 (Michie 2003); IOWA CODE § 714E.1 (2003); LA. REV. STAT. ANN. 14:73.1 (West 2003); ME. REV. STAT. ANN. TIT. 17-A, § 431 (West 2003); MD. CODE ANN., [COM. LAW] § 14-3001 (2002); MICH. COMP. LAWS § 750.411S (2003); MINN. STAT. § 325F.694 (2003); MISS. CODE ANN. § 97-29-45 (2004); MO. ANN. STAT. § 407.1120 (West 2003); NEB. REV. STAT. ANN. § 86-271 (Michie 2003); NEV. REV. STAT. ANN. § 41.705 (Michie 2004); OKLA. STAT. ANN. TIT. 15, § 776.1 (West 2003); R.I. GEN. LAWS § 6-47-1 (2003); S.D. CODIFIED LAWS § 37-24-37 (Michie 2003); TENN. CODE ANN. § 47-18-1602 (2003); UTAH CODE ANN. § 13-11-4 (2003); VA. CODE ANN. § 18.2-152.1 (2003); WASH. REV. CODE ANN. § 19.190.005 (West 2003); W. VA. CODE ANN. § 46A-6G-1 (2003); WIS. STAT. § 944.25 (2003).

[37] *See, e.g.*, N.C. GEN. STAT. § 14-458 (2003). North Carolina focuses its law on spammers who falsely identify themselves with intent to deceive or defraud the recipient. Conversely, Nevada requires only an opt-out instruction. NEV. REV. STAT. ANN. § 41.730 (Michie 2004).

[38] *See, e.g.*, COLO. REV. STAT. § 6-2.5-102 (2003).

[39] ARIZ. REV. STAT. § 13-3506.01 (2003); CAL. BUS. & PROF. CODE § 17538.45 (Deering 2003); CAL. BUS. & PROF. CODE § 17529 (Deering 2003); COLO. REV. STAT. § 6-2.5-102 (2003); CONN. GEN. STAT. ANN. § 53-451 (West 2003); 11 DEL. CODE ANN. TIT. 11, § 937 (2003); FLA. STAT. ANN. § 847.0138 (West 2003); GA. CODE ANN. § 16-9-93.1 (2002); IDAHO CODE § 48-603E (Michie 2003); 815 ILL. COMP. STAT. ANN. 511/1 (West 2003); IND. CODE ANN. § 24-5-19-1 (Michie 2003); IOWA CODE § 714E.1 (2003); LA. REV. STAT. ANN. 14:73.1 (West 2003); ME. REV. STAT. ANN. TIT. 17-A, § 431 (West 2003); MD. CODE ANN., [COM. LAW] § 14-3001 (2002); MICH. COMP. LAWS § 750.411S (2003); MINN. STAT. § 325F.694 (2003); MISS. CODE ANN. § 97-29-45 (2004); MO. ANN. STAT. § 407.1120 (West 2003); NEB. REV. STAT. ANN. § 86-271 (Michie 2003); NEV. REV. STAT. ANN. § 41.705 (Michie 2004); OKLA. STAT. ANN. TIT. 15, § 776.1 (West 2003); R.I. GEN. LAWS § 6-47-1 (2003); S.D. CODIFIED LAWS § 37-24-37 (Michie 2003); TENN. CODE ANN. § 47-18-1602 (2003); UTAH CODE ANN. § 13-11-4 (2003); VA. CODE ANN. § 18.2-152.1 (2003); WASH. REV. CODE ANN. § 19.190.005 (West 2003); W. VA. CODE ANN. § 46A-6G-1 (2003); WIS. STAT. § 944.25 (2003).

issues may be avoided.[40] While there is constitutional protection for free speech, the same protections do not apply to fraudulent speech.

States generally define unsolicited e-mail as having no "[c]urrent or prior business relationship" between the parties.[41] This requires either that "[t]he recipient has indicated a willingness to receive commercial electronic mail messages from that sender...," the recipient has purchased goods or services from the sender in the past, or in situations where the recipient has an ongoing contract with the sender, the message directly concerns the ongoing contract.[42] This definition narrows the type of e-mail subject to legislation. Prior business relationships suggest the requisite willingness to receive more e-mail, removing the assumption that unsolicited advertisements are unwanted. For example, an e-mail advertising special rates on software accessories for a computer purchased from the same company would possibly be of interest to a consumer. In addition to the legislature's definition, a few states defer to ISPs' policy definitions of what constitutes spam.

Some states include specific provisions about jurisdiction while others are silent. The same is true for statutes of limitations on potential claims. States either make spamming a criminal offense, provide a civil cause of action, or allow both.

Once the type of e-mail is defined, states further categorize e-mail based on content. The most popular approach taken is an extension of state and federal consumer law as described in the Federal Trade Commission Act dealing with unfair and deceptive trade acts.[43] It extends consumer protection laws dealing with false or misleading advertising to apply to the content of an e-mail. Fraudulent spam can also be defined by the technology used to falsify information with the intent of misleading the recipient.[44] These laws target spammers sending advertising who wish not to be identified, spammers advertising questionable

---

[40] *See generally* Joshua A. Marcus, *Commercial Speech on the Internet: Spam and the First Amendment*, 16 CARDOZO ARTS & ENT. L.J. 245 (1988). This Note discusses the constitutionality of a regulation against intrusive Internet advertising and how it would have to pass First Amendment muster under the commercial speech doctrine.

[41] *See, e.g.*, COLO. REV. STAT. § 6-2.5-102 (2003). The Colorado Junk E-mail Law appears as part of the state's other consumer and commercial laws, specifically under fair trade and restraint of trade.

[42] *Id.*

[43] 15 U.S.C. § 45 (2003).

[44] *See, e.g.*, LA. REV. STAT. ANN. 14:73.6 (West 2003). Louisiana, like many other states with spam laws, prohibits falsifying an e-mail and also makes it unlawful to sell, distribute or possess any software enabling a computer user to falsify an e-mail.

merchandise, as well as spammers using classic common confidence schemes that have found a new life on the Internet.[45]

States most concerned with protecting consumers focus on restricting fraud through e-mail.[46] The threshold is when spam is sent "with the purpose to devise or execute a scheme to defraud or illegally obtain property."[47] If, with that purpose, the sender of an e-mail falsifies or forges any data included in the transmission, it will be considered unlawful.[48] This includes any false or forged data in the header.[49] The header incorporates the sender's identity along with other information about the source and routing information. It also includes the subject of the e-mail. By restricting false or misleading information contained in the header, a spammer violates the law by hijacking an unwitting user's domain name to misrepresent the point of origin. Hijacking an e-mail account enables spammers to remain anonymous, while ensuring that the hijacked account and not the spammer receives all replies, either from angry consumers or bounced back mail from inactive accounts. It also includes any spammers who create false identities used in confidence schemes.

A recent spam scam using a false identity purports to be from the son of a South African diplomat who needs a safe American bank account to store $15 million to ensure the political safety of his country.[50] The e-mail address where the message originated simply does not exist. The body of the e-mail states an alternate way of contacting the supposed political refugee.[51] It resembles a typical confidence scheme covered traditionally by consumer protection laws, but some states with spam laws spell out the offence as it occurs in e-mail form by including this type of deception in the laws about appropriate headers.[52]

The header also includes routing instructions or the time and date stamp that appears on each e-mail.[53] Typically, spammers will set this

---

[45] *See, e.g.*, N.C. GEN. STAT. § 14-458 (2003).
[46] ARK. CODE ANN. § 5-41-205 (2003).
[47] *Id.*
[48] *Id.*
[49] *Id.*
[50] The author received this spam and then two days later received the same e-mail from a different person purporting to be in the same situation. The spam e-mail is on file with the author.
[51] The United States Secret Service posted a fraud advisory on their website warning recipients not to send any money or give any information about their bank accounts. United States Secret Service, Public Awareness Advisory Regarding "4-1-9" or "Advance Fee Fraud" Schemes, *at* http://www.secretservice.gov/alert419.shtml.
[52] ARK. CODE ANN. § 5-41-205 (2003).
[53] *Id.*

information to an earlier date so that spam e-mail appears first in a recipient's in-box. Also a part of the header is the subject line, making it unlawful to misrepresent the content of an e-mail.[54] Spammers get consumers to open their mail by making the subject seem personal to the recipient. For example, a spammer might put "Do you remember your old friend John?" or "Confirmation about your checking account". By personalizing false subjects for their e-mail, recipients believe the e-mail is important to open. This trick is used by spammers to ensure their e-mail is read and not simply deleted.

States regulating false or misleading headers usually include a provision incriminating anyone who sells or possesses software that enables a computer user to falsify or misrepresent herself in the header.[55] They also stipulate that ISPs are relieved of any liability for sending spam on behalf of another person, unless the ISP itself sends the spam.[56]

Another common type of law is the opt-out provision.[57] It requires a way to contact the sender either by a reliable return e-mail address, a toll-free phone number, or a business address.[58] Some laws also impose limitations on honoring the requests not to receive any more e-mail.[59]

Finally, some laws require senders to label solicitations to give the recipient an opportunity to delete it without reading it.[60] States vary in approaches by restricting spam in one or a hybrid of these ways. Because many of the state laws are different in structure and purpose, combining one or more of the approaches described above, it is important to look at them individually in order to assess the effectiveness of different approaches in dealing with fraudulent users.

1. Laws Against Fraudulent Spam

The laws described above take a similar approach to the Federal Trade Commission Act regarding unfair and deceptive trade acts, focusing on false, fraudulent, or misleading commercial e-mail.[61]

---

[54] *Id.*
[55] *Id.*
[56] *Id.*
[57] *See, e.g.*, CAL. BUS. & PROF. CODE § 17538.45 (Deering 2003); CAL. BUS. & PROF. CODE § 17529 (Deering 2003).
[58] *See, e.g.*, R.I. GEN. LAWS § 6-47-2 (2003). Rhode Island places its spam laws along with telephone and fax solicitation laws.
[59] *See id. See also* NEV. REV. STAT. ANN. § 41.730 (Michie 2004). Nevada's spam law requires no such provision.
[60] *See, e.g.*, NEV. REV. STAT. ANN. § 41.730 (Michie 2004). Nevada requires all e-mail solicitation to be labeled ADV.
[61] 15 U.S.C. § 45 (2003).

Arkansas prohibits any scheme to defraud by sending e-mail with false header information.[62] The state also forbids selling, giving, or possessing any means to falsify the header, subject line, or routing instructions of an e-mail.[63] Arkansas law makes any violation a felony offense, but because it is not explicitly stated, it is unclear whether the law pertains to e-mail sent from either within the state, to a state resident, or both.[64]

Connecticut takes a similar approach by making it illegal to "[f]alsify or forge electronic mail transmission information or other routing information in any manner in connection with the transmission of unsolicited bulk electronic mail through or into the computer network of an electronic mail service provider or its subscribers."[65] It is also unlawful to sell or distribute software designed to facilitate falsification.[66] Violation is a misdemeanor, except in situations where there is damage to the property of another person in an amount exceeding two thousand five hundred dollars to two or more people, in which case it becomes a felony.[67] However, this does not apply to Connecticut-based e-mail service providers and there is no liability to a provider who prevents the transmission of e-mail that violates this law.[68]

In addition to criminal liability, the Connecticut law provides for a civil cause of action for people whose property or person is injured by a violation.[69] Individuals can enjoin and recover actual damages, including loss of profits.[70] Individuals may also recover reasonable attorneys' fees and costs and may elect, "in lieu of actual damages, to recover the lesser of ten dollars for each and every unsolicited bulk electronic mail message transmitted...or twenty-five thousand dollars per day for each day of violation."[71] ISPs may also recover reasonable attorneys' fees and in lieu of actual damages, recover the greater of ten dollars for each and every unsolicited bulk electronic mail message or twenty five thousand dollars per day.[72] There is a two year statute of limitations from the date the offending e-mail is sent and personal jurisdiction is subject to Connecticut's long-arm statute.[73]

---

[62] *See* ARK. CODE ANN. § 5-41-205 (2003).
[63] *Id.*
[64] *Id.*
[65] CONN. GEN. STAT. ANN. § 53-451 (2003).
[66] *Id.*
[67] *Id.*
[68] *Id.*
[69] *Id.*
[70] *Id.*
[71] *Id.*
[72] *Id.*
[73] *Id.*

The law is unclear about what constitutes specific damage and could be interpreted as specific harm to person or property, and not necessarily harm in the form of time and account space taken by the bulk e-mail. This is a harder standard to meet than the general complaint of the amount of spam received. It might include situations where an individual is harmed by having her domain name hijacked to send bulk e-mail. She might not be able to access her account if her ISP's anti-spam filters shut it down. She might also have her account filled with responses to the bulk e-mail either from inactive accounts or from responses from recipients wanting to opt-out. If the e-mail address is one used to conduct business, the law provides damages for lost profits.

Delaware makes unrequested or unauthorized e-mail a computer crime.[74] Bulk e-mail is unrequested or unauthorized if it is sent "intentionally or recklessly" without a request from, or a prior business relationship with, the recipient.[75] An ISP is not liable for any bulk e-mail sent over its network and any "good faith" efforts taken to block receipt or transmission of bulk e-mail.[76] This precludes individuals from any action against an ISP for either blocking a bulk e-mail from being sent or received so long as the ISP reasonably believed it was blocking a violating e-mail.

Delaware also has a fraud provision prohibiting false or forged electronic mail information "in any manner in connection with the transmission of unsolicited bulk electronic mail."[77] This is not as specific as the laws of other states, but it conveys the same message about falsifying any header information. Delaware also makes it illegal to possess deception-enabling software.[78] Offending spam sent from another state is subject to Delaware's long arm statute, "if the receiving address or account was under the control of any authorized user of a computer system who was located in Delaware at the time he or she received the electronic mail or communication and the defendant was aware of circumstances which rendered the presence of such authorized user in Delaware a reasonable possibility."[79] When a reasonable possibility exists is difficult to determine. There may always be a possibility of reaching an e-mail account in Delaware or any state when sending a bulk e-mail. Most e-mail accounts do not exhibit any information to identify the state where a user resides. A spammer may have some idea if the e-mail list came from a local group, but otherwise there is no definitive way to tell.

---

[74] DEL. CODE ANN. TIT. 11, § 937 (2001).
[75] *Id.*
[76] *Id.*
[77] *Id.*
[78] *Id.*
[79] *Id.*

Illinois' Electronic Mail Act defines spam as an "unsolicited electronic mail advertisement," specifically those sent where no prior or existing business or personal relationship exists and where it is sent without request or express consent.[80] This law is explicit in its prohibition of fraudulent material. "No individual or entity may initiate...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."[81] A civil cause of action is created for individuals and ISPs who suffer actual damages as a result of a violation as well as criminal liability if the e-mail also violates state consumer protection laws under the Consumer Fraud and Deceptive Business Practices Act.[82]

Individuals can recover in actual damages as a result of a violation. The injured person may recover attorney's fees and costs, and may elect, in lieu of actual damages, to recover the lesser of $10 for each spam sent or twenty five thousand dollars per day.[83] ISPs suffering actual damages may also recover in the same amounts.[84] Illinois law prohibits action against ISPs for either sending spam in violation of the provision, or blocking complying e-mail so long as the blocking action was taken in "good faith."[85]

The law only applies when the spam is sent to an Illinois resident via an ISP's service or equipment located in the state, but says nothing about spammers outside the state.[86] There is no knowledge requirement, but it is unclear if this statute would apply to an out of state spammer, which would seriously reduce its enforceability.

North Carolina makes it unlawful to "[f]alsely identify with the intent to deceive or defraud the recipient or forge commercial electronic mail transmission information or other routing information in any manner in connection with the transmission of unsolicited bulk commercial electronic mail."[87] In addition to criminal liability, if there is damage to property as a result, individuals may sue and recover damages.[88] This law is broader

---

[80] 815 ILL. COMP. STAT. 511/5 (2003). Illinois' Electronic Mail Act became effective on January 1, 2000.
[81] *Id.*
[82] 815 ILL. COMP. STAT. 511/10 (2003); 815 ILL. COMP. STAT. 511/15 (2003).
[83] 815 ILL. COMP. STAT. 511/10 (2003).
[84] *Id.*
[85] *Id.*
[86] *Id.*
[87] N.C. GEN. STAT. § 14-458 (2002).
[88] *Id.*

than some, containing no exemption for ISPs or liability for selling or possessing facilitating software. Nor does it mention if the law pertains only to recipients within the state or if out-of-state spammers can also be reached. These absent provisions could prove to dilute the effectiveness of the law.

Louisiana, on the other hand, has a more comprehensive spam law, but it defers to the policies of ISPs to define spam.[89] This is one of the only states that makes commercial spamming a criminal offense and gives authority to ISPs to determine policies in which e-mails may be sent or blocked. It goes slightly further than states which merely remove liability from ISPs for facilitating fraudulent spam. E-mail by an organization to its members and noncommercial e-mails are exempt.[90] The statute goes on to define other instances where spam may be unlawful by prohibiting false or forged transmission information or other routing information in any manner.[91] There is also a provision prohibiting enabling software.[92] Although a criminal offense, there is a relatively small penalty for spamming; violators will not be fined more than five thousand dollars.[93] Missing from the law is any indication of whether it only pertains to intra-state spamming or if it reaches spammers from other states.

Maryland's spam laws focus on prohibiting fraudulent e-mails, but rather than appearing under local criminal laws, they are part of the consumer protection provisions.[94] They do not apply to ISPs to the extent that they merely act as a facilitator and do not endorse offensive spam.[95] The laws prohibit hijacking domain names to send spam, containing false or misleading information about the origin or routing information, or a subject line which could deceive the recipient.[96] Out of state spammers who know or should know they are sending e-mails into the state may be liable. The law creates a presumption that the sender knows the recipient is a resident of the state "if the information is available on request from the registrant of the Internet domain name contained in the recipient's electronic mail address."[97] This built-in presumption makes it easier to prosecute out of state spammers.

---

[89] LA. R.S. 14:73:6 (2003).
[90] *Id.*
[91] *Id.*
[92] *Id.*
[93] *Id.*
[94] MD. COMMERCIAL LAW CODE ANN. § 14-3001 (2002).
[95] *Id.*
[96] *Id.*
[97] *Id.*

ISPs are not liable for either facilitating spam or blocking it, provided there is a reasonable belief the e-mail was not compliant with the statute and the action taken to block it was in good faith.[98] The good faith provision protects ISPs from accidentally blocking bulk e-mail sent to groups of people who belong to groups requesting it, as well as noncommercial, religious or educational information.

Penalties for violation of Maryland's law, in addition to reasonable attorney's fees, include damages of either five hundred dollars or actual damages, whichever amount is greater.[99] ISPs are entitled to the greater amount of one thousand dollars or actual damages.

Oklahoma's spam law is also housed in its Consumer Protection Act.[100] Fraudulent spam is unlawful under the statute if it misrepresents or does not contain any information in identifying the point of origin or the transmission path of any spam (regardless of whether it is commercial or not), or contains "false, malicious, or misleading information which purposely or negligently injures a person."[101] Violation carries a penalty of no more than five hundred dollars; however, injured persons may recover the lesser of ten dollars for each spam, or twenty-five thousand dollars per day in damages sustained.[102]

There is also an exemption for ISPs for either transmitting or blocking spam.[103] Sending spam to a recipient, or through an ISP inside the state is considered an act within the state and the spammer is subject to the state spam law.[104] There is no knowledge requirement, but the law nonetheless asserts jurisdiction against noncompliant out-of-state spammers.

South Dakota prohibits transmission of any false or misleading commercial spam.[105] It applies to spam sent inside the state and an e-mail sent to an address the sender knows or has a reason to know is held by a state resident.[106] Knowledge is implied if information that the recipient is a South Dakota resident is available from the registrant of the ISP.[107] The law prohibits hijacking domain names, or any misrepresented or obscured information in identifying the point of origin or routing

---

[98] *Id.*
[99] MD. COMMERCIAL LAW CODE ANN. § 14-3003 (2002).
[100] 15 OKLA. STAT. § 776.1 (2003).
[101] *Id.*
[102] *Id.*
[103] *Id.*
[104] *Id.*
[105] S.D. CODIFIED LAWS § 37-24-37 (2002).
[106] *Id.*
[107] *Id.*

information, or false or misleading information in the subject line.[108]

Pennsylvania has passed a fraudulent spam law.[109] The Unsolicited Telecommunication Advertisement Act applies to fax as well as e-mail solicitations.[110] The general rule prohibits initiating unsolicited commercial e-mail either sent within the state or sent to an address that the sender knows or has reason to know is held by a resident of the state.[111] The law reads in a presumption of knowledge if information identifying the recipient as a state resident is available from the registrant of the Internet domain name contained in the recipient's e-mail message.[112] Prohibited spam includes e-mail that hijacks a domain name, misrepresents or obscures any information identifying the point of origin or routing information, includes a false or misleading return address, or contains false or misleading information in the subject line.[113] The law also requires that unsolicited e-mail contain a valid return e-mail address or toll-free phone number so recipients may opt out of receiving any future solicitations.[114] There is also immunity for ISPs who block legitimate e-mail.[115] ISPs are also given immunity in exercising discretion in suspending or terminating service to any person acting in violation of this act.[116] Consumers are afforded a civil cause of action and courts are given discretion to increase an award amount up to one million, five hundred thousand dollars for willful violations.[117]

Tennessee makes it unlawful to send unsolicited advertising material that would be considered unfair or deceptive under the state Consumer Protection Act.[118] Spammers liable under this law have either disrupted the "normal flow of business" of the recipient or "engaged in a pattern or practice of refusing to comply with requests of those who have notified the initiator that the recipient does not want to receive any further unsolicited...e-mail messages from the initiator."[119] Spammers are subject to penalties and remedies under the state's consumer protection laws.[120] Tennessee's law has no specific provisions about false or misleading header information, but it could certainly be read into the

---

[108] *Id.*
[109] 73 PA. STAT. ANN. § 2250.3 (2003).
[110] *Id.*
[111] *Id.*
[112] *Id.*
[113] *Id.*
[114] *Id.*
[115] 73 PA. STAT. ANN. § 2250.6 (2003).
[116] *Id.*
[117] 73 PA. STAT. ANN. § 2250.8 (2003).
[118] TENN. CODE ANN. § 47-18-1602 (2002).
[119] *Id.*
[120] *Id.*

consumer protection laws. It also provides immunity for ISPs for facilitating or blocking e-mail, so it is unclear if there would be liability in that regard.

Virginia's Computer Crimes Act makes it unlawful to "falsify or forge electronic mail transmission information or other routing information in any manner in connection with the transmission of unsolicited bulk electronic mail."[121] It is also unlawful to sell, give or possess enabling software to facilitate false or forged information.[122] In addition, Virginia has a broad computer harassment law making it illegal to harass any person by communicating "obscene, vulgar, profane, lewd, lascivious, or indecent language."[123] An act of a spammer sending a large quantity of pornographic solicitations to the same e-mail addresses might rise to the level of harassment under the statute and spammers could be prosecuted under this provision. There is a statute of limitations of five years after sending the last e-mail, or one year after the existence of the illegal act and the identity of the offender are discovered.[124] The statutory clock starts after the spammer's identity is known. This helps those damaged by such a violation when the spammer has concealed his or her identity.

Washington's spam law also prohibits fraudulent spam sent either from a computer in the state or to an address the sender knows or has reason to know is held by a state resident.[125] It is unclear if this law applies when the recipient is checking e-mail from another state. Knowledge is implied if information on a resident's status is available from the registrant of the Internet domain name contained in the recipient's electronic mail address.[126] The law prohibits hijacking a third party's domain name, or sending a commercial e-mail that contains false or misleading information in the subject line.[127] Damages for individual recipients are the amount of actual damages or five hundred dollars, whichever is greater. ISPs are entitled to the greater amount of one thousand dollars or actual damages.[128] ISPs are immune from liability for both sending non-compliant spam and blocking compliant e-mail so long as the good faith provision is met.[129]

Washington is one state that has tested the constitutionality of its spam law. Recently the Washington State Supreme Court held that the

---

[121] VA. CODE ANN. § 18.2-152.4 (2002).
[122] *Id.*
[123] VA. CODE ANN. § 18.2-152.7:1 (2002).
[124] *Id.*
[125] REV. CODE WASH. (ARCW) § 19.190.020 (2002).
[126] *Id.*
[127] *Id.*
[128] REV. CODE WASH. (RCWA) § 19.190.040 (2002).
[129] REV. CODE WASH. (RCWA) § 19.190.050 (2002).

statute did not violate the Dormant Commerce Clause of the Constitution and upheld the judgment against a spammer who sent large volumes of unsolicited commercial e-mail to Washington e-mail addresses.[130]

Wyoming is the newest state to introduce spam legislation.[131] The law prohibits sending commercial e-mail to an address the sender knows or has reason to know is held by a Wyoming resident that uses a third party's domain name or otherwise misrepresents any information identifying the point of origin or transmission path.[132] The law also prohibits any false or misleading information in the subject line.[133]

The statute gives Wyoming's Attorney General authority to investigate and bring action against spammers.[134] ISPs are immune from liability for both re-transmitting spam and blocking e-mail it reasonably believes is sent in violation of the law.[135]

2. Laws Requiring Opt-Out Provisions for Commercial but Non-Fraudulent E-mail

Some state spam laws are not concerned with fraudulent so much as annoying content. These states require an opt-out provision to be included in each solicitation so that individuals can decide for themselves what type of e-mail they want to receive.

Nevada was the first state to enact spam legislation in 1997.[136] The law does not mention fraudulent content or routing information, but it was passed before many of the clever spammers started using these devices to ensure their messages were received. The law does require that e-mail advertisements comply with certain restrictions.[137] First, there must be a preexisting business or personal relationship with the recipient or the recipient must have expressly consented to receive the e-mail.[138] If the e-mail is unsolicited and no preexisting relationship exists, the e-mail must be "readily identifiable as promotional, or contain[ing] a statement providing that it is an advertisement and clearly and conspicuously provides: (1) the legal name, complete street address and electronic mail address of the person transmitting the electronic mail; and (2) a notice

---

[130] State v. Heckel, 24 P.3d 404 (Wash. 2001).
[131] 2003 WY. ALS 86.
[132] *Id.*
[133] *Id.*
[134] *Id.*
[135] *Id.*
[136] Sabra-Anne Kelin, *State Regulation of Unsolicited Commercial E-Mail*, 16 BERKELEY TECH. L.J. 435, 445 (2001).
[137] NEV. REV. STAT. ANN. § 41.730 (Michie 2002).
[138] *Id.*

that the recipient may decline to receive additional electronic mail that includes an advertisement from the person transmitting ... and procedures for declining such electronic mail."[139] It does not expressly require that the spammer stop sending e-mail after an opt-out is exercised, but does allow recipients to enjoin the spammer from sending any more solicitations and claim civil damages for noncompliance.[140] There is immunity for ISPs for sending, but not for blocking spam.[141] No specific mention is made as to whom the law applies, so individuals would need to sue out of state spammers using Nevada's long arm statute.[142]

Missouri has a whole chapter of law dedicated to electronic mail practices.[143] It prohibits unsolicited commercial e-mail without a valid sender-operated return e-mail address or toll-free number so that recipients may opt-out.[144] ISPs are immune from liability for sending as well as blocking spam.[145] Damages for individuals are the greater amount of five hundred dollars or actual damages.[146] ISPs can recover one thousand dollars or actual damages, whichever is greater.[147] Missouri expressly states that any federal law will immediately supercede this law.[148] Absent from this statute is any prohibition of fraudulent or misleading header information or labeling as an advertisement.

3. Content-Based Legislation: Laws Requiring Labeling

Some spam laws focus specifically on labeling either as commercial advertisements or as sexually explicit material only suitable for adults. California's spam law has such a requirement.[149] All unsolicited commercial e-mail, that is not requested and where there is no prior relationship, must include "ADV:" as the first four characters in the subject line.[150] This way a recipient will know before opening an e-mail that it contains an advertisement. Presumably it is also a measure against confusing or misleading subject lines that entice a recipient to open it. If the commercial goods or services are for individuals eighteen and older, the subject line must have "ADV:ADLT" as the first eight characters.[151]

---

[139] *Id.*
[140] *Id.*
[141] NEV. REV. STAT. ANN. § 41.735 (Michie 2002).
[142] NEV. REV. STAT. ANN. § 41.730 (Michie 2002).
[143] MO. ANN. STAT. § 407.1120 (West 2002).
[144] MO. ANN. STAT. § 407.1123 (West 2002).
[145] MO. ANN. STAT. §§ 407.1123, 1132 (West 2002).
[146] MO. ANN. STAT. § 407.1129 (West 2002).
[147] *Id.*
[148] MO. ANN. STAT. § 407.1132 (West 2002).
[149] CAL. BUS. & PROF. CODE § 17538.4 (Deering 2002) (repealed 2003).
[150] *Id.*
[151] *Id.*

This has the same effect of warning recipients of the contents before they open e-mail. The hope is to save recipients from the psychic harm of opening sexually explicit material without knowing its contents.

In addition to the labeling requirement, unsolicited commercial e-mail must have an opt-out provision in the form of a toll-free telephone number, a valid return address, or valid sender-operated e-mail address.[152] This text must be at the very beginning of the e-mail and must be the same size as the rest of the text in the message.[153] This is the only state that demands the opt-out be placed so conspicuously in the e-mail. There is also a provision that upon notification, spammers must not send any more e-mail to the objecting recipient.[154] It also provides for an employer to opt-out on behalf of all of the employees who might also receive spam.[155] The law states that it will become inoperative after federal law is enacted that also regulates spam.[156]

Like Washington, California's law has also been tested under Dormant Commerce Clause scrutiny. In *Ferguson v. Friendfinders, Inc.*, the California Court of Appeals held that the law did not violate the Dormant Commerce Clause because it did not discriminate against or directly regulate commerce occurring wholly outside the state.[157] It only applied when spam was sent to a California resident. The law claims only to apply to those conducting business within the state and makes no knowledge requirement of senders from outside the state.[158] Therefore, the burdens imposed on interstate commerce were minimal and did not outweigh the benefits of the law.[159] The court stated that the law furthers an important interest in regulating deceptive spam.[160]

Wisconsin's law does not address fraudulent e-mail or require an opt-out, but only seeks to control unsolicited e-mail solicitations that contain "obscene material or a depiction of sexually explicit conduct."[161] The law requires the subject line of such e-mail to contain the words "Adult Advertisement."[162] It is part of a larger statute regulating crimes against sexual morality. Many of the typical concerns of other types of

---

[152] *Id.*
[153] *Id.*
[154] *Id.*
[155] *Id.*
[156] *Id.*
[157] Ferguson v. Friendfinders, Inc., 115 Cal. App. 4th 1255 (1st Dist. 2002).
[158] CAL. BUS. & PROF. CODE § 17538.4 (Deering 2002) (repealed 2003).
[159] *Ferguson*, 115 Cal. App. 4th at 1269.
[160] *Id.*
[161] WIS. STAT. ANN. § 944.25 (West 2002).
[162] *Id.*

spam are not addressed.[163]

4. Hybrid Laws

The remaining spam laws enacted by state legislatures use some combination of the fraudulent restrictions, opt-out requirement and/or labeling obligations.

West Virginia combines a law against fraudulent as well as pornographic spam.[164] The law prohibits unauthorized e-mail with the intent to deceive and defraud that either hijacks a domain name or otherwise misrepresents any information identifying the point of origin or transmission path, has a false or misleading subject line, or does not "clearly provide the date and time the message was sent, the identity of the person sending the message, and the return electronic mail address of that person."[165] Also, unauthorized e-mail with the intent to deceive and defraud may not contain "sexually explicit materials" defined as "visual depiction, in actual or simulated form, or an explicit description in a predominately sexual context, nudity, human genitalia, or any act of natural or unnatural sexual intercourse."[166]

The law applies to e-mail addresses that the sender either knows or has reason to know are held by residents of West Virginia.[167] However, the law does not define the knowledge requirement. It does go on to say that sending e-mail to a recipient within the state constitutes an act within the state subjecting the sender to its laws.[168] In addition, ISPs have immunity for either transmitting spam or blocking e-mail it believes in good faith violates these provisions.[169] Under the law, it is also prohibited for anyone to sell, give, distribute, or possess software that enables falsification of electronic mail transmission information.[170]

Recipients of e-mail violating this law may enjoin the sender or be entitled to reasonable attorney fees as well as actual damages for injury or a minimum damage assessment of one thousand dollars.[171] The law provides for punitive damages for "the willful failure to cease initiating" spam.[172] ISPs are entitled to damages as well as loss of profits or the

---

[163] *Id.*
[164] W. VA. CODE § 46A-6G-2 (2003).
[165] *Id.*
[166] *Id.*
[167] *Id.*
[168] W. VA. CODE § 46A-6G-5 (2003).
[169] W. VA. CODE § 46A-6G-3 (2003).
[170] W. VA. CODE § 46A-6G-4 (2003).
[171] W. VA. CODE § 46A-6G-5 (2003).
[172] *Id.*

greater amount between ten dollars per spam in violation or twenty-five thousand dollars per day.[173]

Idaho's law combines fraudulent and opt-out provisions in its spam law.[174] First, it is unlawful to send bulk e-mail advertisements by hijacking a domain name, misrepresenting any information in identifying the point of origin of the transmission path or failing to identify the point of origin.[175] Second, all bulk e-mail advertisements must contain a return e-mail address so the recipient may opt-out of receiving future e-mail.[176] It is also unlawful to send e-mail within five days of a recipient exercising the opt-out provision.[177]

ISPs are exempt from liability for transmitting spam in violation of the law and from good faith efforts to block spam it reasonably believes to be in violation.[178] In actions for damages in violation of these provisions, one may recover either actual damages or the greater of one hundred dollars for each e-mail sent or one thousand dollars.[179]

Iowa also combines fraudulent e-mail restrictions and opt-out provisions for unwanted commercial e-mail.[180] It is unlawful to send bulk e-mail that either uses the name of a third party in the return address field without permission, or misrepresents or does not include information identifying the point of origin or transmission path.[181] If the bulk e-mail is unsolicited, it must, at a minimum, provide an e-mail address so the recipient may opt-out.[182] It is also unlawful to send e-mail to an address five days after the recipient has exercised the opt-out provision.[183] The language suggests that sending one or two e-mails after an individual declines future e-mail would not rise to the level of a violation but rather the law intends to target spammers who pay no attention to repeated attempts to opt-out.[184]

Persons and ISPs injured are entitled to either an injunction or damages including lost profits and reasonable attorney fees.[185] The

---

[173] *Id.*
[174] IDAHO CODE § 48-603E (Michie 2002).
[175] *Id.*
[176] *Id.*
[177] *Id.*
[178] *Id.*
[179] *Id.*
[180] IOWA CODE § 714E.1 (2002).
[181] *Id.*
[182] *Id.*
[183] *Id.*
[184] *Id.*
[185] *Id.*

recipient may choose between actual damages and the greater of ten dollars for each e-mail sent or five hundred dollars.[186]

ISPs are exempt from liability under this statute for both the mere act of re-transmitting illegal e-mail and for blocking e-mail so long as it was done in good faith.[187] Also exempt are electronic bulletin boards and free e-mail accounts where terms of access require users to receive spam.[188]

Ohio also prohibits fraudulent e-mail solicitations and requires an opt-out provision for unsolicited commercial e-mail.[189] The e-mail must contain a no-cost way for the recipient to decline any future solicitations and the opt-out requests must be honored by senders.[190] There is no ISP liability for retransmitting spam or for blocking e-mail it believes in good faith to be in violation of the law.[191]

All unsolicited commercial e-mail must contain the sender's name, e-mail address and complete residence or business address.[192] The law prohibits falsifying the originating address or other routing information in connection with the transmission of an unsolicited commercial e-mail.[193] Recipients of e-mail in violation have a civil cause of action and may recover up to fifty thousand dollars and reasonable attorney's fees.[194]

Rhode Island begins with an opt-out approach to regulating spam.[195] Unsolicited commercial e-mail must have a toll-free telephone number or a valid return e-mail address so the recipient may notify the sender not to e-mail any future solicitations.[196] The law also restricts spammers from sending any additional e-mail solicitations to addresses that have exercised the opt-out instruction.[197] This state also prohibits hijacked domain names or otherwise fraudulent misrepresentations in the point of origin or transmission path of a commercial e-mail.[198] The law applies to e-mail sent within the state as well as to an address that the

---

[186] *Id.*
[187] *Id.*
[188] *Id.*
[189] OHIO REV. CODE ANN. § 2307.64 (Anderson 2002).
[190] *Id.*
[191] *Id.*
[192] *Id.*
[193] *Id.*
[194] *Id.*
[195] R.I. GEN LAWS § 6-47-2 (2002).
[196] *Id.*
[197] *Id.*
[198] *Id.*

sender knows, or has reason to know, is held by a state resident.[199] The knowledge requirement is met if the recipient has requested not to receive any further e-mail.[200] This is different from other states that provide the information of residency by request from ISPs. The sender becomes liable if the recipient can prove she tried to exercise the opt-out provision. There is also immunity for ISPs because they merely carry the transmission over the network.[201] Spammers who violate this law can be liable for damages to the recipient up to one hundred dollars for each violation in addition to reasonable attorney's fees.[202]

By far the most restrictive and comprehensive of the spam laws are those that combine the requirement of content regulations, including an opt-out and labeling scheme, with a prohibition of fraudulent spam. Colorado's Junk E-mail Law is an example.[203] Spam is defined as unsolicited and unrequested commercial e-mail sent to an address having no current or prior business relationship with the sender.[204] The statute specifies that spam must include the actual point of origin.[205] It also prohibits falsifying any transmission information or routing information as well as hijacking a domain name without consent.[206] Spam must also include "ADV:" as the first four characters in the subject line unless it is sent from an organization to its members or employees.[207] Colorado has no requirement of "ADV:ADLT" for sexually explicit e-mail.

Colorado also requires an opt-out mechanism "allowing recipients to easily and at no cost remove themselves from the sender's electronic mail address lists so they are not included in future mailings."[208] The law also makes it a violation to continue sending e-mail to an address after the opt-out provision has been exercised.[209] Additionally, it prohibits giving those e-mail addresses to another spammer, however, the spammer is permitted to give the addresses to a do-not-e-mail list.[210]

A party entitled to damages may recover attorney's fees and costs as well as a civil penalty of ten dollars for each spam sent in violation.[211]

---

[199] *Id.*
[200] *Id.*
[201] *Id.*
[202] *Id.*
[203] COLO. REV. STAT. § 6-2.5-103 (2002).
[204] COLO. REV. STAT. § 6-2.5-102 (2002).
[205] COLO. REV. STAT. § 6-2.5-103 (2002).
[206] *Id.*
[207] *Id.*
[208] *Id.*
[209] *Id.*
[210] *Id.*
[211] COLO. REV. STAT. § 6-2.5-104 (2002).

ISPs have an exemption for sending or blocking spam that is in violation of the law.[212] There is no good faith requirement suggesting that an ISP may be liable for blocking compliant e-mail.

Kansas also combines fraudulent, opt-out and labeling instructions.[213] The law prohibits commercial e-mail that hijacks a third party's domain name, misrepresents any information identifying the point of origin or transmission path or contains a false or misleading subject line.[214] It requires that all commercial e-mail label itself as "ADV:" in the subject line, and "ADV:ADLT" if it is advertising sexually explicit or otherwise adult-oriented material.[215] It also calls for a reliable opt-out provision at no cost to the recipient.[216]

This law prohibits enabling software that allows senders to falsify or forge any part of a bulk e-mail.[217] ISPs have immunity for good faith blocking or re-transmitting e-mail in violation.[218] There is, however, an affirmative defense available one time only for violation of this law.[219] If the sender is able to demonstrate certain business practices by clear and convincing evidence, she may avoid liability.[220] Those seeking to use this defense must essentially prove they complied with the requirements of the statute. Specifically, they must show that they kept lists of those who exercised the opt-out provision; maintained reasonable practices and procedures to effectively prevent illegal spam; maintained records demonstrating compliance with the law; and that the unsolicited commercial e-mail was a result of error.[221]

Tennessee's law is similar to Kansas' and Colorado's, combining fraudulent, opt-out and labeling provisions.[222] Spam is defined as an unsolicited advertising e-mail conducting business.[223] It requires an opt-out provision of either a reliable toll-free telephone number or return e-mail address.[224] The opt-out must be honored upon notification.[225] Unsolicited advertising material must also include "ADV:" as the first four

---

[212] *Id.*
[213] KAN. STAT. ANN. § 50-6,107 (2002).
[214] *Id.*
[215] *Id.*
[216] *Id.*
[217] *Id.*
[218] *Id.*
[219] *Id.*
[220] *Id.*
[221] *Id.*
[222] TENN. CODE. ANN. § 47-18-2501 (2002).
[223] *Id.*
[224] *Id.*
[225] *Id.*

characters of the subject line. Also, spam advertising goods or services that "may only be viewed, purchased, rented, leased, or held in possession by an individual eighteen years of age or older," must include "ADV:ADLT" as the first eight characters.[226] The law prohibits selling, distributing or possessing software enabling a spammer to falsify transmission or routing information but it does not mention sending the same false transmissions.[227] Presumably, it is covered by possession of such software.

Jurisdiction applies when the spam is sent to a Tennessee resident through an ISP or computer equipment in the state.[228] Injured individuals and ISPs may recover actual damages or the lesser of ten dollars for each spam sent in violation or five thousand dollars per day.[229] They are also entitled to attorney's fees and costs.[230] ISPs have immunity for merely sending spam.[231] The law will become inoperative if federal spam legislation is passed.[232]

Minnesota defines spam as a commercial e-mail promoting goods or services.[233] It does not include situations where there is a prior business relationship or the recipient has consented or requested e-mail from the sender.[234] Also exempt are organizations using e-mail to "communicate exclusively" with its members or employees.[235] The law prohibits sending spam that hijacks a domain name, misrepresents the point of origin or contains a false or misleading subject line.[236] Commercial e-mail must also include "ADV" as the first characters in the subject line.[237] Messages containing "material of a sexual nature that may only be viewed by an individual 18 years of age and older," must include in the subject line "ADV-ADULT" as the first characters."[238]

As an opt-out provision, spammers must include either a toll-free telephone number, a valid sender-operated return e-mail address or some other easy to use electronic method.[239] ISPs are not liable for

---

[226] *Id.*
[227] *Id.*
[228] *Id.*
[229] *Id.*
[230] *Id.*
[231] *Id.*
[232] MINN. STAT. § 325F.694 (2002).
[233] *Id.*
[234] *Id.*
[235] *Id.*
[236] *Id.*
[237] *Id.*
[238] *Id.*
[239] *Id.*

merely transmitting spam and for blocking spam so long as the good faith requirement is met.[240] The law has a defense against liability for people whose domain names are hijacked.[241] Individuals and ISPs may recover damages up to thirty-five thousand dollars as well as reasonable attorney's fees.[242] Class action suits are prohibited, and federal law supersedes state law.[243]

Utah's law is called the "Unsolicited Commercial and Sexually Explicit E-mail Act."[244] It requires spammers sending unsolicited commercial e-mail or unsolicited sexually explicit e-mail comply with certain provisions.[245] Spammers must conspicuously state the sender's legal name, correct street address and valid Internet domain name.[246] The subject line must include as the first characters "ADV:" for commercial e-mail and "ADV:ADULT" for sexually explicit e-mail.[247] ISPs have immunity for the mere act of transmitting e-mail that violates these provisions.[248]

The opt-out provision must be a mechanism with no cost to the recipient in the form of a valid, functioning return e-mail address.[249] If the spam sent is sexually explicit and the sender has a toll-free number, she must include it in addition to the valid return e-mail address.[250] In both commercial and sexual-commercial e-mail, there must be a conspicuous notice that a convenient, no cost opt-out provision exists.[251] Spammers must honor an opt-out request and may not continue to send e-mail through either a subsidiary or affiliate.[252] The law also prohibits hijacking a third party's domain name or misrepresenting or failing to include any information in identifying the point of origin or transmission path of the e-mail.[253]

Violations of sexually explicit spam provisions are a criminal and civil offense while civil liability is the penalty for violations of commercial spam restrictions.[254] Victims may recover costs and attorney's fees in

---

[240] *Id.*
[241] *Id.*
[242] *Id.*
[243] UTAH CODE ANN. § 13-36-101 (2003).
[244] *Id.*
[245] *Id.*
[246] *Id.*
[247] *Id.*
[248] *Id.*
[249] *Id.*
[250] *Id.*
[251] *Id.*
[252] *Id.*
[253] *Id.*
[254] *Id.*

addition to actual damages or the lesser of ten dollars per e-mail received or twenty-five thousand dollars per day that the violation occurs.[255]

States that do not have active spam laws may still offer a cause of action for individuals under state consumer protection laws. For example, states such as Alaska which have no spam law per se, still may regulate spam through their deceptive business practices laws. In Alaska, it is unlawful to make a "false statement in advertisement or communication addressed to ... a substantial number of persons."[256]

III. TOO MUCH SPAM TO SLICE WITH ONLY ONE KNIFE

No one solution will solve the problems posed by the different and distinct types of spam. Technical remedies are either over or under inclusive by blocking all e-mail believed to be unsolicited or sent in bulk. It does not allow for some commercial e-mail that may be of interest to a recipient. The present legal remedies and attempts at industry self-regulation are not completely effective unless all spammers comply. As long as spammers are easily concealed and without any real incentive or threat to comply, they will continue to flout laws and industry standards.

A. Technical Solutions

Technical remedies, while effective in reducing overall amounts of spam,[257] do not alone provide a complete solution, because they treat all spam as if it were the same.[258] Anti-spam software blocks all bulk mail regardless of content, making it increasingly possible that expected e-mail will miss its destination.[259] Spam blocking services like SpamCop Blocking List (BL) have been accused of such inaccuracy by blocking thousands of legitimate e-mail messages.[260] In addition, the software cannot stop spam at its source but merely deflects it from reaching its destination so ISPs systems are still taxed by the flow of the e-mail.[261]

---

[255] ALASKA STAT. § 11.46.710 (Michie 2002).
[256] *Id.*
[257] For a discussion of various consumer available technical remedies that can be bought separate from those offered by Internet service providers, *see generally* J.D. Biersdorfer, *D.I.Y. Tools That Leave Spam D.O.A.*, N.Y. TIMES, Jan. 30, 2003, at G1.
[258] Oren Etzioni, *Fighting the Menace of Unwanted E-mail*, N.Y. TIMES, Sept. 14, 2002, at A15.
[259] J.D. Biersdorfer, *D.I.Y. Tools That Leave Spam D.O.A.*, N.Y. TIMES, Jan. 30, 2003, at G1.
[260] A detailed discussion about the complaints made against SpamCop BL is *available at* http://jhoward.fastmail.fm/spamcop.html (last visited Mar. 3, 2003).
[261] Matt Richtel, *In Spam Fight, the Opposite of a Filter*, N.Y. TIMES, Dec. 9, 2002, at C8.

Even though filtering software is constantly improving, spammers are elusive and quickly anticipate and adapt to software advances to avoid having their spam filtered out.[262]

There is also the problem of technology taking matters too far. Businesses and individuals sending out legitimate bulk e-mail may find themselves put on a "black hole list" unable to send any e-mail.[263] The lists are usually generated by anti-spam advocates who make their own determinations about what e-mail should and should not be sent.[264] ISPs get these lists from various organizations and then bounce any e-mail sent to their subscribers.[265] Those overseeing the lists usually operate in a block-now-and-ask-questions-later approach.[266] Individuals and businesses put on a black hole list could suffer considerable harm.[267] The lists are not mentioned in any of the state laws, so these organizations essentially act with no redress whatsoever.

B. Industry Self-Regulation

Like technological solutions, industry self-regulation has only limited success of effectively cutting down on the amounts of spam sent. As a practice, industry self-regulation would work if all companies sending bulk e-mail were concerned about consumer confidence in name recognition.[268] For example, the Direct Marketing Association (DMA), a trade association that represents users and suppliers in the direct, database, and interactive marketing field, must abide by the DMA's Privacy Promise and members are prohibited from sending unsolicited commercial e-mail messages to addresses that appear in the DMA's e-mail Preference Service database.[269] Rather, spammers who do not wish to be identified have no interest in complying and flout any generally

---

[262] *Id.*

[263] *Available at* http://www.allwebarticles.com/articles/1blacklists.html (last visited Mar. 3, 2003).

[264] Bret A. Fausett, *Blind Vigilantes – Blackhole Lists Offer Dark Prospects*, New Architect, Aug. 1, 2002.

[265] *Available at* http://www.allwebarticles.com/articles/1blacklists.html (last visited Mar. 3, 2003).

[266] *Available at* http://www.politechbot.com/p-03730.html (last visited Mar. 3, 2003).

[267] Companies put on "black hole lists" have trouble sending e-mail that may be essential to conduct business. IBill was wrongfully reported to the Mail Abuse Prevention System (MAPS) which put the company on their black hole list. As a result of the four day blacklisting, IBill lost $400,000 in revenue. Sharon Gaudin, *The Spam Police; Tactics Used By Self-Appointed Spam Fighters Come Under Fire*, NETWORK WORLD, Sept. 10, 2001, at 58.

[268] *See* Lee *supra* note 1, at G1.

[269] The DMA's policy on spam is *available at* http://www.the-dma.org/ (last visited Mar. 3, 2003).

accepted techniques to ensure their spam gets into e-mail accounts.[270] These spammers spoil the attempts made by businesses to build confidence in e-mail solicitation and make industry self-regulation on its own an unworkable solution.[271] As a result, these informal responses have generally had little effect on spam.[272]

C. The Problem of Inconsistent State Laws and the Current Federal Standard

1. Effect of Federal Law

Although the CAN-SPAM Act now is law, it does not preempt all state laws. Indeed, has "savings clauses" for specified types of state provisions and enforcement proceedings. It thus narrows but does not abolish the possibility of conflicts between state regimes.

Some of these issues were anticipated by pre-Act decisions under the Dormant Commerce Clause.

2. Inconsistent State Laws

Spam laws in both California and Washington have been challenged under the Dormant Commerce Clause.[273] The Commerce Clause of the Constitution provides that "Congress ...has the power to regulate commerce... among the several states..."[274] Implicit in this affirmative grant is the negative or Dormant Commerce Clause. This is the principle that states impermissibly intrude on the federal power when they enact laws that unduly burden interstate commerce.[275] Defendants in both challenges argued that the anti-spam statutes create inconsistent obligations and impose burdens on interstate commerce that outweigh the local benefits.[276] The California Court of Appeals held that the burdens imposed on interstate commerce "are minimal and do not

---

[270] *Did You Get the Check I Sent?*, N.Y. TIMES, Aug. 6, 2002, at A14. This article also gives common examples of misleading subject lines contained in fraudulent spam.

[271] Sorkin, *supra* note 14, at 325.

[272] Sorkin, *supra* note 14, at 325.

[273] Ferguson v. Friendfinders, Inc., 94 Cal. App. 4th 1255 (2002); Washington v. Heckel, 24 P.3d 404 (Wash. 2001).

[274] U.S. CONST., Art. I, § 8.

[275] For a more detailed discussion of the dormant commerce clause *see generally*, Jack L. Goldsmith, *The Internet and the Dormant Commerce Clause*, 110 YALE L.J. 785 (2001).

[276] Ferguson v. Friendfinders, Inc., 94 Cal. App. 4th 1255 (2002); Washington v. Heckel, 24 P.3d 404 (2001).

outweigh the local benefits."[277] Likewise, the Washington State Supreme Court held that the local benefits outweigh the burdens on sending commercial e-mail.[278]

The issue, however, is not resolved by these cases. With more states enacting inconsistent laws, a court could find that numerous states regulating spam makes compliance with all affirmative requirements very burdensome or even impossible.[279] For instance, it may be true that no state would ever pass a law directly inconsistent with other states for example a law requiring spammers to use misleading subject lines or hijack domain names. However, it is difficult to know if e-mail addresses reside in states with affirmative duties placed on sending unsolicited e-mail. Also, a sender of pornography can not comply with California's requirement of "ADV:ADLT" and Wisconsin's requirement of "Adult Advertisement" in the subject line.

States differ in the penalties they impose. Some make sending spam a criminal offense. Others create a civil cause of action to enjoin senders or award damages to victims. Those awarding damages may also have different definitions of what constitutes a harm to an individual or ISP. States also vary in the amount of damages to be awarded. Finally, because state approaches vary between labeling, opt-out and anti-fraudulent requirements, it is unclear if a sender of unsolicited commercial e-mail must comply with every state to avoid sanction.

3. Fraudulent Spam Laws, Opt-Out and Labeling

State laws prohibiting fraudulent spam are effective in providing a remedy for false or misleading e-mail. On the other hand, the reality is that spammers who engage in the practice of falsifying information in the header, usually do so to avoid revealing their true identity. With the global reach of the Internet, these spammers are difficult, if not impossible to find. While opt-out provisions allow consumers to respond to spam positively or decline future solicitations, spammers have little incentive to honor these requests and, in fact, these provisions may spur more unwanted mail.[280] Unfortunately, there is a growing concern among consumers that an opt-out instruction serves only to tell a spammer that the e-mail has reached a valid e-mail address and will only increase the volume of e-mail sent.[281] While the FTC claims that this fear is unfounded, it contributes to a general lack of confidence in e-mail as a

[277] *Friendfinders*, 94 Cal. App. 4th 1255.
[278] *Heckel*, 24 P.3d 404 (2001).
[279] Michelle Armond, *Cyberlaw: State Internet Regulation and the Dormant Commerce Clause*, 17 BERKELEY TECH. L.J. 379, 399 (2002).
[280] Sorkin, *supra* note 14, at 352.
[281] Lee, *supra* note 1, at G5.

legitimate type of marketing.[282]

There have been attempts to create a universal "global remove" list similar to the national "do not call" list curtailing telemarketing calls. However, despite the questionable constitutionality of the "do not call" list, a similar solution for spam is an unrealistic solution.[283] People frequently change e-mail accounts, making the accuracy of such a list questionable. Also, there is the same problem that elusive spammers, content operating outside industry norms, would not be compelled to abide by it.[284]

Labeling requirements face similar benefits and challenges as opt-out provisions. Recipients know by the "ADV" or "ADV:ADULT" warnings that the e-mail contains a solicitation and gives them an opportunity to delete it without reading. However, unlike an opt-out provision, these laws do nothing to stop the flow of spam, so burdens still exist to ISP bandwidth and consumer account storage space. Labeling requirements are also impractical unless the practice is followed consistently. Again, the spammers who are content operating outside the law go unaffected and unchecked as a result of these laws. Different states impose inconsistent duties for labeling unsolicited commercial e-mail and only a few states require it at all.

There is an additional problem for state laws giving discretion to ISPs to define spam in their own policy provisions, as well as granting them immunity from sending spam or blocking legitimate mail because it appears to be spam by their own definition. This delegation of authority from state legislatures to ISPs allows them to formulate incompatible or improbable policies that would subject violators to legal liability.[285] Moreover, they would be of questionable validity under new federal law.

4. The Current Federal Scheme

When the Can-Spam Act was passed, it superceded state spam laws, thereby eliminating concern over inconsistent state laws.[286] By taking the model of best state practices, Congress passed legislation that

---

[282] In a telephone conversation with Brian Heuseman at the Federal Trade Commission, he explained that the FTC conducted a study of opt-out provisions for several e-mail accounts set up specifically to test the reliability of these provisions. Opting-out of spam sent to the accounts had no affect on the amount of spam received.

[283] Sorkin, *supra* note 14, at 353.

[284] Sorkin, *supra* note 14, at 352.

[285] Derek D. Simmons, *No Seconds on Spam: A Legislative Prescription to Harness Unsolicited Commercial E-Mail*, 3 J. SMALL & EMERGING BUS. L. 389 (1999).

[286] 117 Stat. 2688 § 8(b) (2003).

deals with both fraudulent as well as annoying spam.[287] However, it does not put an end to the problems spam causes.[288] One of the fundamental flaws of the Act is the limitation on who has the ability to enforce the new law. While the Federal Trade Commission has the primary responsibility for enforcing the Act, state attorneys general and ISPs also have standing to seek remedies for spammers who violate the federal law.[289] Private individuals have no standing to pursue claims based on violations.

Another criticism of the federal law is that it lacks the teeth of some of the more stringent state laws.[290] California and Virginia both had rather aggressive anti-spam laws in place.[291] The federal law does not criminalize spamming; it only affords a civil penalty.[292]

IV. A RECIPE FOR MODEL LEGISLATION AND CONSUMER REDRESS

Spam that is fraudulent or deceptive should be dealt with by legal remedy; the often undesirable, but not illegal, commercial speech should be subject to industry self-regulation. Conflation of the various types relies too much on legislation to make choices for consumers and takes control over what commercial e-mail consumers will receive. A more comprehensive federal law that gives individuals the power to enforce is important. Consumer and ISP activism makes the best possible remedy for dealing with spam.

The federal law should keep its current fraudulent and opt-out approaches by banning false or misleading headers, routing information and transmission paths. It should also prohibit using false or hijacked third-party domain names, as well as enabling-software to facilitate any of the above offenses. Also, unsolicited e-mail should contain a reliable opt-out provision in the form of a no cost way consumers may contact the senders to exercise the terms. Spammers should be bound to honor all requests within a reasonable amount of time of receipt.

Focusing on the fraudulent and deceptive aspects of spam draws

---

[287] *Id.* at § 4.
[288] *See* Doug Bedell, *Study Finds Law Fails to Cut Spam; Volume of Unwanted E-mails Has Actually Increased,* DALLAS MORNING NEWS, Mar. 18, 2004, at 1D; Carrie Kirby, *Spam Keeps Coming Despite the New Law*, THE SAN FRANCISCO CHRONICLE, Jan. 19, 2004, at E1.
[289] 117 Stat. 2699 § 7 (2003).
[290] Samuel Lewis, *Law Didn't Stop Deluge*, NATIONAL LAW JOURNAL, Mar. 22, 2004, at 23.
[291] CAL. BUS. & PROF. CODE § 17538.4 (Deering 2002) (repealed 2003); VA. CODE ANN. § 18.2-152.1 (2002).
[292] 117 Stat. 2699 § 7 (2003).

a firm line between the illegal and the merely offensive. It also successfully avoids First Amendment challenges because, while there is an argument for free speech relating to e-mail solicitation, the same protections do not apply to fraudulent speech.

Also, it is important that some immunity is afforded to ISPs for sending or blocking spam, but there should also be a cause of action created against the "black hole lists" that cause harm by blocking legitimate e-mail. Because this legal remedy, however, only solves one part of the problem, an incentive must be created for finding and controlling spammers using many of these techniques. This is where consumers and ISPs can help themselves by helping to enforce the laws and stop spammers from operating outside the law. Several consumer organizations like TRAC and CAUCE have made it easier to report unlawful spamming to the Federal Trade Commission.[293] They have designed websites with questionnaires that consumers may fill out and have their complaints sent directly to the Federal Trade Commission.

This legislative prescription solves many problems associated with fraudulent e-mail but has no effect on annoying e-mail. This leaves the issue of the often undesirable but not illegal commercial speech. This type of e-mail is best addressed by industry self-regulation.

V. CONCLUSION

For both types of spam, fraudulent and annoying, a combination of legislation, technology and industry self-regulation will make e-mail a more legitimate and reliable form of marketing. A more comprehensive federal legislation and an awareness and advocacy on the part of consumers and ISPs will help to effectuate this. Specifically, those who want to lose weight or secure a low interest home loan will be able to receive e-mail of interest, while those who do not will be able to cut down on the number of unwanted solicitations they receive.

---

[293] The Telecommunications Research and Action Center (TRAC) launched an initiative to ban spam and have a link on their website to complain to the FTC about fraudulent spamming activity. *Available at* http://trac.policy.net/banspam/. Likewise, the Coalition Against Unsolicited Commercial E-mail (CAUCE) offers consumers ways to cut down on spam received in their e-mail boxes. *Available at* http://www.cauce.org/pressreleases/math.shtm. Consumers can also use a variety of techniques on their own, including keeping their e-mail addresses from public view, using complex addresses that spammers will not easily guess, utilizing blocking techniques offered by ISPs, and forwarding spam to the FTC. For a more detailed list of individual precautions, *see* Jennifer 8. Lee, *From Filtering to Forwarding: Ways to Fight Junk E-mail*, N.Y. TIMES, June 27, 2002, at G5.