35 U.S.F. L. REV. 325 (2001)

Technical and Legal Approaches to Unsolicited Electronic Mail[†]

By DAVID E. SORKIN[*]

> “Spamming” is truly the scourge of the Information Age. This problem has become so widespread that it has begun to burden our information infrastructure. Entire new networks have had to be constructed to deal with it, when resources would be far better spent on educational or commercial needs.
>
> *United States Senator Conrad Burns (R-MT)*[1]

UNSOLICITED ELECTRONIC MAIL, also called “spam,”[2] causes or contributes to a wide variety of problems for network administrators,

[†] Copyright © 2000 David E. Sorkin.

[*] Assistant Professor of Law, Center for Information Technology and Privacy Law, The John Marshall Law School; Visiting Scholar (1999–2000), Center for Education and Research in Information Assurance and Security (CERIAS), Purdue University. The author is grateful for research support furnished by The John Marshall Law School and by sponsors of the Center for Education and Research in Information Assurance and Security. Paul Hoffman, Director of the Internet Mail Consortium, provided helpful comments on technical matters based upon an early draft of this Article. Additional information related to the subject of this Article is available at the author’s web site *Spam Laws*, *at* http://www.spamlaws.com/.

[1] *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 [hereinafter *1998 Senate Hearing*].

[2] The term “spam” reportedly came to be used in connection with online activities following a mid-1980s episode in which a participant in a MUSH created and used a macro that repeatedly typed the word “SPAM,” interfering with others’ ability to participate. *See* J.D. Falk, *The Net Abuse FAQ Revision 3.2, § 2.4, at* http://www.cybernothing.org/faqs/net-abuse-faq.html#2.4 (Dec. 23, 1998). A MUSH, or multi-user shared hallucination, is a type of MUD—a multi-user dimension or dungeon. *See* Denis Howe ed., *Free On-Line Dictionary of Computing, at* http://foldoc.doc.ic.ac.uk/foldoc/foldoc.cgi?Multi-User+Shared+Hallucination (last visited Nov. 16, 2000) (defining “MUSH”) & *at* http://foldoc.doc.ic.ac.uk/foldoc/foldoc.cgi?MUD (last modified Apr. 16, 1995) (defining “MUD”). The perpetrator presumably chose the word “spam” as an allusion to a Monty Python skit that depicted a restaurant in which every meal contained Spam, a meat product that many people apparently consider unpalatable. *See* Falk, *supra*. Other reports omit the MUSH episode entirely, linking current usage of the word “spam” directly to the Monty Python routine or even to the meat product itself. *See, e.g.*, CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1018 n.1 (S.D. Ohio 1997); David T. Bartels, Note, *Canning Spam: California Bans Unsolicited Commercial E-Mail*, 30 MCGEORGE L. REV. 420, 420 n.1 (1999); Steven E. Bennett, Note, *Canning Spam:* CompuServe, Inc. v. Cyber Promotions, Inc., 32 U. RICH. L. REV. 545,

businesses and other organizations, and individual users of the Internet.[3] Spam has traditionally been viewed mainly as a nuisance, but it also constitutes a security threat.[4]

Three general categories of approaches have been used to address the spam problem: informal measures, such as social norms and self-regulatory efforts;[5] technical measures undertaken by individuals and organizations;[6] and legal responses,[7] including both litigation under existing statutes and traditional common-law theories and new

549 n.30 (1998); Anne E. Hawley, Comment, *Taking Spam Out of Your Cyberspace Diet: Common Law Applied to Bulk Unsolicited Advertising via Electronic Mail*, 66 UMKC L. REV. 381, 381 n.3 (1997); Joshua A. Marcus, Note, *Commercial Speech on the Internet: Spam and the First Amendment*, 16 CARDOZO ARTS & ENT. L.J. 245, 247 n.14 (1998); Gary S. Moorefield, Note, *SPAM—It's Not Just for Breakfast Anymore: Federal Legislation and the Fight to Free the Internet From Unsolicited Commercial E-Mail*, 5 B.U. J. SCI. & TECH. L. 10, ¶ 1 n.1 (1999), *at* http://www.bu.edu/law/scitech/volume5/5bujstl10.pdf; Hormel Foods Corp., *SPAM and the Internet*, *at* http://www.spam.com/ci/ci_in.htm (last visited Aug. 8, 2000).

At first, the term "spam" was used to refer to articles posted to Usenet newsgroups or other discussion forums in violation of certain forum policies or other rules or customs. *See* Denis Howe ed., *Free On-Line Dictionary of Computing*, *at* http://foldoc.doc.ic.ac.uk/foldoc /foldoc.cgi?query=spam (last modified Apr. 8, 1997) (defining "spam"). Later, the term came to be used for various types of unwanted e-mail messages, usually advertisements sent out in large quantities. *See id.*; *see also generally* ALAN SCHWARTZ & SIMSON GARFINKEL, STOPPING SPAM 17–35 (1998) (telling the history of spam). The latter sense—more precisely, "e-mail spam"—has eclipsed the former, and is the sense in which the term is used in this Article.

"Spam" has also been used to describe other online phenomena, such as the gratuitous repetition of words in a web page and similar activities designed to increase the likelihood that the page will be retrieved by search engines. *See, e.g.*, David J. Loundy, *E-LAW 4: Computer Information Systems Law and System Operator Liability*, 21 SEATTLE U. L. REV. 1075, 1183 n.702 (1998); Ira S. Nathenson, *Internet Infoglut and Invisible Ink: Spamdexing Search Engines with Meta Tags*, 12 HARV. J.L. & TECH. 43, 45–46 (1998); Steve Silberman, *Net Mom Battles "Spamdexing" by Sex Site*, WIRED NEWS, Feb. 11, 1997, *at* http://www.wired.com/news/ culture/0,1284,1978,00.html.

The term "spam" has become so well-known that it is now being used to describe unwanted telephone calls and faxes. *See, e.g.*, Bradley Foss, *"Blasts" Filling Voice Mail: A Nuisance, or an Efficient Way to Communicate?*, CHI. TRIB., Oct. 11, 1999, 1999 WL 2920496 (describing automated voicemail blasts as "phone spam"); Drew Cullen, *LA Citizens Tackle NFL in Mass Fax Spam*, REG. (London), Aug. 25, 1999, http://www.theregister.co.uk/content/archive/6369.html.

[3] *See* discussion *infra* Part I.B.

[4] *See* CERT Coordination Ctr., *Email Bombing and Spamming*, *at* http://www.cert.org/tech_tips/email_bombing_spamming.html (last modified Apr. 26, 1999) (discussing ways to react and respond to spam); Computer Incident Advisory Capability, U.S. Dep't of Energy, *E-Mail Spamming Countermeasures*, *at* http://ciac.llnl.gov/ciac/bulletins/i-005c.html (Nov. 25, 1997) (same); *see also* discussion *infra* Part I.B.3 (discussing spam's threat to security).

[5] *See* discussion *infra* Part II.

[6] *See* discussion *infra* Part III.

[7] *See* discussion *infra* Part IV.

legislation that specifically targets spam.[8] The current trend appears to involve a diminished reliance on self-regulation and other informal measures in favor of increased emphasis on more formal responses, both technical and legal. This Article discusses the variety of mechanisms that have been used in the war on spam.

I. Background

To many people, spam means little more than "unwanted e-mail," it is perhaps tautological to say that nearly everyone agrees that spam is undesirable. The controversies surrounding spam, therefore, tend to relate less to its legitimacy than to how it should be defined, how important a problem it is, and what, if anything, ought to be done about it.[9]

A. Defining Spam

The difficulties in addressing the problem of spam begin at the definitional stage: Internet users and providers differ widely in how they define spam and other forms of objectionable e-mail. Some people consider all advertisements or even all unwanted messages to be spam,[10] while others try to define it in terms of existing acceptable use

[8] These categories can be loosely compared to the four types of constraints on behavior outlined by Lawrence Lessig: law, norms, markets, and architecture (or "code"). *See* LAWRENCE LESSIG, CODE, AND OTHER LAWS OF CYBERSPACE 89 (1999); Lawrence Lessig, Comment, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501, 508–09 (1999) [hereinafter Lessig, *Law of the Horse*].

[9] Though it may seem unnecessarily loaded, the term "legitimate" is commonly used to describe e-mail that is not spam. *See, e.g.*, Am. Online, Inc. v. Prime Data Sys. Inc., No. 97-1652-A, 1998 U.S. Dist. LEXIS 20226, at *13 n.13 (E.D. Va. Nov. 20, 1998) (noting that "there is no legitimate market for unsolicited bulk e-mail"); Lorrie Faith Cranor & Brian A. LaMacchia, *Spam!*, COMM. ACM, Aug. 1998, at 74, 78 (distinguishing spam from "legitimate messages"), *available at* http://www.research.att.com/~lorrie/pubs/spam/spam.html.

[10] For example, in March 2000, the mayor of Denver and other government officials received thousands of e-mail messages alleging racial bias in criminal charges that had been filed against a Kuwaiti man, after the man's relatives posted a web site encouraging people to send such messages. *See* Kevin Flynn, *Defendant's Family Urges Spam E-mail Officials See Blizzard of Messages Regarding Kuwaiti Facing Charges of Attempted Murder*, ROCKY MOUNTAIN NEWS (Denver), Mar. 25, 2000, 2000 WL 6591185. Both the mayor's spokesperson and a newspaper article describing the incident referred to the messages as "spam." *See id.* The term "spam" has also been used to describe virus warnings, urban legends, jokes, chain letters, and similar messages forwarded by relatives and other acquaintances. *See, e.g.*, Phaedra Hise, *Mom Spam: The Cyber-Scourge of Families Everywhere*, SALON, Dec. 20, 1999, *at* http://www.salon.com/mwt/feature/1999/12/20/spam/.

Perhaps more akin to the type of spam discussed in this Article is the use of "viral" marketing techniques in which merchants recruit individuals to forward solicitations to their acquaintances on the merchant's behalf. *See* Ed Foster, *Viral Marketing Goes One Step* policies or network etiquette (or "netiquette") rules. The two most common definitions of spam are unsolicited commercial e-mail ("UCE") and unsolicited bulk e-mail ("UBE").[11]

1. Unsolicited

The key aspect of nearly all definitions of spam is that the e-mail messages must be "unsolicited." In general, a communication is considered to be unsolicited if there is no prior relationship between the parties, and the recipient has not explicitly consented to receive the communication.[12] It can also mean that the recipient has previously

Too Far—to a Place Where Friends Spam Friends, INFOWORLD, Feb. 7, 2000, http://www.infoworld.com/articles/op/xml/00/02/07/000207opfoster.xml.

[11] In a 1999 survey of over 13,000 Internet users, the majority of respondents considered both UCE and UBE to be spam. *See* Gartner Group, *ISPs and Spam: The Impact of Spam on Customer Retention and Acquisition*, at 6, *at* http://www.brightmail.com/global/pdf/gartner.pdf (June 14, 1999). A smaller number of respondents also said they viewed chain letters, duplicate postings, and pop-up ads as spam. *See id.*

UCE and UBE are not mutually exclusive, of course, and a third alternative is to define spam as unsolicited bulk commercial e-mail ("UBCE"), although this may be functionally equivalent to UCE. *See* discussion *infra* Part I.A.4. Delaware's statute—probably the most restrictive anti-spam statute enacted to date—prohibits UBCE outright, but includes an exception for messages that are "sent between human beings," whatever that means. *See* Act of July 2, 1999, ch. 135, § 1, 72 Del. Laws 7, 7 (1999) (to be codified at DEL. CODE tit. 11, § 937(a)).

[12] *See, e.g.*, CAL. BUS. & PROF. CODE §§ 17538.4(e), 16538.45(a)(2) (Deering Supp. 2000); Illinois Electronic Mail Act, 815 ILL. COMP. STAT. ANN. 511/5 (West Supp. 2000); NEV. REV. STAT. ANN. § 41.730(1) (Michie Supp. 1999); N.C. GEN. STAT. § 14-453(10) (1999); R.I. GEN. LAWS § 6-47-2(e) (Supp. 1999); Colorado Junk Email Law, ch. 388, § 1, 2000 Colo. Sess. Laws 2031, 2032 (to be codified at COLO. REV. STAT. § 6-2.5-102(5)). A bill introduced in the House of Representatives last year would have limited the "pre-existing business relationship" to the preceding five-year period for purposes of determining whether a message is unsolicited. *See* Unsolicited Commercial Electronic Mail Act of 2000, H.R. 3113, 106th Cong. § 3(10)(A)(i). This bill has been reintroduced in the 107th Congress. *See* Unsolicited Electronic Mail Act of 2001, H.R. 95, 107th Cong.

Some jurisdictions omit "unsolicited" altogether. Washington and Oklahoma's restrictions on falsified routing information apply to solicited as well as unsolicited e-mail messages. *See* WASH. REV. CODE ANN. § 19.190.010(2) (West Supp. 2001); Act of June 8, 1999, ch. 337, § 1, 1999 Okla. Sess. Laws 1515, 1515 (to be codified at OKLA. STAT. tit. 15, § 776.1(A)).

Interestingly, none of the definitions of "unsolicited" even consider whether or how narrowly the message is targeted. Thus, for example, a publisher's message promoting a new textbook qualifies as unsolicited whether it is sent to ten million random e-mail addresses, to 100,000 people whose addresses include ".edu," or to 100 professors who teach courses in the field covered by the book, absent a prior relationship between the publisher and the recipients of the message. "Opt-in" e-mail marketing firms generally promise to target solicitations in exchange for obtaining recipients' permission to send advertising messages. *See, e.g.*, ChooseYourMail, *About Us*, *at* http://www.chooseyourmail.com/AboutUs.cfm (last visited Aug. 8, 2000); PostMasterDirect.com, *Welcome to PostMasterDirect.com, the Leader in 100% Opt-In® Email Marketing!*, *at* http://www.postmasterdirect.

sought to terminate the relationship, usually by instructing the other party not to send any more communications in the future.[13]

From a legal perspective, the term "unsolicited" is nothing new; it has the same meaning in the context of restrictions on telephone solicitations and other forms of direct marketing.[14] From a technical perspective, however, it may be much more difficult to assess whether an e-mail communication is unsolicited, particularly if the prior relationship is comprised of something other than a previous exchange of e-mail messages.

2. Commercial

Some definitions of spam include only messages that are commercial in nature. "Commercial" is generally defined in terms of message content rather than the sender's actual or presumed motivation for sending the message; a typical definition includes any message that

com/ (last visited Aug. 8, 2000); YesMail.com, T*he YesMail Network*, *at* http://www.yesmail.com//network.asp?sec=mkt (last visited Nov. 21, 2000). It is the permission, not the targeting, that prevents such messages from being considered unsolicited.

[13] Such a request is commonly referred to as an "opt-out" request. Communication with a person who has previously opted out is frequently omitted from statutory definitions of "unsolicited," but statutes that omit such communications from the definition typically include a separate provision restricting post-opt-out communications. *See, e.g.*, CAL. BUS. & PROF. CODE § 17538.4(c) (Deering Supp. 2000); IOWA CODE ANN. § 714E.1(2)(e) (West Supp. 2000); R.I. GEN. LAWS § 6-47-2(c) (Supp. 1999); TENN. CODE ANN. § 47-18-2501(c) (Supp. 1999); Colorado Junk Email Law, ch. 388, § 1, 2000 Colo. Sess. Laws 2031, 2033 (to be codified at COLO. REV. STAT. § 6-2.5-103(5)); Act of July 2, 1999, ch. 135, § 1, 72 Del. Laws 7, 8 (1999) (to be codified at DEL. CODE tit. 11, § 938(a)); Act of Apr. 17, 2000, ch. 423, § 1, 2000 Idaho Sess. Laws 1373, 1374 (to be codified at IDAHO CODE § 48-603E(3)(d)).

A broad interpretation of "unsolicited" might include all contacts that are not part of a current transaction. For example, suppose that a person purchases a bottle of aspirin at a supermarket using a credit card, and the store somehow is able to obtain the person's e-mail address. If the store subsequently sends the person an e-mail message advertising a sale on acetaminophen, this communication could be considered unsolicited under such a definition. Such a scenario is more likely to occur if the purchaser presents a membership card for the store's discount or "loyalty" program during the transaction, enabling the store to link the transaction to personal information about the purchaser already in its files. However, in this modified version of the scenario, the purchaser may have previously consented to receive subsequent unrelated communications from the store, so the communication probably would not be considered unsolicited.

[14] *See, e.g.*, Telephone Consumer Protection Act of 1991, 47 U.S.C. § 227(a)(4) (1994) (defining "unsolicited advertisement" as advertising material transmitted without the recipient's prior express consent); *id.* § 227(a)(3)(B) (exempting calls made to persons with whom the caller has an established business relationship); 47 C.F.R. § 64.1200(e)(2)(iii), (vi) (1999) (requiring telemarketers to record and honor "do-not-call" requests).

promotes the sale of goods or services.[15] Ideally, indirect as well as direct commercial content ought to qualify—for example, an e-mail message containing a review of a free web site that contains advertisements should be considered commercial if it is sent on behalf of the web site's operator. In any event, with an appropriate legal definition, it will normally be relatively easy to determine whether a message is commercial. In close cases, the question will be one of fact.[16] However, the content-sensitive nature of the distinction may make it much more difficult to implement such a distinction using an automated technical process.

3. Bulk

The real problem with spam lies in the volume of e-mail messages, not their content. For that reason, spam is sometimes defined as messages sent in large quantities—i.e., "bulk" e-mail.[17] A single message sent to a very large number of recipients clearly qualifies as bulk.[18] By the same token, separate but identical copies of a mes-

[15] *See, e.g.*, CAL. BUS. & PROF. CODE § 17538.45(a)(1) (Deering Supp. 2000); Illinois Electronic Mail Act, 815 ILL. COMP. STAT. ANN. 511/5 (West Supp. 2000); IOWA CODE ANN. § 714E.1(1)(a) (West Supp. 2000); LA. REV. STAT. ANN. § 14:73.1(13) (West Supp. 2000); NEV. REV. STAT. ANN. § 41.710 (Michie Supp. 1999); N.C. GEN. STAT. § 14-453(1b) (1999); R.I. GEN. LAWS § 6-47-2(e) (Supp. 1999); TENN. CODE ANN. § 47-18-2501(a) (Supp. 1999); WASH. REV. CODE ANN. § 19.190.010(2) (West Supp. 2001); Colorado Junk Email Law, ch. 388, § 1, 2000 Colo. Sess. Laws 2031, 2032 (to be codified at COLO. REV. STAT. § 6-2.5-102(5)); Act of July 2, 1999, ch. 135, § 3, 72 Del. Laws 7, 9 (1999) (to be codified at DEL. CODE tit. 11, § 931(17)); Act of June 27, 2000, ch. 763, § A, 2000 Mo. Laws 735, 747–48 (to be codified at MO. REV. STAT. § 407.1300(2)); *cf.* Telephone Consumer Protection Act of 1991, 47 U.S.C. § 227(a)(4) (1994) (defining "unsolicited advertisement" in context of solicitations by telephone and facsimile machine).

[16] *See, e.g.*, Lutz Appellate Servs. v. Curry, 859 F. Supp. 180, 181 (E.D. Pa. 1994) (holding that "help wanted" ads are not "advertisements" under narrow definition in Telephone Consumer Protection Act).

[17] *See infra* note 23 (defining what constitutes "bulk").

[18] A single message sent to a large number of recipients commonly is sent with the recipients' addresses contained in one or more blind carbon copy ("BCC") header lines. *See* SCHWARTZ & GARFINKEL, *supra* note 2, at 53. The header of a standard e-mail message includes several lines identifying the intended recipients of the message. *See id.* The "TO" line identifies the primary addressee or addressees; the carbon copy line ("CC") designates secondary addressees; and the BCC line is used to list recipients whose names and e-mail addresses will not appear on the copies of the message delivered to the recipients. *See id.* at 49, 53; David H. Crocker, *Standard for the Format of ARPA Internet Text Messages (Request for Comments No. 822)*, at 23, *at* http://www.isi.edu/in-notes/rfc822.txt (Aug. 13, 1982). Particularly when a message is being sent to a large number of people, the BCC field is useful because it reduces the size of the message header—conserving bandwidth and improving readability of the message—while protecting the privacy of recipients. *See* Avi Mesher, *Third Party Software Support*, *at* http://www.palmtoppaper.com/ptphtml/51/51000020.htm (last visited Dec. 22, 2000). Spammers often use the BCC field to conceal the

sage that are sent to a large number of recipients are also considered to be sent in bulk. The only distinction between the two is the stage at which the message is copied, or "exploded."[19]

Substantially similar messages, as well as identical copies of a single message, probably also qualify as "bulk" under this rule. For example, a sender may make very minor changes to each copy of a message—perhaps by personalizing it in a manner similar to the computer-generated mailings that promote sweepstakes offers,[20] by placing a unique, and typically invalid, sender address on each copy, or by spreading them out over hours or days rather than sending them all simultaneously. Bulk messages that use one or more such variations may be somewhat more difficult to detect from a technical perspective, but that problem is certainly easier than the subjective evaluation of content required to distinguish between commercial and noncommercial messages.[21]

The main issue lies in how many copies of a message must be sent and within what time period for them to qualify as a bulk transmission. There is no generally agreed upon threshold; indeed, there is even some resistance in the anti-spam community to establishing or

fact that a message is being sent to many people simultaneously, although the lack of a TO or CC header containing the recipient's address can be used by filters to help determine whether an inbound message should be classified as spam. *See* Jim Hu, *Hotmail Adds Filters to Combat Unsolicited Email*, CNET NEWS.COM, Mar. 9, 2000, *at* http://news.cnet.com/category/0-1005-200-1568584.html.

Internet e-mail messages are transmitted using the Simple Mail Transfer Protocol ("SMTP"). *See* Jonathan B. Postel, *Simple Mail Transfer Protocol (Request for Comments No. 821*), at 1, *at* http://www.isi.edu/in-notes/rfc821.txt (Aug. 1982). The sender transmits the message using an SMTP server—usually, one maintained by the sender's own Internet service provider. *See id.* at 2. Unless the intended recipient is a local user of that server, the message is then forwarded to another SMTP server, which accepts it for delivery to the recipient. *See id.* at 3. When a message contains multiple addresses in the TO, CC, and BCC fields, the SMTP server through which the message is sent contacts the servers that receive messages on behalf of each of the addressees, and transmits one copy of the message to each such server. *See id.*

[19] A "mail exploder" is a server that takes an incoming message and forwards copies of the message to multiple recipients. *See* Denis Howe ed., *Free On-Line Dictionary of Computing*, *at* http://foldoc.doc.ic.ac.uk/foldoc/foldoc.cgi?mail+exploder (last visited Nov. 16, 2000) (defining "mail exploder"). One common application of mail exploders is the operation of Internet mailing lists. *See id.*

[20] Sending separate copies of a message to many recipients, whether identical or merely similar, may be more costly to the sender in terms of bandwidth and computing resources than sending a single copy to multiple recipients. It may also be more difficult for recipients and third parties to detect, but the end result is roughly the same.

[21] Collaborative filtering techniques, for example, can be used to compare messages sent to many different received in order to evaluate whether they should be classified as spam. *See* discussion *infra* Part III.A.2.

disclosing a precise threshold.[22] An arbitrary number could certainly be selected, such as ten or one thousand copies sent within one day or one week.[23] Alternatively, a specified number of independent reports of a message sent to undisclosed recipients[24] could give rise to a presumption that the message was sent in bulk.[25]

[22] Among the arguments against a precise threshold are: while the damage caused by spam is usually related to the number of copies of a message that are transmitted, the relationship is not necessarily proportional, and a small-scale spam can cause as much damage as a large-scale one; spammers would respond to a clearly disclosed threshold by adjusting their message volume to accommodate it (for example, by sending one message fewer than the threshold within the specified time period); the existence of a fixed threshold would encourage spammers to find ways to circumvent it (for example, by sending spam under different names, or by spreading their message traffic over a slightly longer time period); and the certainty and approbation afforded by such a threshold would legitimize the actions of existing spammers and encourage others to begin spamming.

In contrast, there are commonly applied formulae for determining whether messages posted to Usenet newsgroups qualify as spam. The Breidbart Index is one example, which uses a function of the number of separate copies of a message that are posted and the number of newsgroups to which each copy is cross-posted. *See* SCHWARTZ & GARFINKEL, *supra* note 2, at 31. Various automated and manual services use the Breidbart Index to decide whether to post "cancel" messages intended to halt propagation of the putative spam. *See id.*

[23] *See, e.g.*, LA. REV. STAT. ANN. § 14:73.1(13) (West Supp. 2000) (defining "unsolicited bulk electronic mail" as an e-mail advertisement that is "sent in the same or substantially similar form to more than one thousand recipients"); Act of Apr. 17, 2000, ch. 423, § 1, 2000 Idaho Sess. Laws 1373, 1373 (to be codified at IDAHO CODE § 48-603E(1)(a)) (defining "bulk electronic mail advertisement" as "the same or similar advertisement . . . contemporaneously transmitted to two (2) or more recipients"); Eriecoast, *Eriecoast Service Policy and Acceptable Practices*, *at* http://www.eriecoast.com/About_Us/Policies_Procedures/policies_procedures.html (last visited Aug. 8, 2000) (20 or more recipients); Flashcom, Inc., *Acceptable Use Policy*, *at* http://www.flashcom.com/pdfs/acceptableuse.pdf (Feb. 2000) (10 or more recipients); InterAccess Co., *Acceptable Use Policy*, *at* http://www.interaccess.com/products/aup.shtml (last modified Aug. 19, 1999) (more than 10 recipients) [hereinafter InterAccess, *Acceptable Use Policy*]; Juno Online Servs., Inc., *Guidelines for Acceptable Use*, *at* http://account.juno.com/policies/guidelines.html (last visited Aug. 8, 2000) (more than 50 recipients) [hereinafter Juno, *Guidelines*].

[24] *See* discussion *supra* note 18 (describing use of BCC header lines to conceal recipients of a bulk message).

[25] The number of copies that ought to be required to trigger a presumption of bulk mailing should be relatively low, since it is unlikely that most of the copies will be reported—even if most of them are deliverable, and even if centralized spam collection efforts such as the Spam Recycling Center are successful. *See* discussion of Spam Recycling Center *infra* note 99. If the conclusion that a message constitutes spam is likely to result in sanctions, then the severity of those sanctions also ought to be considered in determining the number of copies that must be reported, since that number will have a substantial effect on the rate of false positives.

4. UBE Versus UCE

There are many varieties of noncommercial spam, including charitable fundraising solicitations,[26] opinion surveys,[27] religious messages,[28] political advertisements,[29] wartime propaganda,[30] virus hoaxes and other urban legends,[31] chain letters,[32] and hate e-mail.[33] Nonetheless, at present, most unsolicited bulk e-mail messages contain commercial advertisements, and the vast majority of unsolicited commercial e-mail messages are sent in bulk.[34] The distinction between unsolicited commercial e-mail ("UCE") and unsolicited bulk e-mail ("UBE"), therefore, may be somewhat academic, though it is the subject of considerable controversy within the anti-spam community, as well as among legislative bodies that have considered enacting restrictions on spam.[35]

[26] *See, e.g.*, Chris Partridge, *Charities Learn to Love the Internet*, TIMES (London), July 20, 1999, 1999 WL 8009970.

[27] *See, e.g.*, SCHWARTZ & GARFINKEL, *supra* note 2, at 21–22; Jean Goodwin, *Research or Spam? A Case Study in University Network Use Policy*, *at* http://pubweb.acns.nwu.edu/~jgo259/resspam/front.html (1998).

[28] *See, e.g.*, Eric Blom, *Online Evangelists Spread Word but the Message Is Not Always Welcome on the Internet, as Barrages of Hostile E-Mail Attest*, PORTLAND PRESS HERALD, Feb. 16, 1997, 1997 WL 4117507; WitchVox, *Community Thoughts Specifically on PAGAN Spam*, *at* http://www.witchvox.com/surveys/pagan_spamthoughts.html (Sept. 4, 1999).

[29] *See* Deborah Scoblionkov, *When Candidates Spam*, SALON, Feb. 19, 1999, *at* http://www.salon.com/21st/feature/1999/02/19feature.html.

[30] *See* Editorial, *Waging War by E-Mail*, CHI. TRIB., Apr. 3, 1999, 1999 WL 2859907 (describing Serbian spam campaign ridiculing NATO attack).

[31] *See* Computer Incident Advisory Capability, U.S. Dep't of Energy, *Hoax Busters*, *at* http://hoaxbusters.ciac.org/ (last modified Jan. 17, 2001); Patrick Crispen, *Map09: Spamming and Urban Legends*, *at* http://www.webreference.com/roadmap/map09.html (last modified Sept. 30, 1996).

[32] *See* Computer Incident Advisory Capability, U.S. Dep't of Energy, *Hoax Busters*, *at* http://hoaxbusters.ciac.org/ (last modified Jan. 17, 2001); Ind. Univ. Knowledge Base, *What Is Electronic Chain Mail?*, *at* http://kb.indiana.edu/data/aexs.html (last modified June 12, 1997).

[33] *See, e.g.*, David Rosenzweig, *Man Charged in Sending Hate E-Mail to Latinos Across U.S.*, L.A. TIMES, Jan. 29, 1999, at B1; Eric Slater, *Racist E-Mail at Iowa College Is Linked to Black Student*, L.A. TIMES, Apr. 21, 2000, at A31.

[34] *See* Brad Templeton, *Top Ten Reasons Not to Regulate Non-Bulk E-mail*, *at* http://www.templetons.com/brad/spume/top10.html (last visited Dec. 27, 2000).

[35] The leading anti-spam advocacy group is the Coalition Against Unsolicited Commercial Email (CAUCE); its international affiliates include CAUCE India, the European Coalition Against Unsolicited Commercial Email (EuroCAUCE), and the Coalition Against Unsolicited Bulk Email, Australia (CAUBE.AU). *See CAUCE*, *at* http://www.cauce.org (last visited Aug. 8, 2000); *CAUBE.AU*, *at* http://www.caube.org.au (last visited Aug 8, 2000); *CAUCE India*, *at* http://www.india.cauce.org/ (last visited Aug. 8, 2000); *EuroCAUCE*, *at* http://www.euro.cauce.org/ (last visited Aug. 8, 2000). Among American states that have enacted spam-related legislation, some have focused on UCE, others on UBE, and yet others on UBCE. *See* discussion *infra* Part IV.B.

a. Arguments for Defining Spam as UCE

Several arguments support defining spam as UCE: (1) Because spam shifts costs from the sender to recipients,[36] its use for commercial purposes is particularly objectionable; (2) Defining spam as UCE rather than UBE avoids the need to establish a specific threshold for "bulk;" (3) Noncommercial messages (especially political and religious messages) may be protected speech, while commercial messages can be regulated without running afoul of the First Amendment;[37] (4) Existing laws regulating commercial telephone and facsimile machine solicitations[38] could easily be extended to cover commercial solicitations transmitted by e-mail;[39] and (5) Regulation limited to commercial messages stands a better chance of being adopted than does regulation applicable to both commercial and noncommercial messages.

[36] *See* David E. Sorkin, *Unsolicited Commercial E-Mail and the Telephone Consumer Protection Act of 1991*, 45 BUFF. L. REV. 1001, 1010 & nn.45–46 (1997) (describing cost-shifting effects of spam), *available at* http://www.spamlaws.com/articles/buffalo.html.

[37] *Cf., e.g.*, Lutz Appellate Servs. v. Curry, 859 F. Supp. 180, 182 (E.D. Pa. 1994) (dictum) (questioning whether Congress could constitutionally prohibit all unsolicited fax transmissions, rather than only unsolicited advertisements). *But cf.* City of Cincinnati v. Discovery Network, Inc., 507 U.S. 410, 424 (1993) (holding that government cannot restrict only commercial speech without an adequate basis for distinguishing between commercial and noncommercial speech). First Amendment concerns are largely beyond the scope of this Article. For analyses of the First Amendment implications of legal restrictions on spam, see Steven E. Bennett, Note, *Canning Spam:* CompuServe, Inc. v. Cyber Promotions, Inc., 32 U. RICH. L. REV. 545 (1998); Michael W. Carroll, *Garbage In: Emerging Media and Regulation of Unsolicited Commercial Solicitations*, 11 BERKELEY TECH. L.J. 233 (1996), *available at* http://www.law.berkeley.edu/journals/btlj/articles/11-2/carroll.html; Cathryn Le, Note, *How Have Internet Service Providers Beat Spammers?*, 5 RICH. J.L. & TECH. 9 (1998), *at* http://www.richmond.edu/jolt/v5i2/le.html; Richard C. Lee, Note, Cyber Promotions, Inc. v. America Online, Inc., 13 BERKELEY TECH. L.J. 417 (1998); Marcus, *supra* note 2.

Nearly all of the spam-related lawsuits to date have involved commercial messages. *See* discussion *infra* Part IV.A. *But see* Intel Corp. v. Hamidi, No. 98AS05067, 1999 WL 450944, at *1, *3 (Cal. Super. Ct. Apr. 28, 1999) (enjoining defendant from sending bulk messages protesting plaintiff's employment practices into plaintiff's e-mail system), *appeal filed*, No. C033076 (Cal. Ct. App. Jan. 18, 2000), http://www.intelhamidi.com/appealbrief.htm. *Intel Corp.* is discussed at length in Susan M. Ballantine, Note, *Computer Network Trespasses: Solving New Problems with Old Solutions*, 57 WASH. & LEE L. REV. 209 (2000), and in *Developments in the Law—The Law of Cyberspace: The Long Arm of Cyber-reach*, 112 HARV. L. REV. 1610, 1622–24, 1629–34 (1999) [hereinafter *Developments*].

[38] *See, e.g.*, Telephone Consumer Protection Act of 1991, 47 U.S.C. § 227 (1994).

[39] This approach was taken in one of the first federal spam bills. *See* Netizens Protection
Act of 1997, H.R. 1748, 105th Cong. (1997).

b. Arguments for Defining Spam as UBE

The primary argument for defining spam as UBE is simply that the commercial or noncommercial nature of an unsolicited message has little or nothing to do with the damage that is inflicted. The problem is not exactly that costs are shifted from the sender to recipients, but merely that recipients, and intermediate networks, sustain costs involuntarily—the sender's motivation is largely irrelevant.[40] Furthermore, a legal rule against all unsolicited bulk e-mail is arguably more content-neutral than a rule that focuses on commercial messages.[41] A rule focusing only on commercial messages might well open the floodgates to a massive increase in noncommercial spam.[42] Since the problem with spam is volume, not content, the UBE approach seems to make more sense.

Restricting all unsolicited e-mail, rather than merely UCE or UBE, is probably not a realistic option. Individual, noncommercial, unsolicited messages are far less objectionable than UCE or UBE,[43] and a much stronger case can be made for constitutional protection of such messages than for either UCE or UBE.

A fourth alternative would be to limit the definition to messages that are both commercial and sent in bulk, "UBCE" for short. Since nearly all UCE is sent in bulk, this approach is roughly equivalent to defining spam as UCE, though it would be accompanied by the same evidentiary difficulties as the UBE definition.

Whichever definition of spam is used, there are likely to be significant problems in defining precisely what is meant by "commercial" or

[40] It may make more sense to adjust the penalty according to the sender's motives or the message content, just as one might penalize a thief more harshly than a vandal.

[41] This is not to argue that a distinction between commercial and noncommercial messages is legally indefensible—the Ninth Circuit deferred to Congress' findings when it upheld the unsolicited fax law, 47 U.S.C. § 227 (1994), in *Destination Ventures, Ltd. v. FCC*, 46 F.3d 54, 54 (9th Cir. 1995). Similar legislative findings could likely support a ban on UCE, as well as a ban on all UBE.

[42] For example, one person could send messages espousing a particular view on a political or social issue to millions of Internet users. If recipients appear to be hostile to such messages, then the sender might send messages espousing the opposite view—and conceivably, the sender's goal might be merely to draw attention to an issue. It is perhaps surprising that anti-spam activists have not already begun using spam to promote their views—certainly most people who found themselves receiving hundreds or thousands of such "junk" messages each day would want something to be done about it.

[43] Examples of individual noncommercial unsolicited messages include a message of introduction to a person whom the sender believes to be a relative or former classmate, and a request for permission to quote another person in print, or to reprint an excerpt from the person's writing, or to link to the person's web site. All of these are unsolicited messages, but under ordinary circumstances few people would consider them to be spam.

"bulk" e-mail, and these definitional problems may serve as a barrier to effective responses to the spam problem.

B. The Spam Problem

1. Objectionable Content

Spam is problematic for a number of reasons. Many of the objections to spam relate to its content. For example, some object to receiving commercial messages, particularly those that promote questionable ventures like pyramid schemes and multi-level marketing scams.[44] Others are offended by messages that contain or advertise sexually explicit material.[45] Such messages are particularly troubling when they are sent to minors; senders of unsolicited messages rarely know the age of persons to whom the messages are sent.[46] Spam with hostile file attachments or embedded code can even pose a security threat, as was the case with the Melissa virus spam.[47] But spam is also problematic for reasons unrelated to its content.

2. Consumption of Internet Resources

Spam represents a significant proportion of all e-mail traffic, consuming massive amounts of network bandwidth, memory, storage space, and other resources.[48] Internet users and system administrators

[44] The Federal Trade Commission ("FTC") in particular has focused on spam that promotes fraudulent activities. *See, e.g.*, *Spamming: The E-Mail You Want to Can: Hearing Before the Subcomm. on Telecomm., Trade, & Consumer Protection of the House Comm. on Commerce*, 106th Cong. 23 (1999) (statement of Eileen Harrington, FTC Bureau of Consumer Protection), 1999 WL 27596532 [hereinafter *1999 House Hearing*]; Federal Trade Comm'n, *FTC Consumer Alert!: FTC Names Its Dirty Dozen: 12 Scams Most Likely to Arrive Via Bulk Email*, *at* http://www.ftc.gov/bcp/conline/pubs/alerts/doznalrt.htm (July 1998); Federal Trade Comm'n, *FTC Sues Spammer: Alleges Business Opportunity Falsely Promoted in Unsolicited Commercial E-Mail*, *at* http://www.ftc.gov/opa/1998/9803/ibb.htm (Mar. 4, 1998). *See generally* Jennifer M. Kappel, Comment, *Government Intervention on the Internet: Should the Federal Trade Commission Regulate Unsolicited E-Mail Advertising?*, 51 ADMIN. L. REV. 1011 (1999).

[45] *See, e.g.*, W. VA. CODE ANN. § 46A-6G-2(4) (Michie 1999); Jo Vandermause, Comment, *You've Got Indecent E-Mail!*, 1999 WIS. L. REV. 1259.

[46] *See* Reno v. ACLU, 521 U.S. 844, 855–56 & n.20 (1997).

[47] *See* Andrew Brown, *Micro Organism (Spamming)*, NEW STATESMAN, Apr. 9, 1999, 1999 WL 13029502; Mitch Wagner, *Melissa Puts IT Readiness to Test*, INTERNET WK., Apr. 5, 1999, http://www.internetwk.com/story/INW19990402S0003 (discussing how the Melissa virus infected computers use "of Microsoft Office macros and the Microsoft Outlook e-mail client to broadcast itself over the Internet, tying up network traffic and infecting computers with code that could rebroadcast any document created with Microsoft Word").

[48] *See 1999 House Hearing*, *supra* note 44, at 41 (statement of Michael Russina, SBC Internet Services) (citing spam rate of 35%, and describing spam-related costs incurred by SBC); *1998 Senate Hearing*, *supra* note 1, at 27–28 (statement of Ray Everett-Church, Coalition Against Unsolicited Commercial Email) (discussing costs imposed by spam); Cranor &

spend a great deal of time reading, deleting, filtering, and blocking spam, so Internet users pay more for Internet access as a result of spam.[49] Spam and anti-spam measures frequently interfere with other e-mail traffic and other legitimate Internet uses.[50]

Spam has few redeeming features to balance these substantial costs. It is a singularly ineffective method of direct marketing,[51] but

LaMacchia, *supra* note 9, at 75, 78 (reporting spam rates of 2% for a large ISP and 10% for a corporate network, and citing other estimates of 30% to 50% for AOL and 15% for another ISP); Daniel P. Dern, *Postage Due on Junk E-Mail—Spam Costs Internet Millions Every Month*, INTERNET WK., May 4, 1998, at T1 (citing spam rates ranging from 3% to 30% at various ISPs, and discussing costs imposed by spam), http://www.techweb.com/se/directlink.cgi?INW19980504S0003; Jim Hu, *Yahoo Adds Spam Filter to Email, But Will It Work?*, CNET NEWS.COM, Dec. 1, 1999 (citing estimate that spam represents 10% of all e-mail traffic), *at* http://news.cnet.com/news/0-1005-200-1476013.html.

[49] *See, e.g.*, Dern, *supra* note 48 (claiming that individual customers of ISPs pay nearly $2 extra per month because of e-mail and Usenet spam); *see also* authorities cited *supra* note 48.

[50] *See, e.g.*, Am. Online, Inc. v. Prime Data Sys. Inc., No. 97-1652-A, 1998 U.S. Dist. LEXIS 20226, at *6 (E.D. Va. Nov. 20, 1998) (describing outages caused by inbound spam); *1998 Senate Hearing*, *supra* note 1, at 27 (statement of Ray Everett-Church, Coalition Against Unsolicited Commercial Email) (same); Alan Boyle, *Spam Hits the House of Representatives*, ZDNET, Oct. 5, 1999 (same), *at* http://www.zdnet.com/zdnn/stories/news/0,4586,2347919,00.html; Jeremy Crandell, *The Cost of Spam*, *at* http://www.brightmail.com/spam/cost/ (last visited Aug. 8, 2000) (same); Cyber Promotions, Inc. v. Apex Global Info. Servs., Inc., No. 97-5931, 1997 U.S. Dist. LEXIS 15344, at *2 n.2 (E.D. Pa. Sept. 30, 1997) (describing denial-of-service attacks on spammer's ISP); Carol Neshevich, *ISP Burned by Spammer*, NETWORK WORLD CAN., Apr. 24, 1998, LEXIS, All News Group File (describing denial-of-service attacks targeting company whose name appeared in spam); Plaintiff's Complaint, Hall v. Earthlink Network, Inc. (S.D.N.Y. July 30, 1998) (No. 98-CIV-5489) (describing ISP's cancellation of subscriber's account based upon erroneous spamming accusation), http://www.epic.org/privacy/internet/hall-complaint-798.html [hereinafter Hall Complaint]; Chris Oakes, *The Case of the Mistaken Spammer*, WIRED NEWS, May 4, 1998 (same), *at* http://www.wired.com/news/news/technology/story/12065.html; Ed Foster, *Spammers Get Aggressive: Readers Report Threats and E-Mail Bomb Attacks*, INFOWORLD, Apr. 10, 2000, at 114 (describing mailbombing attacks by spammers against anti-spam activists), http://www.infoworld.com/articles/op/xml/00/04/10/000410opfoster.xml; Todd Wallack, *AOL Blocking Pac Bell E-Mail in Effort to Thwart Spammers*, S.F. CHRON., Apr. 21, 2000, at B1 (describing how spam-blocking measures also block legitimate e-mail); Jon Swartz, *Anti-Spam Service or McCarthyism?*, S.F. CHRON., May 10, 1999, at B1 (same); Andrew Backover, *E-mail "Spat" Being Settled at E-snail's Pace*, DENVER POST, Nov. 13, 1999, 1999 WL 27561751 (same); Paul Eng, *An Innocent Company Gets Snared in an Anti-Spam Sweep*, BUS. WK. ONLINE, Dec. 17, 1998 (same), *at* http://www.businessweek.com/smallbiz/news/date/9812/e981217.htm; Jason Krause, *Anti-Spam Zealots Cross the Line*, INDUSTRY STANDARD, Dec. 17, 1998 (same), http://www.thestandard.net/article/display/0,1151,2889,00.html; Lawrence Lessig, *The Spam Wars*, INDUSTRY STANDARD, Dec. 31, 1999 (same), http://www.thestandard.com/article/display/0,1151,3006,00.html [hereinafter Lessig, *Spam*]; Paul McNamara, *War on Spam Claims Legit E-mail*, NETWORK WORLD, May 17, 1999, 1999 WL 11619735 (same). For a definition of "mailbombing," see *infra* note 68. For a definition of "denial-of-service" attack, see *infra* note 66.

[51] Response rates for spam generally are infinitesimal compared to other forms of direct marketing. *See, e.g.*, Posting of Robert Maynard, Robert.Maynard@goodparents.com,

for the fact that few of the costs involved are incurred by the spammers themselves. In most forms of communication, the sender experiences significant and, usually, measurable costs. Therefore, the sender usually has an incentive to compare the expected benefits of the communication against these costs in deciding whether to proceed with the communication, and, in the case of an advertisement, how broad or narrow a group of prospects to target.[52] E-mail changes the entire equation because the cost of sending unsolicited bulk e-mail is negligible.[53] Spammers, unlike senders of non-electronic communications, have little incentive to consume resources in an efficient manner.

Much of the concern over spam arises because of the prospect that its volume could increase exponentially in the future.[54] Some of the current responses to spam, such as deletion and filtering by recipients, could be rendered obsolete by such an expansion.[55] The cost increases that would result from a massive increase in volume could

to news.admin.net-abuse.email, *available at* http://www.physics.helsinki.fi/~puolamak/spam/maynard.txt (June 24, 1997) (citing response rate of zero in 100,000); Deborah Scoblionkov, *Politician Spams 5 Million Users*, WIRED NEWS, June 29, 1998 (quoting a 22-year-old local political candidate who spammed Internet users around the world as seeking a response rate of one percent of one percent of one percent), *at* http://www.wired.com/news/news/politics/story/13329.html; Wave 5 Mktg., *Bulk and Opt-In Mail Lists: The Good and the Bad, at* http://www.wave5marketing.com/bulkemail.htm (last modified Sept. 20, 2000) (citing response rate of 0.1%).

[52] Traditional advertisers calculate what it costs to place a commercial on a television program, or to send a brochure to everyone on a mailing list, and weigh that against the projected revenues of the ad campaign. A projected response rate of 2% may be sufficient for a direct mail solicitation if the average net revenue per sale is $25 and the cost of preparing and sending out the mailing is less than 50 cents per piece.

[53] A spammer's costs include finding a cooperative or naïve Internet service provider, figuring out how to send spam, composing the message text, and setting up a system for receiving payment and processing orders. These costs generally are independent of the volume of messages that is sent (or at the least, the marginal cost is negligible), and, therefore, the spammer has an incentive to send as many messages as humanly possible, with little regard for the response rate or the costs borne by third parties.

[54] *See* Sally Hambridge & Albert Lunde, *Don't Spew: A Set of Guidelines for Mass Unsolicited Mailings and Postings (Spam) (Request for Comments No. 2635)*, at 5, *at* http://www.isi.edu/in-notes/rfc2635.txt (June 1999). In addition to an increase in the number of unsolicited messages, the average size of each message is also likely to increase. Campaign messages e-mailed on behalf of United States presidential candidate Steve Forbes in early 2000 included a multimedia file that was nearly 1 megabyte in size. *See Steve Forbes Aligns with eCommercial.com to Create Next-Generation Video Internet Marketing Campaign Tool*, BUS. WIRE, Jan. 14, 2000, LEXIS, News Library, Bwire File ("'We look forward to leveraging eCommercial's powerful video delivery to promote Steve Forbes' candidacy and to get his message out, unfiltered, to the millions of voters who now use the Internet to get their information.'").

[55] *See* discussion of filtering *infra* Part III.A.

even lead many sites to discontinue supporting standard e-mail altogether.[56] Within a few years, e-mail may no longer be the near-universal method for communicating with people via the Internet that it is today.

3. Threat to Internet Security

Spam is both a wasteful activity and one that poses a threat to the security and reliability of Internet communications. For example, a common practice by many spammers is the exploitation of "mail relays." A third-party mail relay is when a spammer connects to a Simple Mail Transfer Protocol ("SMTP") server operated by a third party, where neither the spammer nor the recipients are local users, and directs the server to send copies of a message to a long list of recipients.[57] Many sites permit use of their servers only to messages sent to or from their own users, but there are still many so-called "open" servers that lack such restrictions—17% in July 1999, according to one survey, down from 36% a year earlier.[58]

Spammers use open relays to disguise the origin of their messages, to deflect complaints, to circumvent "spamblocking" by other sites, and to increase the volume of messages they can send.[59] Third-party relaying usually represents theft of service because it is an unauthorized appropriation of computing resources. Third-party re-

[56] Admittedly, it is hard to envision the Internet without e-mail, but there are already some signs that point in this direction. E-mail address harvesting by spammers has led many people to replace "mailto" links on web pages with web-based response systems that conceal one or both parties' e-mail addresses. *See, e.g.*, *FormMail.To/You!*, *at* http://formmail.to/ (last visited Aug. 8, 2000); Cameron Gregory, *Spambot.com*, *at* http://www.spambot.com (last visited May 1, 2000); *Memo.to*, *at* http://memo.to/ (last visited Aug. 8, 2000); *Response-O-Matic*, *at* http://www.response-o-matic.com/ (last visited Aug. 8, 2000). Usenet articles frequently appear with fictitious, munged, or disposable addresses, and some Usenet and mailing list archives obscure all e-mail addresses, also to frustrate harvesting. *See, e.g.*, eGroups*: No Spam!*, *at* http://www.egroups.com/info/nospam.html (last visited Aug. 8, 2000); Topica, *Topica's Position on "Spam," at* http://www.topica.com/pop/spam.html (last visited Aug. 8, 2000); *see infra* note 121 and accompanying text (defining "munge"). Many service providers now restrict even their own subscribers' access to e-mail services, primarily because of abuse by third parties. *See* discussion *infra* note 109.

[57] *See* SCHWARTZ & GARFINKEL, *supra* note 2, at 90–91; *supra* note 18 (discussing Simple Mail Transfer Protocol).

[58] *See* Paul Hoffman, *Allowing Relaying in SMTP: A Series of Surveys (Internet Mail Consortium Report: UBE-RELAY IMCR-013)*, *at* http://www.imc.org/ube-relay.html (last modified July 5, 1999). *See generally* Gunnar Lindberg, *Anti-Spam Recommendations for SMTP MTAs (Request for Comments No. 2505)*, at 2, *at* http://www.isi.edu/in-notes/rfc2505.txt (Feb. 1999) (noting that "[e]ven if 99% of the SMTP [mail transfer agents] implemented [anti-relay rules] from Day 1, spammers would still find the remaining 1% and use them").

[59] *See* Hambridge & Lunde, *supra* note 54, at 4; Hoffman, *supra* note 58.

laying consumes bandwidth and storage capacity and can result in performance degradation and even system crashes.[60] The highest costs usually are the staff time needed to deal with bounced messages,[61] complaints, and system reconfiguration.[62] A company's reputation can also be damaged if it is associated with spam as a result of third-party relaying.[63]

Forgery of message headers is another tactic commonly used by spammers.[64] Spam tends to generate a lot of complaints from irate recipients, so spammers usually try to deflect those complaints by using a false return e-mail address in the message header, often combined with a false "remove" address in the body of the message.[65] Web sites that appear in spam through forgery may be entirely unrelated to the sender of the spam, but often find themselves deluged with complaints and even intentional denial-of-service attacks.[66] There have even been instances of spammers targeting anti-spammers by including the domain names of anti-spammers in the spam as a reputation attack.[67]

4. Other Consequences of Spam

Responses to spam can also be problematic. For example, web sites that have been implicated in spamming—correctly or incor-

[60] *See* Lindberg, *supra* note 58, at 2.

[61] *See* Denis Howe ed., *Free On-Line Dictionary of Computing*, *at* http://foldoc.doc.ic.ac.uk/foldoc/foldoc.cgi?bounce+message (last modified Nov. 29, 1994) (defining "bounce message" as "[a] notification message returned to the sender by a site unable to relay e-mail to the intended recipient").

[62] *See* Hambridge & Lunde, *supra* note 54, at 4; Hoffman, *supra* note 58.

[63] *See* Juno Online Servs., Inc., *Juno Sues E-mail Forgers in Fight Against Spam*, *at* http://help.juno.com/privacy/lawsuit/juno_sues.html (last visited Dec. 27, 2000).

[64] "Forgery" in this context refers merely to the use of fictitious message headers; it does not carry the same implications as the criminal sense of the term. *See* Seidl v. Greentree Mortgage Co., 30 F. Supp. 2d 1292, 1317 (D. Colo. 1998). Forgery of mail headers is sometimes referred to as "e-mail spoofing." *See* CERT Coordination Ctr., *Spoofed/Forged Email*, *at* http://www.cert.org/tech_tips/email_spoofing.html (last modified Mar. 20, 2000); IBM, *Spamming Issues and Topics*, *at* http://www.vm.ibm.com/related/tcpip/spam-mc.html (last visited Aug. 8, 2000).

[65] *See* Hambridge & Lunde, *supra* note 54, at 2.

[66] *See, e.g.*, Neshevich, *supra* note 50 (describing denial-of-service attacks targeting a company whose name appeared in spam, yet did not send any). For a definition of "denial-of-service attack," see CERT Coordination Ctr., *Denial of Service*, *at* http://www.cert.org/tech_tips/denial_of_service.html (last modified Feb. 12, 1999) ("A 'denial-of-service' attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service.").

[67] *See* Hambridge & Lunde, *supra* note 54, at 15.

rectly—have been subjected to e-mail bombs[68] and other attacks.[69] Companies that provide services to spammers also can find themselves under siege.[70]

Individual users with no connection to spammers or spamfighters are also affected by responses to spam. For example, many mobile users rely on open relays for sending e-mail while connected from a remote site, and restrictions on relaying make it harder for companies to support such users.[71] Automated filtering and blocking techniques,[72] blackholing[73] of spam-friendly sites, and other responses to spam also interfere with legitimate e-mail traffic.[74]

II. Informal Approaches

A. Self-Regulation: Netiquette and Acceptable Use Policies

Until about 1996, social pressures were the predominant approach used to combat spam.[75] Particularly in the early stages of the

[68] Referred to as either an "e-mail bomb," a "mailbomb," or "mailbombing," this practice refers "[t]o send[ing], or urg[ing] others to send, massive amounts of electronic mail to a single system or person, with intent to crash or spam the recipient's system." Denis Howe ed., *Free On-Line Dictionary of Computing*, *at* http://foldoc.doc.ic.ac.uk/foldoc/foldoc.cgi?query=mailbomb (last modified Apr. 4, 1995) (defining "mail bomb"). *See, e.g.*, Cyber Promotions, Inc. v. Am. Online, Inc., 948 F. Supp. 436, 437 & n.1 (E.D. Pa. 1996) (describing alleged mailbombing of spammer's ISP); Ed Foster, *Spammers Get Aggressive: Readers Report Threats and E-Mail Bomb Attacks*, INFOWORLD, Apr. 10, 2000, at 114 (describing mailbombing attacks by spammers against anti-spam activists), http://www.infoworld.com/articles/op/xml/00/04/10/000410opfoster.xml; Karen Stuart, *Telstra and Optus Blacklisted by ORBS*, INTERNETNEWS.COM, July 31, 2000 (citing claim that a major ISP accused of harboring spammers mailbombed people who submitted complaints), *at* http://www.internetnews.com/intl-news/article/0,,6_425981,00.html.

[69] *See, e.g.*, Neshevich, *supra* note 50, Tim Richardson, *Cisco Tells Spam Victims to Reply with Abusive Emails*, REG. (London), Apr. 4, 2000 (reporting recommendation, later recanted, that Internet users should retaliate against spammers by sending abusive e-mail messages or by clogging their servers with massive files), http://www.theregister.co.uk/content/archive/10158.html.

[70] *See* Cyber Promotions, Inc. v. Apex Global Info. Servs., Inc., No. 97-5931, 1997 U.S. Dist. LEXIS 15344, at *2 n.2 (E.D. Pa. Sept. 30, 1997); Cyber Promotions, Inc. v. Am. Online, Inc., 948 F. Supp. 436, 437 & n.1 (E.D. Pa. 1996); SCHWARTZ & GARFINKEL, *supra* note 2, at 179–81.

[71] *See* SCHWARTZ & GARFINKEL, *supra* note 2, at 90.

[72] *See* discussion *infra* Part III.A.1.

[73] *See* discussion *infra* Part III.A.3 and accompanying notes (discussing blackholing and blackhole lists).

[74] *See* discussion *supra* note 50 and accompanying text.

[75] The historical prevalence of informal remedies can be attributed in part to the largely informal nature of Internet governance as a whole. *See, e.g.*, David E. Sorkin, *Revocation of an Internet Domain Name for Violations of "Netiquette": Contractual and Constitutional*

Internet, informal rules of netiquette and loosely applied acceptable use policies prohibited or at least discouraged most commercial uses of Internet resources.[76] Spam, and, to a lesser extent, all commercial activity, had a substantial stigma attached to it, enough to dissuade most Internet users from considering such activity.[77]

As commercial activities became generally accepted on the Internet and ultimately far surpassed the volume of academic and research usage, network rules and policies gradually began to focus on more specific objectionable uses, including spam. Now, nearly all Internet service providers ("ISPs") post clear policies prohibiting the use of their facilities for sending spam.[78] Spammers and spam-friendly providers increasingly find themselves blacklisted and boycotted,[79] just as those who violate real-world norms may be criticized or shunned by their peers.

Industry groups representing marketers and ISPs have attempted to address the spam problem with self-regulatory efforts. For example, members of 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 are prohibited from sending unsolicited commercial e-mail messages to addresses that appear in the DMA's e-Mail Preference Service database.[80] The Internet Alliance's "spamming guidelines" say

Implications, 15 J. MARSHALL J. COMPUTER & INFO. L. 587, 595 (1997) (describing private entities with influence and authority over the Internet). In addition, spam simply did not represent a significant problem until the mid-1990s, even though it was recognized as a potential problem as early as 1975. *See* Cranor & LaMacchia, *supra* note 9, at 74; Jon Postel, *On the Junk Mail Problem (Request for Comments No. 706), at* http://www.isi.edu/in-notes/rfc706.txt (Nov. 1975).

[76] A summary of generally accepted rules of netiquette appears in Sally Hambridge, *Netiquette Guidelines (Request for Comments No. 1855), at* http://www.isi.edu/in-notes/rfc1855.txt (Oct. 1995).

[77] *See* Cranor & LaMacchia, *supra* note 9, at 82.

[78] A compilation of such policies is available at Whew.com!, *ISP/Domain Acceptable Use Policies/Terms of Service, at* http://www.whew.com/Spammers/aup.shtml (last visited Apr. 24, 2000).

[79] *See, e.g.*, Axel Boldt, *Blacklist of Internet Advertisers, at* http://math-www.uni-paderborn.de/~axel/BL/blacklist.html (last modified Nov. 6, 2000); *see also* discussion *infra* Part III.A.3 and accompanying notes (discussing Realtime Blackhole List and similar technical responses). Although such responses represent a form of social pressure, they are treated in this Article primarily as a more formal technical response, since their effects on spamming seem to result primarily from the architectural constraints that they impose (i.e., actually blocking e-mail message traffic) rather than from the unfavorable publicity or other social effects that they generate.

[80] *See 1999 House Hearing*, *supra* note 44, at 49–50 (statement of Jerry Cerasale, Direct Mktg. Ass'n); Direct Mktg. Ass'n, *e-Mail Preference Service, at* http://www.e-mps.org/ (last visited Aug. 8, 2000); Direct Mktg. Ass'n, *Privacy Promise Member Compliance Guide, at* http://www.the-dma.org/library/privacy/privacypromise.shtml (last visited Aug. 8, 2000).

that marketers should not collect e-mail addresses in online forums for the purpose of sending unsolicited e-mail unless permitted to do so by the forum.[81] The Association for Interactive Media ("AIM") has stated its opposition to unsolicited bulk commercial e-mail, but has not prohibited the practice.[82]

B. Problems with Self-Regulation

Yet informal responses like social pressure and industry self-regulation have generally had little effect on spam. Spamming has always been a fringe activity, and social pressures tend to be relatively ineffectual against those at the fringes of society, be they stealth spammers seeking relative obscurity or self-proclaimed "spam kings" flourishing in their own notoriety.[83] Furthermore, rules of netiquette generally lack enforcement mechanisms, and ISPs have had little success in attempting to impose their acceptable use policies upon those with whom they are not in privity, such as spammers attempting to send e-mail messages to their subscribers.[84] It is true that a significant stigma remains attached to the practice of spamming, and this stigma has helped stem the tide of spam.[85] Most commercial users of the Internet do not engage in spam, as much due to its stigma as because their own ISPs happen to prohibit the practice. But the rapid expansion of e-commerce has led more people to experiment with spam, and the stigma appears to be diminishing.[86] Voluntary industry efforts have

[81] *See* Internet Alliance, *IA Addresses Unsolicited Bulk E-Mail, at* http://www.internetalliance.org/policy/spamming_guidelines.html (last visited Aug. 8, 2000); *cf*. Internet Alliance, *Internet Alliance Sets Its Consumer E-Mail Agenda, at* http://www.internetalliance.org/news/000110.html (Jan. 10, 2000) (expressing support for "a combined industry/public/government response" to spam, including "surgically crafted legislation"). The DMA acquired the Internet Alliance (formerly the Interactive Services Association) in 1999.

[82] *See* Ass'n for Interactive Media, *Responsible E-Mail Marketing: Resolutions Hailed at Net.Marketing Conference in Seattle, at* http://www.interactivehq.org/html/pr_pages_26.htm (Feb. 29, 2000). AIM was acquired by the DMA in 1998.

[83] *See, e.g.*, Janet Kornblum, *Spamford Speaks*, CNET NEWS.COM, Mar. 31, 1997 (profiling Sanford Wallace, president of Cyber Promotions), *at* http://news.cnet.com/news/0-1014-201-1474964-0.html.

[84] *See* discussion *infra* Part IV.A.4 and accompanying notes.

[85] *See* Cranor & LaMacchia, *supra* note 9, at 82.

[86] Self-regulation arguably has done little more then lessen the stigma attached to spam. *See, e.g.*, Ian Oxman, *How the DMA Supports Spammers*, DM NEWS, Nov. 29, 1999 ("The only possible purpose of the E-MPS is to legitimize spamming."), *at* http://www.dmnews.com/archive/1999-11-29/5463.html. Another likely contributor to the destigmatization of spam is legislation that regulates spam without prohibiting it, such as the statutes enacted in Nevada and several other states beginning in 1997. *See* Cranor & LaMacchia, *supra* note 9, at 82; David E. Sorkin, *Written Comment, Federal Trade Commission Public Workshop on Consumer Information Privacy*, at 9, *at* http://www.ftc.gov/bcp/privacy/

failed for many reasons, perhaps most importantly because they have simply been ignored by most spammers, who have little reason to participate in such efforts.[87]

III. Technical Approaches

The first line of defense against spam normally consists of self-help and other technical mechanisms.[88] These mechanisms can be implemented by individual Internet users, ISPs and other destination operators,[89] as well as by various third parties, some of which specialize in battling spam.

A. Filtering and Blocking

1. End User Filtering

The easiest approach for individual end users is usually just to ignore unwanted messages. Users may try to recognize unwanted messages quickly—perhaps based upon an unfamiliar sender address, or a subject line that contains an obvious solicitation—and delete them without wasting much time reading them. Depending upon the e-mail software[90] being used, it may be possible to selectively delete

wkshp97/comments2/sorkin.htm (Apr. 14, 1997). Indeed, many unsolicited commercial e-mail messages now include claims of compliance with various statutes and unenacted bills. *See, e.g.*, Foster, *supra* note 50 ("Many [spammers] are citing the long-dead 'Murkowski' amendment . . . as giving them the legal right to send unsolicited commercial e-mail.").

[87] Although the Direct Marketing Association invites non-member companies to purge their e-mail lists using the DMA's e-Mail Preference Service, it charges them a fee for the privilege. *See* Direct Mktg. Ass'n, *e-Mail Preference Service: Clean My List, at* http://www.e-mps.org/en/list_sub_process.html (last visited Jan. 17, 2001). Even if there were no fee and no effort involved in purging a list, there would be little reason for non-DMA members to use the service. Indeed, it might even be reasonable for a spammer to expect the response rate for e-mail addresses that appear in the e-MPS database to be *higher* than for other addresses. *See* discussion *infra* note 130 (discussing opt-outs as prospects for subsequent solicitations).

[88] *See* CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1023 (S.D. Ohio 1997) (noting that "the implementation of technological means of self-help, to the extent that reasonable measures are effective, . . . should be exhausted before legal action is proper").

[89] A "destination operator" is "an organization or individual that maintains or controls a service for recipients of email and for allowing recipients to access their mail using a mail user agent." Paul Hoffman, *Unsolicited Bulk Email: Definitions and Problems (Internet Mail Consortium Report: UBE-DEF IMCR-004), at* http://www.imc.org/ube-def.html (Oct. 5, 1997). The term includes consumer-oriented ISPs, free web-based e-mail providers, corporate e-mail networks, and other e-mail service providers. *See id.*

[90] The word "software" is used rather loosely here; it includes the end user's e-mail client software, the mail server software, the protocol used to access the server, and other components of the system.

unwanted messages on the server without having to download them first. Most modern e-mail client software, such as Eudora and Microsoft Outlook, includes automatic filtering capabilities, some of which are specifically designed to identify and delete spam.[91] Messages can be filtered based upon the headers of a message or its full text and various spammer blacklists and spam archives can be used to help identify spam.[92]

While most filtering techniques involve rejecting messages that appear to be spam, it is also possible to reject all inbound messages except those that can be recognized as legitimate. Thus, for example, a recipient might accept only those messages with a header line saying "this message is not spam,"[93] or those accompanied by an electronic payment.[94] Nearly all filtering techniques result in false positives—le-

[91] *See* SCHWARTZ & GARFINKEL, *supra* note 2, at 75–78.

[92] *See* discussion *infra* Part III.A.3 (discussing blacklists).

[93] In theory, it would seem to be more efficient (and less burdensome on legitimate users) to require that spam include an affirmative statement that "this is spam," rather than to require legitimate messages to include the negative statement. In either instance, spammers would have an incentive to lie in order for their messages to get through—that is, to omit the "this is spam" statement, or to include a false "this is not spam" statement. The latter act might well be actionable under existing law, while new legislation would be needed to induce spammers to use affirmative labels.

Of course, the problem is much more complex than this summary analysis suggests. For example, blocking of unlabeled messages would be impractical until labeling became ubiquitous, and changes in most existing e-mail client software would be required to reach this stage. Definitional questions regarding what constitutes spam or other classifications subject to mandatory labeling must be addressed at the outset, and their resolution might well vary over time and across jurisdictions. Labels could provide much more information. For example, the Platform for Internet Content Selection ("PICS") specification allows labels to be associated with Internet content. *See Platform for Internet Content Selection, at* http://www.w3.org/PICS/ (last modified June 14, 2000). However, PICS in its current state does not support labeling of e-mail messages. *See* PICS, *PICS Frequently Asked Questions (FAQ), at* http://www.w3.org/2000/03/PICS-FAQ/ (last modified Apr. 4, 2000). If PICS did allow e-mail labeling, it would ameliorate the definitional concerns, but likely make the solution more expensive and less effective. *See generally* Lawrence Lessig & Paul Resnick, *Zoning Speech on the Internet: A Legal and Technical Model*, 98 MICH. L. REV. 395, 427–28 (1999).

[94] A variant of the "not spam" labeling idea would be to promote the inclusion of electronic payments in e-mail messages. Recipients and destination operators could refuse to accept messages not accompanied by sufficient payment, and recipients might choose to return the payment upon verifying the legitimacy of a message. Payments could be minimal—micropayments of a fraction of a cent per message, just enough to discourage large bulk mailings—or substantial enough to compensate recipients for the time and resource costs that they incur and possibly even provide funds for other purposes. *See* Lessig & Resnick, *supra* note 93, at 429; Sorkin, *supra* note 36, at 1031; Bob Metcalfe, *E-Postage Would Not Only Help Fund the System, but it Could Stop Spammers*, INFOWORLD, Jan. 20, 1997, *at* http://www.infoworld.com/cgi-bin/displayNew.pl?/metcalfe/bm012097.htm; Bob Metcalfe, *Pay-as-We-Go Internet Puts Your Money Where Your Consumption Is*,

gitimate messages mistakenly identified as spam.[95] It therefore may be desirable to place apparent spam into a lower priority channel rather than deleting it automatically,[96] but this approach obviously lessens the value of filtering as a solution since the spam has already been delivered.[97]

Filtering algorithms cannot detect all spam, so spammers have an incentive to structure their messages in a way that defeats automated filters, such as using false domain names or generic or personalized subject lines, for example. Furthermore, many individual users lack the sophistication necessary to implement filters effectively. Client-based filters generally do not eliminate the need to download each message before deciding whether to delete it—much of the damage is already done by the time the filter has an opportunity to do its job.

2. Collaborative Filtering by Third Parties

Filtering by ISPs and third-party proxy filtering services like Brightmail can be more effective than end user filtering, requiring less effort and expertise on the part of the users. For example, an ISP can block all traffic originating from a known spammer and may cooperate with other providers in identifying spammers. Individuals can have their incoming e-mail routed through a third-party proxy service that attempts to filter out spam.[98] One advantage to these technolo-

INFOWORLD, Sept. 21, 1998, *at* http://www.infoworld.com/cgi-bin/displayNew.pl?/metcalfe/980921bm.htm; Victoria Shannon, *Sending E-Mail and Paying Postage?*, INT'L HERALD TRIB., Sept. 17, 1998, 1998 WL 4794101. But the e-postage approach shares most of the problems of labeling, and carries with it substantial overhead costs, not to mention the likelihood of substantial resistance among Internet users.

[95] Another potential drawback of filtering and related approaches is the effect that they can have on legitimate users of anonymous and pseudonymous remailers, free web-based e-mail services like Hotmail, and e-mail "greeting card" services. Users of these services may find their communications blocked or filtered for no apparent reason, either because others have abused the services or, in some instances, because the services have been falsely associated with spam. *See, e.g.*, Plaintiff's Complaint, Hartford House, Ltd. v. Microsoft Corp. (Cal. Super. Ct. Dec. 8, 1998) (No. CV778550) (alleging that Microsoft's e-mail software improperly filters or blocks plaintiff's electronic greeting cards by designating them as junk mail), http://www1.bluemountain.com/home/bluemountain_vs_Microsoft.html; George William Herbert, *Greeting Card Websites and Spam, at* http://mail-abuse.org/gc_rbl.html (last modified July 20, 2000).

[96] *See, e.g.*, Hu, *supra* note 18.

[97] Prioritization of incoming messages does little to address the bandwidth and storage capacity problems caused by spam, and periodic manual review of putative spam is still necessary to minimize the risk of deleting legitimate messages. *See id.* (discussing the Hotmail inbox filter which places e-mail addressed to the user in the "BCC" header into a bulk mail folder for the user to sort through).

[98] Brightmail now offers such a service to individuals at no charge. *See* Brightmail, *Free Brightmail, at* http://www.brightmail.com/individual/ (last visited Aug. 8, 2000).

gies is that they are more likely to stop spam before it even reaches the end user's e-mail inbox. More importantly, the collaborative filtering employed by these approaches can be much more effective than individual filtering since it permits identification of multiple identical copies of a message that otherwise might not be obvious as spam, except to human eyes.[99] However, collaborative filtering introduces other potential inefficiencies into the system, such as requiring circuitous routing, examination of messages, and a high level of trust in the ISP or third-party proxy service that is given access to the client's e-mail.

Even when performed by a destination operator rather than by end users, filtering is still an inefficient solution since the destination operator and intermediate networks still must devote bandwidth and storage capacity to receiving the message. It would be more efficient if the destination operator could refuse delivery of spam altogether or, better yet, if the spam could be prevented from reaching the destination operator in the first place.[100]

3. Blocking Spam

Several technological measures have been developed to enable destination operators to refuse delivery of spam. Many databases, sometimes referred to as blacklists or "blackhole lists," list Internet hosts frequented by spammers.[101] Destination operators can use these

[99] Brightmail, for example, plants decoy e-mail addresses in various places on the Internet to be "harvested" unwittingly by spammers. The company's spam-filtering rules are based largely on messages received at these decoy addresses. *See* Paul Festa, *Are New Yahoo, Hotmail Spam Filters Better Than Past Efforts?*, CNET NEWS.COM, Dec. 8, 1999, *at* http://news.cnet.com/category/0-1005-200-1488576.html. The Spam Recycling Center collects spam specimens submitted by individuals and forwards them to government officials and spam-filter developers. *See Spam Recycling Center*, *at* http://chooseyourmail.com/spamindex.cfm (last visited Nov. 10, 2000).

[100] These approaches are similar to refusing delivery of a certified letter based upon its return address (although perhaps a C.O.D. package would be a closer analogy) or instructing the postal service not to deliver any mail from a particular source. Because Internet e-mail is not routed through a central agency (unlike postal mail), there generally is no choke point at which e-mail can be stopped between the origination and destination networks. However, many efforts at stopping spam represent attempts to prevent messages from leaving the origination network in the first place. For the most part, these efforts fall within the categories of informal and legal responses, although some Internet service providers have implemented a partial technical solution by limiting outbound SMTP traffic. *See infra* note 109 (discussing port 25 blocking and redirection).

[101] The term "blackholing" means denying delivery of any e-mail, or other data, coming from a certain Internet host, without returning a bounce message. The destination operator blocks the data coming from the blacklisted ISP and the data disappears without a trace, falling into a "blackhole." *See Jargon 4.2*, *at* http://www.science.uva.nl/~mes/jargon/b/blackhole.html (last visited Jan. 27, 2001) (defining "blackhole"); *see supra* note 61 (defining "bounce message").

databases to identify and refuse delivery of selected incoming messages.[102] The best known such database, the Mail Abuse Prevention System's Realtime Blackhole List ("RBL"),[103] includes open relays,[104] as well as other sites that are deemed "friendly, or at least neutral, to spammers."[105] About one-third of all destination operators reportedly subscribe to the RBL.[106] Similar databases include the Relay Spam Stopper,[107] the Open Relay Behaviour-modification System,[108] the Dial-up User List,[109] and the Spamhaus Project.[110] A

[102] *See, e.g.*, Paul Festa, *Hotmail Uses Controversial Filter to Fight Spam*, CNET NEWS.COM, Nov. 9, 1999, *at* http://news.cnet.com/news/0-1005-200-1433577.html. Destination operators can choose how to use these lists—for example, some sites accept messages from listed hosts but filter them into a folder containing suspected spam, while others may refuse connectivity for both incoming and outgoing e-mail traffic. *See, e.g., id.*; *Using ORBS to Protect Your E-mail*, *at* http://www.orbs.org/usingindex.html (last visited Aug. 8, 2000); Paul Vixie, *MAPS RBL Usage*, *at* http://www.mail-abuse.org/rbl/usage.html (last modified July 3, 2000).

[103] Mail Abuse Prevention Sys. LLC, *MAPS Realtime Blackhole List*, *at* http://www.mail-abuse.org/rbl/ (last modified Feb. 28, 2000).

[104] *See* discussion *supra* Part I.B.3 and accompanying notes (discussing third-party relaying).

[105] Paul Vixie & Nick Nicholas, *Getting into the MAPS RBL*, *at* http://www.mail-abuse.org/rbl/candidacy.html (last modified Feb. 2, 2000). There are a number of grounds on which a host may be added to the RBL, including operating an open mail relay, hosting web pages or e-mail drop boxes that are promoted in spam, and providing other services or software for use in spamming. *See id.*

[106] *See* Derek Scruggs & Heidi Anderson, *Sometimes the Messenger Should Be Shot: Building a Spam-Free E-mail Marketing Program*, at 8, *at* http://www.messagemedia.com/rc/spam.PDF (Dec. 3, 1999) (reporting that nearly a third of mail administrators subscribe to the RBL); Michelle Finley, *Other Ways to Fry Spam*, WIRED NEWS, Apr. 24, 2000 (quoting claim by SpamCop operator Julian Haight that 30% to 40% of mail servers participate in the RBL), *at* http://www.wired.com/news/culture/0,1284,35776-2,00.html; Nick Wingfield, *MAPS Can Be a Roadblock to E-Mail Access*, WALL ST. J., Aug. 3, 2000, at B5 (citing claim by MAPS project manager that "MAPS's subscribers control upward of 40% of the e-mail accounts on the Internet").

[107] Mail Abuse Prevention Sys. LLC, *MAPS Relay Spam Stopper*, *at* http://www.mail-abuse.org/rss/ (last modified Aug. 1, 2000).

[108] *Open-Relay Behaviour-modification System*, *at* http://www.orbs.org/ (last visited Aug. 8, 2000).

[109] Mail Abuse Prevention Sys. LLC, *MAPS Dial-up User List*, *at* http://www.mail-abuse.org/dul/ (last modified Aug. 1, 2000). Unlike most of the other databases mentioned here, the Dial-up User List contains Internet Protocol ("IP") addresses normally assigned to personal computers when they connect to the Internet by dialing into an ISP. Internet users with dial-up access normally send e-mail by configuring their client software to use their ISP's SMTP server, while a spammer may be more likely to bypass its ISP's server. *See* discussion *supra* note 18. Some ISPs have responded to this technique by blocking outbound traffic on port 25 (the port used to send e-mail via SMTP), or by redirecting such traffic to their own SMTP servers. *See* Mail Abuse Prevention Sys. LLC, *MAPS DUL Response to BYTE Column by Jason and Ted Coombs*, *at* http://mail-abuse.org/dul/0405coombs-response.htm (last modified July 31, 1999); *cf.* Scott Bradner, *Blocking Data for a Good Cause*, NETWORK WORLD, June 7, 1999, 1999 WL

separate blacklist, Spam Whack!,[111] helps ISPs identify potential subscribers who have been terminated by other ISPs for spamming.[112] The operators of the RBL and similar databases have been threatened with lawsuits, though they appear eager to defend their activities in court.[113] While it is difficult to argue that an individual company should not have the right to block spam,[114] persuasive arguments can be raised concerning widely used databases like the RBL.[115]

Unfortunately, none of the filtering and blocking technologies are perfect: most of them cost money to implement on a widespread basis, interfere with some legitimate message traffic, allow some spam through, and fail to eliminate many of the costs imposed by spam. Advances in filtering and blocking technology thus far seem to have

11619858 (recommending that ISPs remove such restrictions from subscriber accounts after a probationary period).

[110] *The Spamhaus Project*, *at* http://www.spamhaus.org/ (last visited Aug. 8, 2000). The Spamhaus blacklists focus on ISPs that host support services used by spammers.

[111] *Spam Whack!*, *at* http://www.spamwhack.com/ (last visited Aug. 8, 2000).

[112] *See id*.

[113] *See* Paul Vixie & Nick Nicholas, *How to Sue MAPS*, *at* http://mail-abuse.org/lawsuit/ (last modified Feb. 29, 2000). MAPS was actually named as a defendant in two lawsuits filed in July 2000—a suit brought by opt-in e-mail marketer YesMail.com was quickly settled, with MAPS agreeing not to add YesMail.com to the RBL, while MAPS was named as a co-defendant along with AOL and other ISPs that subscribe to the RBL in a similar case brought by pollster Harris Interactive. *See* Wingfield, *supra* note 106, at B5 (discussing Harris Interactive Inc. v. Am. Online, Inc., No. 00-CV-6364LF (W.D.N.Y. filed July 31, 2000)); Jessica Madore Fitch, *E-Mail Marketer Fights "Spam" Label*, CHI. SUN-TIMES, July 25, 2000, 2000 WL 6686599 (discussing the case brought by YesMail); Laurie J. Flynn, *Harris Files Suit Against AOL over Blocking of E-Mail*, N.Y. TIMES, Aug. 3, 2000, *available at* http://www.nytimes.com/library/tech/00/08/biztech/articles/03spam.html.

[114] Many companies have asserted this right to block incoming spam. *See, e.g.*, Intel Corp. v. Hamidi, No. 98AS05067, 1999 WL 450944, at *3 (Cal. Super. Ct. Apr. 28, 1999) (enjoining defendant from sending bulk messages protesting plaintiff's employment practices into plaintiff's e-mail system), *appeal filed*, No. C033076 (Cal. Ct. App. Jan. 18, 2000); Am. Online, Inc. v. GreatDeals.Net, 49 F. Supp. 2d 851 (E.D. Va. 1999); CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015 (S.D. Ohio 1997); Cyber Promotions, Inc. v. Am. Online, Inc., 948 F. Supp. 456 (E.D. Pa. 1996); Cyber Promotions, Inc. v. Am. Online, Inc., 948 F. Supp. 436 (E.D. Pa. 1996). *But see* Hartford House, Ltd. v. Microsoft Corp., No. CV778550 (Cal. Super. Ct. Feb. 24, 1999) (order modifying preliminary injunction) (enjoining Microsoft from incorporating junk mail filters into its Outlook e-mail programs that filter or block plaintiff's electronic greeting cards), http://www1.bluemountain.com/home/order021899.html; Microsoft, *Microsoft to Remove Popular Filtering Feature From Outlook Express In Light of California Court Order*, *at* http://www.microsoft.com/PressPass/bluemt/bluemtnpr.asp (Feb. 24, 2000).

[115] *See, e.g.*, David A. Gottardo, Comment, *Commercialism and the Downfall of Internet Self Governance: An Application of Antitrust Law*, 16 J. MARSHALL J. COMPUTER & INFO. L. 125 (1997); Lessig, *Law of the Horse*, *supra* note 8, at 546 (describing blacklisting as "a form of vigilanteism"); Krause, *supra* note 50; Lessig, *Spam*, *supra* note 50.

been matched by advances by spammers in circumventing such measures.

B. Hiding from Spammers

Just as an unlisted telephone number can help reduce the number of telemarketing solicitations that one receives, Internet users can reduce the amount of spam that they receive by making it harder for spammers to learn their e-mail addresses. It is also possible to request that a spammer remove a particular e-mail address from its list, although this approach tends to be ineffective and even counterproductive.[116]

Address concealment has become an increasingly common practice, largely because of spam.[117] Spammers frequently compile mailing lists by "harvesting" e-mail addresses from web pages, Usenet newsgroups, chat rooms, and public directories and profiles available on services like America Online.[118] Individuals who post to newsgroups and those whose addresses appear on web pages tend to receive more spam as a result.[119]

Hiding one's e-mail address from spammers can be an effective way to reduce spam, but it is impractical for Internet users who want to remain open to other communications, both solicited and unsolicited. Some people include anti-spam statements in places where they post their e-mail addresses in an effort to warn off spammers,[120] though it seems unlikely that such statements would even be noticed by automated harvesting techniques. A more common technique is to disguise, or "munge,"[121] one's address—for example, by inserting "nospam" or other characters—so that the correct address can be determined by other individuals, but not by address-harvesting

[116] *See* SCHWARTZ & GARFINKEL, *supra* note 2, at 99.

[117] *See generally id.* at 66–74 (discussing how users can hide their e-mail addresses from spammers).

[118] *See* SCHWARTZ & GARFINKEL, *supra* note 2, at 66; Cranor & LaMacchia, *supra* note 9, at 75.

[119] *See* Cranor & LaMacchia, *supra* note 9, at 77.

[120] *See, e.g.*, *Emailing Leaf*, *at* http://www.gweep.net/~leaf/nospam.html (last modified July 13, 2000). *But see* Michael Roeder, *Spam Offer by Michael Roeder to Senders of Uninvited Email Solicitations*, *at* http://www.infernosoft.com/spamoff.shtml (last modified May 26, 2000) (offering to receive e-mail solicitations for $10 per message); Nima Taradji, *Notice of Offer to Receive Unsolicited Advertising (Spam)*, *at* http://www.taradji.com/spam.html (last modified June 3, 1999) (offering to receive e-mail solicitations for $500 per message).

[121] *See* W.D. Baseley, *Address Munging FAQ: Spam-Blocking Your Email Address*, *at* http://members.aol.com/emailfaq/mungfaq.html (last modified Aug. 8, 1999); *Jargon 4.2*, *at* http://www.science.uva.nl/~mes/jargon/s/spamblock.html (last visited Dec. 28, 2000) (defining "spamblock").

software.[122] Internet users can also maintain multiple e-mail accounts[123] and use web-based response services[124] as methods of concealing their e-mail addresses from spammers, while still providing other people with a means of contacting them.[125]

[122] *See* SCHWARTZ & GARFINKEL, *supra* note 2, at 69–70; Baseley, *supra* note 121.

[123] Free e-mail services such as Hotmail are frequently used to obtain secondary or even disposable addresses, both by individuals who want to avoid spam and by spammers themselves. *See* SCHWARTZ & GARFINKEL, *supra* note 2, at 67, 118. There are even services that offer e-mail addresses containing phrases such as "do-not-spam" and "suespammers." *See, e.g., Do-Not-Spam.com*, *at* http://do-not-spam.com/ (last visited Aug. 8, 2000); Tom Geller, *Suespammers.org E-Mail Accounts*, *at* http://www.suespammers.org/pop3/ (last visited Aug. 8, 2000).

Multiple e-mail accounts can also be used in tandem to help filter spam from legitimate e-mail messages. *See, e.g.*, Brightmail, *Free Brightmail*, *at* http://www.brightmail.com/individual/ (last visited Aug. 8, 2000); *MsgTo.com*, *at* http://www.msgto.com/ (last visited Aug. 8, 2000). The approach taken by MsgTo.com is particularly interesting: The first time that someone attempts to send e-mail to a MsgTo.com user, the service responds by asking the sender to pass a simple test by clicking on a specified word within an image before letting the message through. *See* MsgTo.com, *How It Works*, *at* http://www.msgto.com/works.htm (last visited Aug. 8, 2000). MsgTo.com has since suspended its service. *See* MsgTo.com, *Au Revoir*, *at* http://www.msgto.com/ (last visited Nov. 17, 2000).

[124] Freedback.com and Response-O-Matic are among several services that offer feedback forms that people can place on their web pages. A web page visitor who fills out and submits the form will cause a single e-mail message to be sent to the web page owner. *See Freedback.com*, *at* http://www.freedback.com (last visited Aug. 8, 2000); *Response-O-Matic*, *at* http://www.response-o-matic.com/ (last visited Aug. 8, 2000). With these and some other feedback forms, the web page owner's e-mail address must be included in the web page HTML code—and thus remains vulnerable to harvesting. A similar service, FormMail.To/You!, addresses this concern by maintaining a database containing each registered user's e-mail address rather than requiring that it be embedded in the feedback form. *See FormMail.To/You!*, *at* http://formmail.to (last visited Aug. 8, 2000).

[125] Another measure that has been used to combat address harvesting is the posting of web pages containing very long lists of bogus e-mail addresses (or e-mail addresses of spammers, government officials, or both), intended to frustrate harvesters by filling their lists with invalid or non-responsive addresses. *See* SCHWARTZ & GARFINKEL, *supra* note 2, at 73; *see, e.g.*, Christopher B. Browne, *Spam Bait*, *at* http://www.ntlug.org/~cbbrowne/commspambait.html (last visited Aug. 8, 2000); Ian Chadwick, *Spam Bot Trap/Bait Page*, *at* http://www.georgian.net/rally/trap.html (last visited Aug. 8, 2000); E-Scrub Technologies, *Wpoison Web Poisoning Tool*, *at* http://www.monkeys.com/wpoison/ (last visited Nov. 10, 2000); David Harper & Lynne Marie Stockman, *Welcome, Hungry Spambots!*, *at* http://www.obliquity.com/computer/spambait/ (last modified July 13, 2000); Greg Sabino Mullane, *Spambot Beware*, *at* http://www.turnstep.com/Spambot/ (last modified Dec. 19, 1999); Chip Rosenthal, *Spambait*, *at* http://www.unicom.com/spambait/ (last modified July 3, 2000). However, some harvesting software apparently can recognize these pages, *see, e.g.*, Microsys Technologies, Inc., *Atomic Harvester 2000: Professional Email Address Harvesting for Windows 98*, *at* http://www.emailtools.com/products/ah2000/ (last visited Aug. 8, 2000), and, in any event, the negligible incremental cost of sending e-mail makes this technique unlikely to have a significant impact.

C. Opting Out

Once spammers obtain an e-mail address and begin sending messages to it, however, it is much more difficult to stem the tide of spam. Some people reply to spam with an "opt-out" request, asking the sender not to send any further messages and to remove the person's e-mail address from its mailing list. Unsolicited commercial e-mail messages commonly include opt-out instructions, including an e-mail address or web page's uniform resource locator ("URL") for use in submitting such requests. Such e-mail addresses and URLs often are invalid, or become so once the spam is reported, and the spammer's service provider discontinues its service.[126]

Opting out is relatively effective in other forms of direct marketing, namely direct mail solicitation and outbound telemarketing, at least with respect to each marketer to which an opt-out request is submitted.[127] In direct mail and telemarketing, the incremental cost of each communication provides marketers with a sufficient incentive to refrain from communication with persons who have submitted opt-out requests.[128] Bulk e-mail, however, does not involve an analogous incremental cost, and spammers, therefore, lack a similar incentive to respect opt-out requests.[129] Furthermore, many experts advise Internet users not to submit opt-out requests since they are rarely effective and

[126] The Direct E-Mail Advertisers Association, which appears to be a trade organization representing companies that send unsolicited commercial e-mail, makes the rather ironic claim that such service terminations are counterproductive since they make it more difficult for recipients to be removed from mailing lists. *See* Direct E-Mail Advertisers Ass'n, *The Comparison: UCE vs. Spam!*, *at* http://www.deaa.org/uce_vs__spam.shtml (last visited Aug. 8, 2000).

[127] *See* Sorkin, *supra* note 36, at 1029.

[128] Postage, materials, and labor costs all contribute to the significant incremental costs of direct mail and telemarketing solicitations; a marketer might well save as much as one dollar or more by eliminating a name from its list. Furthermore, the legal consequences of continuing to communicate with an individual who has sought to discontinue receiving solicitations are also likely to influence a direct mailer or telemarketer's actions. *See, e.g.*, Rowan v. United States, 397 U.S. 728, 735–36, 739 n.6 (1970) (interpreting prohibitory order statute as conferring unfettered, unreviewable discretion upon the addressee to determine what advertisements qualify as pandering); 39 U.S.C. § 3008 (1994) (requiring postal service to issue prohibitory order to mailer upon addressee's request, following receipt of "pandering advertisement," and requiring mailer to purge addressee's name from its mailing lists); 16 C.F.R. § 310.4(b) (1999) (requiring telemarketers to honor "do-not-call" requests); 47 C.F.R. § 64.1200(e)(vi) (1999) (same).

[129] The effort required to remove an address from a spammer's list is likely to exceed any negligible savings that would result from sending a bulk e-mail message to one fewer address. Furthermore, a spammer typically must violate several providers' policies by sending the spam in the first place, so it makes sense that spammers would be less likely than other marketers to be concerned with social or legal consequences of ignoring opt-out requests.

some spammers reportedly collect and sell e-mail addresses of those who have submitted such requests.[130] Finally, sender-specific opt-out is problematic in the case of e-mail because the sheer number of potential spammers far exceeds the number of direct marketers using other communication methods.[131] For these reasons, sender-specific opt-out represents a singularly ineffective method of curbing spam.

A universal opt-out system would require spammers to use a single "global remove" list to filter addresses from their mailing lists.[132] There have been several attempts to develop such a system, but nearly all have failed miserably,[133] and the prospect of creating a true univer-

[130] *See* SCHWARTZ & GARFINKEL, *supra* note 2, at 74. Individuals who have submitted opt-out requests may not seem like particularly good prospects for a subsequent solicitation. However, the fact that they have responded to a spam confirms their addresses to be valid, and indicates that they are probably more likely to actually read unsolicited e-mail, that they probably receive less of it than many other users, and that they may be relatively unsophisticated Internet users and, therefore, more susceptible to questionable solicitations.

[131] The ephemeral nature of identity on the Internet effectively gives each spammer an unlimited stock of separate identities, some of which may exist only at the point in time that a particular solicitation is being sent, and as already noted, spammers have little or no incentive to honor opt-out requests. Unsolicited e-mail messages frequently contain statements representing that they are a one-time mailing and promising never to contact the recipient again, often as an justification for not providing opt-out instructions, and the spammer naturally will send its next message out under a different name. For these reasons, even if there were very few separate entities engaged in spamming, contacting a significant proportion of spammers is likely to be much more difficult than contacting a comparable proportion of direct mailers or telemarketers.

[132] Both caller-specific and universal opt-out systems have been implemented by laws that govern telemarketing. Under federal law, each company that engages in telemarketing activities must maintain a "do-not-call" list. *See, e.g.*, 47 C.F.R. § 64.1200(e)(vi) (1999). A few states prohibit telemarketers from calling persons who are listed in a central "do-not-call" registry, sometimes called "black dot" or "asterisk" laws. *See, e.g.*, ALASKA STAT. § 45.50.475(b), (c) (Michie 1998); ARK. CODE ANN. §§ 4-99-404 to -405 (Michie Supp. 1999); FLA. STAT. ANN. § 501.059(3), (4) (West Supp. 2000); GA. CODE ANN. § 46-5-27(d), (e) (Supp. 2000); KY. REV. STAT. ANN. § 367.46955(15) (Banks-Baldwin 1999); Act of July 8, 1999, ch. 564, § 1, 1999 Or. Laws 1317, 1317 (to be codified at OR. REV. STAT. § 646.569).

[133] In some instances, spammers have reportedly operated opt-out services as a tactic to obtain additional e-mail addresses; in other cases, apparently good-faith attempts to create universal exclusion lists have been terminated by their operators because spammers referred to the lists in their messages and used them to justify the practice of spamming. *See* SCHWARTZ & GARFINKEL, *supra* note 2, at 74; *Tactical Net Abuse FAQ, ver. 1.4*, *at* http://members.aol.com/macabrus/tacticalfaq.html (last modified Jan. 19, 1998) (describing universal remove lists as "[t]he oldest trick in the spammer's handbook"); Do-Not-Spam.com, *Global Remove*, *at* http://do-not-spam.com/remove.htm (last visited Aug. 8, 2000) (explaining temporary removal of removal service "as it has been falsely and maliciously used against our wishes in unsolicited advertising via e-mail"). One service even charges individuals a fee to be included in its "remove" database. *See NoThankYou.com*, *at* http://www.nothankyou.com/ (last visited Aug. 8, 2000).

sal list raises significant administrative and privacy concerns.[134] Even if such a list could be constructed, it would be unlikely to have a significant effect on spam unless spammers were legally compelled to use it.

D. Reporting and Retaliation

Another category of technical responses involves complaints and other retaliatory actions directed at spammers by spam recipients.[135] An Internet user who receives spam with a bogus reply address may be sufficiently incensed to trace the message and complain to the spammer's service provider, the user's own ISP, and elsewhere.[136] Such complaints may be motivated by revenge or a desire to vent frustra-

Two recent attempts at universal opt-out systems have fared somewhat better, but neither appears likely to have a significant effect on spam. The first, SAFEeps, went online in 1998 and quickly grew to include millions of e-mail addresses—in large part because it permitted services like America Online and Hotmail to opt-out all of their subscribers' addresses—but apparently is rarely used by spammers to filter their mailing lists. *See SAFEeps*, *at* http://www.safeeps.com/ (last visited Aug. 8, 2000); Andrew Leonard, *The War for Your E-Mail Box*, SALON, Oct. 30, 1998, *at* http://www.salon.com/21st/feature/1998/10/cov_30feature.html; Deborah Scoblionkov, *Direct Mail Double-Cross?*, SALON, Nov. 12, 1999, *at* http://www.salon.com/tech/feature/1999/11/12/spam/. In 1998, the Direct Marketing Association promised to create a universal opt-out system and the operator of SAFEeps offered to license that system to the DMA for $1. *See* Nick Nicholas, *DMA to Internet: Shut Up and Eat Your Spam*, *at* http://www.mail-abuse.org/anti-dma.html (last modified Feb. 28, 2000). The DMA declined this offer, apparently because of hostility to the concept of domain-wide opt-out. *See id.* Instead, it developed its own system, e-MPS, which went online in 2000. *See* Direct Mktg. Ass'n, *e-Mail Preference Service*, *at* http://www.e-mps.org/ (last visited Aug. 8, 2000). The DMA requires its members to filter their spam mailing lists using e-MPS and permits other spammers to do so for a fee. *See id.*

[134] Furthermore, since nearly all Internet users would prefer not to receive an unlimited amount of spam and nearly all destination operators have policies that prohibit spam from being sent to their subscribers, and, therefore, possibly *requiring* their subscribers to opt out, it would seem much more efficient to construct an *opt-in* list comprised of a few dozen addresses than an *opt-out* list comprised of nearly all Internet users. To a lesser extent, the same could be said for telemarketing, although there probably is a much larger proportion of the public that enjoys receiving telemarketing calls. For example, those who like talking to strangers on the telephone and those who enjoy dispensing verbal abuse. Also, the volume of telemarketing calls that a person is likely to receive is significantly constrained by economic factors, unlike the volume of spam.

[135] In some instances destination operators have also engaged in retaliatory tactics. *See, e.g.*, Cyber Promotions, Inc. v. Am. Online, Inc., 948 F. Supp. 436, 437 & n.1 (E.D. Pa. 1996). But these appear to be much less common than acts of retaliation by individual recipients.

[136] *See* Phil Agre, *How to Complain About Spam, or, Put a Spammer in the Slammer*, *at* http://dlis.gseis.ucla.edu/people/pagre/spam.html (Dec. 1997); Jim Kingdon, *How to Complain to the Spammer's Provider*, *at* http://spam.abuse.net/spam/howtocomplain.html (last visited Aug. 8, 2000). Axel Boldt's *Blacklist of Internet Advertisers* cites to several public fora in which spammers are vilified. *See* Boldt, *supra* note 79.

tion, but they can help alleviate the spam problem by imposing costs upon spammers and threatening their Internet connectivity.

Frequently, however, tracing spam can be quite difficult; in addition to forging message headers, spammers omit other contact information such as telephone numbers and physical addresses.[137] They may invite recipients to access a web site, usually one that is hosted by a spam-friendly provider, or may solicit responses only by means designed to discourage or screen complaints, such as a "bulletproof" voice mail number.[138]

Internet users can choose from several services and tools designed to assist them in tracing and reporting spam. Sam Spade, for example, is a collection of utilities that can help users decipher addresses and related information contained in e-mail messages.[139] A web-based service called SpamCop automatically parses message headers and generates complaint messages to appropriate parties on the user's behalf.[140]

Retaliation can go far beyond merely the complaint stage. Spammers and their service providers have been subjected to flames,[141] reputation attacks, invasions of privacy, e-mail bombs and other denial-of-service attacks, and even threats of violence and property damage.[142] Such extreme retaliatory acts may well be somewhat effective in deterring spam, but they obviously have problems of their own.

[137] *See generally* SCHWARTZ & GARFINKEL, *supra* note 2, at 86–99.

[138] One such service, for example, advertises that it identifies the telephone number of each caller and can limit the number of calls accepted from each number, presumably in order to control the usage charges incurred in receiving complaints about spam. *See* Freedomstarr Communications Inc., *Bulletproof! 800/888# Voicemail Instructions and FAQ*, *at* http://www.voicemail.org/faq.html (last visited Aug. 8, 2000).

[139] *See* Steve Atkins, *Sam Spade*, *at* http://www.samspade.org/ (last visited Aug. 8, 2000); Bill Machrone, *Digital Sam Spade Takes on the Spam Gang*, PC WK., June 15, 1998, http://www.zdnet.com/pcweek/opinion/0615/15mach.html. Ultradesign Xperimental Network, *UXN Spam Combat*, *at* http://combat.uxn.com/ (last visited Aug. 8, 2000) is a similar set of utilities.

[140] *See* Julian Haight, *SpamCop*, *at* http://spamcop.net/ (last visited Aug. 8, 2000).

[141] *See* Denis Howe ed., *Free On-Line Dictionary of Computing*, *at* http://foldoc.doc.ic.ac.uk/foldoc/foldoc.cgi?flame (last modified May 27, 1998) (defining "flame" as "[a]n electronic mail or Usenet news message intended to insult, provoke or rebuke, or the act of sending such a message" or "[t]o speak incessantly and/or rabidly on some relatively uninteresting subject or with a patently ridiculous attitude or with hostility towards a particular person or group of people").

[142] *See, e.g.*, SCHWARTZ & GARFINKEL, *supra* note 2, at 26 (discussing "Anti-Spam Vigilantes"); Michael Castelluccio, *Spam and Cheese?*, MGMT. ACCT., Feb. 1999, at 82 (noting that "vigilantes have published the names, voicemail numbers, home addresses, and social security numbers of spammers"); Amy Harmon, *The American Way of Spam*, N.Y. TIMES, May 7, 1998, at G1; Agre, *supra* note 136.

E. Limitations of Technical Approaches

While technological measures are the most flexible approach to spam, spammers have consistently succeeded in adapting their techniques to circumvent advances in anti-spam technology. Technical approaches are unlikely ever to eradicate spam, partly because of the time and resources that spammers devote to their activities (and the economies of scale from which they benefit) and partly because of the inherent openness of the Internet and e-mail protocols.[143]

Another problem with technical approaches is the deleterious effects that they can have on legitimate communications. Blocking e-mail traffic from a spam-friendly site often means blocking a great deal of legitimate e-mail, for example. Closing down an open relay that has been used for sending spam as well as for legitimate purposes can be inconvenient for many users.

The costs of implementing technical mechanisms is also of great concern.[144] Spamming is profitable only because spammers are almost entirely unaffected by these substantial costs.

Finally, technical approaches have been criticized for a lack of transparency and accountability. Blacklist maintainers, for example, need not disclose the criteria they use nor afford due process to accused spammers. The market does provide a check on such activity, but incomplete information, complexity of the issues, and concentration of market power[145] all affect the extent to which blacklists and other anti-spam measures are likely to be held accountable.

IV. Legal Approaches

Many lawsuits involving unsolicited e-mail have been filed in recent years, and a number of them have been successful.[146] Most of the cases brought to date, however, involve instances of what might be considered "aggravated" spamming—sending messages with forged headers, unauthorized third-party relaying, and persistent refusals to comply with opt-out demands—and nearly all involve commercial

[143] This openness is frequently desirable—for example, relatively few Internet users are interested in receiving e-mail only from persons they have designated in advance, and there are legitimate and important applications for anonymous electronic communications.

[144] *See* sources cited *supra* note 48 (discussing the costs imposed by spam).

[145] *But see* Cyber Promotions, Inc. v. Am. Online, Inc., 948 F. Supp. 456, 464 (E.D. Pa. 1996) (holding that AOL is not likely to be proven an "essential facility" despite its substantial market share).

[146] *See* discussion *infra* Part IV.A.

messages.[147] It stands to reason that more extreme forms of spam are more likely to lead to litigation, but the resulting cases have done little to clarify the legal status of "pure" spam.

Meanwhile, legislatures have been busy considering a variety of legislative approaches to controlling spam, at both state and federal levels. Several spam-related bills have been introduced in the United States Congress,[148] and many states have already enacted spam legislation,[149] including, in at least one instance, a virtual ban on unsolicited bulk commercial e-mail messages.[150] The European Union and other countries have also considered enacting anti-spam legislation.[151]

A. Litigation

The first spam-related lawsuit was a small claims case filed by Robert Arkow against CompuServe in early 1995.[152] Arkow had received unsolicited e-mail advertisements from CompuServe.[153] He argued that the federal law prohibiting unsolicited facsimile advertisements[154] defined "facsimile machine" broadly enough to include computers that send and receive electronic mail.[155] The parties settled out of court and the terms were never disclosed.[156] Thus, the applicability of the law governing the use of facsimile machines to e-mail has never been formally adjudicated.[157]

[147] *See id*.

[148] *See* discussion *infra* Part IV.B.

[149] *See id*.

[150] *See* Act of July 2, 1999, ch. 135, § 1, 72 Del. Laws 7, 7 (1999) (to be codified at DEL. CODE tit. 11, § 937(a)).

[151] *See* discussion of European legislation *infra* Part IV.B and accompanying notes.

[152] *See* Sorkin, *supra* note 36, at 1002 n.12; Bruce V. Bigelow, *Infuriated Client Sues Over Junk E-mail*, SAN DIEGO SUN TRIB., Feb. 19, 1995, LEXIS, San Diego Sun Tribune News File; Mark Eckenwiler, *Just the Fax, Ma'am*, *at* http://www.panix.com/~eck/junkmail.html (Mar. 1996) (discussing Arkow's suit against CompuServe filed Feb. 1995).

[153] *See* Bigelow, *supra* note 152.

[154] Telephone Consumer Protection Act, 47 U.S.C. § 227 (1994).

[155] *See* Eckenwiler, *supra* note 152.

[156] *See* Sorkin, *supra* note 36, at 1002 n.12.

[157] *See* Eric J. Sinrod & Barak D. Jolish, *Controlling Chaos: The Emerging Law of Privacy and Speech in Cyberspace*, 1999 STAN. TECH. L. REV. 1, 15 n.102 *at* http://stlr.stanford.edu/STLR/Articles/99_STLR_1/article_pdf.pdf. *See generally* Sorkin, *supra* note 36, at 1032 (concluding that the Telephone Consumer Protection Act is not likely to be construed to cover e-mail advertisements). The issue has been raised in other cases, but apparently has yet to be addressed on its merits. *See, e.g.*, ErieNet, Inc. v. Velocity Net, Inc., 156 F.3d 513, 520 (3d Cir. 1998) (dismissed for lack of jurisdiction); Seidl v. Greentree Mortgage Co., 30 F. Supp. 2d 1292, 1298 (D. Colo. 1998) (claim brought but not discussed by the court); Snow v. Doherty, No. 3:97-CV-0635 (RM) (N.D. Ind. filed Sept. 22, 1997) (case dismissed without prejudice for the inability to obtain a

There have been relatively few spam-related suits involving individual recipients of spam since *Arkow v. CompuServe*.[158] Most spam litigation has been brought by ISPs and other destination operators that have received large quantities of spam addressed to their users, or by third parties whose names or resources have been appropriated by spammers.[159]

valid address for service of process); *Docket History*, *at* http://mama.indstate.edu/users/dougie/docket.txt (last visited Jan. 25, 2001).

[158] The dearth of individual actions is probably attributable in part to the relatively small damages that would likely be available, together with the difficulty in proving actual damages. ISPs are often in a better position than end users to demonstrate substantial damages. America Online, for example, apparently attributes $0.00078 in equipment costs to each incoming e-mail message by pro rating its overall investment in e-mail hardware, enabling the company to quantify at least part of the costs it sustains when spammers send millions of messages to AOL subscribers. *See, e.g.*, Am. Online, Inc. v. Prime Data Sys. Inc., No. 97-1652-A, 1998 U.S. Dist. LEXIS 20226, at *4, *9 (E.D. Va. Nov. 20, 1998); Am. Online, Inc. v. Christian Bros., No. 98 Civ. 8959 (DAB) (HBP), (S.D.N.Y. Dec. 9, 1999), at 17 (report and recommendation of magistrate judge), http://legal.web.aol.com/decisions/dljunk/CHRIST~1.pdf; Am. Online, Inc. v. CN Prods., Inc., No. 98-552-A (E.D. Va. Feb. 10, 1999) (order granting judgment and permanent injunction in favor of plaintiff), http://legal.web.aol.com/decisions/dljunk/cnpmemo.html [hereinafter CN Order]; Am. Online, Inc. v. IMS, No. 98-0011-A (E.D. Va. Nov. 20, 1998) (report and recommendation of magistrate judge), http://legal.web.aol.com/decisions/dljunk/imsreport.html. Also, since end users can reduce their spam intake merely by changing providers and often blame their own provider for the spam that they receive, ISPs have an additional incentive to take on spammers. *See generally* Gartner Group, *supra* note 11, at 8.

Interestingly, while few of the United States spam-related cases have been brought by individual recipients, there have been several cases brought by recipients of spam in Germany, most of which have been successful. *See, e.g.*, OLGZ 16, 320 (reporting an Oct. 13, 1998 decision of the Berlin Landgericht (Regional Court)), http://www.online-recht.de/vorent.html?LGBerlin981013; OLGZ 16, 301 (reporting a May 14, 1998 decision of the Berlin Landgericht), http://www.online-recht.de/vorent.html?LGBerlin980514; OLGZ 16, 201 (reporting an Apr. 2, 1998 decision of the Berlin Landgericht), http://www.online-recht.de/vorent.html?LGBerlin980402; CLGZ 7, 748 (reporting a Feb. 11, 1998 decision of the Brakel Amtsgericht (District Court, similar to a Magistrate)), http://www.online-recht.de/vorent.html?AGBrakel980211; HKO 2, 3755 (reporting an Oct. 14, 1997 resolution of the Traunstein Landgericht), http://www.online-recht.de/vorent.html?LGTraunstein971014; *cf*. CLGZ 1110, 243 (reporting a Sept. 30, 1999 decision of the Kiel Amtsgericht which dismissed plaintiff's case since the offending communication was not spam), http://www.online-recht.de/vorent.html?AGKiel990930.

[159] *See infra* Parts IV.A.1–4. In addition to the types of cases discussed in this Section, there have been a number of cases involving claims related to the content of unsolicited e-mail messages. *See, e.g.*, Curtis v. DiMaio, 46 F. Supp. 2d 206, 213 (E.D.N.Y. 1999) (discussing applicability of discrimination laws to racially or sexually offensive e-mail messages); People v. Lipsitz, 663 N.Y.S.2d 468, 468 (Sup. Ct. 1997) (applying consumer fraud and false advertising laws to unsolicited commercial e-mail); Securities Exchange Comm'n, *Litigation Release No. 15959*: *SEC Fines Internet Stock Promoter Responsible for Massive Spam Campaign*, *at* http://www.sec.gov/enforce/litigrel/lr15959.txt (Oct. 27, 1998) (discussing *SEC v. Tribble*, No. 98-8699 (RVX) (C.D. Cal. filed Oct. 27, 1998) in which securities laws where applied to spam containing investment recommendations without required disclosures); *see also* Securities Exchange Comm'n, *SEC Charges 44 Stock Promoters in First Internet Securities Fraud Sweep: Purveyors of Fraudulent Spam*, *Online Newsletters*,

1. Destination Operators

Destination operators have sued spammers using a number of different legal theories. Most common are claims based upon the spammer's unauthorized use of the destination operator's facilities, usually characterized as trespass to chattels or conversion. Trespass to chattels in particular has been alleged by destination operators in many spam cases;[160] conversion is less helpful since it requires a more substantial

Message Board Postings, and Websites Caught, *at* http://www.sec.gov/news/netfraud.htm (Oct. 28, 1998); authorities cited *supra* note 33 (discussing criminal prosecutions for sending racist threats by e-mail).

[160] *See, e.g.*, Am. Online, Inc. v. GreatDeals.Net, 49 F. Supp. 2d 851, 854 (E.D. Va. 1999); Am. Online, Inc. v. Prime Data Sys. Inc., No. 97-1652-A, 1998 U.S. Dist. LEXIS 20226, at *1 (E.D. Va. Nov. 20, 1998); Am. Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444, 451–52 (E.D. Va. 1998); Am. Online, Inc. v. IMS, 24 F. Supp. 2d 548, 550–51 (E.D. Va. 1998); Hotmail Corp. v. Van$ Money Pie Inc., 47 U.S.P.Q.2d (BNA) ¶ 1020 (N.D. Cal. Apr. 16, 1998); CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1020–23 (S.D. Ohio 1997); Intel Corp. v. Hamidi, No. 98AS05067, 1999 WL 450944, at *2 (Cal. Super. Ct. Apr. 28, 1999); Am. Online, Inc. v. Blue Card Publ'g, No. 98-905-A (E.D. Va. Jan. 5, 2000), at 6 (report and recommendation by magistrate judge), http://legal.web.aol.com/decisions/dljunk/bluecardreport.pdf [hereinafter Blue Card Report]; CN Order, *supra* note 158; Plaintiff's Complaint, Am. Online, Inc. v. Bliss (M.D. Fla. Dec. 1998) (No. 98-1397-Civ-Orl-19A), http://legal.web.aol.com/decisions/dljunk/blisscomplaint.html [hereinafter Bliss Complaint]; Plaintiff's Complaint, Am. Online, Inc. v. Christian Bros. (S.D.N.Y. Dec. 18, 1998) (No. 98 Civ. 8959(DAB)(HBP)), http://legal.web.aol.com/decisions/dljunk/christiancomp.html [hereinafter Christian Complaint]; Plaintiff's Complaint, Am. Online, Inc. v. Dayton (E.D. Va. Dec. 1998) (No. 98-1815-A), http://legal.web.aol.com/decisions/dljunk/daytoncomp.html [hereinafter Dayton Complaint]; Plaintiff's Complaint, Am. Online, Inc. v. Global Mktg. Solutions, Inc. (M.D. Fla. Dec. 1998), http://legal.web.aol.com/decisions/dljunk/global.html [hereinafter Global Complaint]; Plaintiff's Complaint, Am. Online, Inc. v. Nat'l Health Care Discount, Inc. (N.D. Iowa Dec. 1998), http://legal.web.aol.com/decisions/dljunk/national.html [hereinafter Nat'l Health Complaint]; Plaintiff's Complaint, Am. Online, Inc. v. Persaud (S.D. Cal. Dec. 1998) (No. 98-CY-2284 7W (LAB)), http://legal.web.aol.com/decisions/dljunk/persaudcomp.html [hereinafter Persaud Complaint]; Plaintiff's Complaint, Am. Online, Inc. v. USA Home Employment (C.D. Cal. Dec. 1998) (No. CV 98-10225 DDP (MANx)), http://legal.web.aol.com/decisions/dljunk/usacomp.html [hereinafter USA Home Complaint]; Plaintiff's Complaint, Am. Online, Inc. v. Wrhel (C.D. Cal. Dec. 1998), http://legal.web.aol.com/decisions/dljunk/wrhel.html [hereinafter Wrhel Complaint]; Earthlink Network Inc. v. Cyber Promotions, Inc., No. BC 167502 (Cal. Super. Ct. Mar. 30, 1998) (consent judgment and entry of judgment & stipulation), http://www.jmls.edu/cyber/cases/earth1.html [hereinafter Earthlink Judgment]; Plaintiff's Complaint, Am. Online, Inc. v. Web Communications (E.D. Va. Mar. 2, 1998) (No. 98-289-A), http://legal.web.aol.com/decisions/dljunk/webcommc.html [hereinafter Web Complaint]; Plaintiff's Complaint, Am. Online, Inc. v. Squeaky Clean Mktg. (Va. Cir. Ct. Dec. 18, 1997) (No. 152613), http://legal.web.aol.com/decisions/dljunk/squeakyc.html [hereinafter Squeaky Complaint]; Plaintiff's Complaint, Bigfoot Partners, L.P. v. Cyber Promotions, Inc. (S.D.N.Y. Oct. 6, 1997) (No. 97 CIV 7397), http://legal.web.aol.com/decisions/dljunk/bigfootc.html [hereinafter Bigfoot Complaint]; Plaintiff's Complaint, Am. Online, Inc. v. Over the Air Equip., Inc. (E.D. Va. Oct. 1997) (No. 97-1547-A), http://legal.web.aol.com/decisions/dljunk/oaecomp.html [hereinafter OAE Complaint];

interference with property rights.[161]

Trespass to chattels is committed when a person uses or intermeddles with another's personal property without authorization.[162] The trespasser is liable to the rightful possessor of the property if the property's value or condition is impaired, or if the possessor is deprived of its use for a substantial time.[163] Anyone, including a spammer, who sends e-mail messages to subscribers of an ISP or other destination operator necessarily makes use of the operator's SMTP server. However, routine use of an SMTP server for legitimate message traffic is implicitly authorized and rarely causes the damage necessary for liability. The trespass to chattels theory, therefore, seems best suited to cases in which the destination operator has previously communicated to the spammer that its use of the operator's facilities is not authorized and the spammer subsequently ignores the operator's demands, thereby causing damage to the operator's system.[164]

Destination operators have attempted to capture other costs inflicted by spam with claims such as unjust enrichment and misappropriation. For example, America Online ("AOL") has argued that spammers have misappropriated its infrastructure.[165] AOL collects advertising fees from marketers in exchange for placing their advertisements in its subscribers' screens.[166] Spammers are able to circumvent this process while still taking advantage of AOL's infrastructure to de-

Carl S. Kaplan, *Company Says Junk E-Mailer Stole Its Identity*, N.Y. TIMES CYBER L.J., Nov. 19, 1999, *at* http://www.nytimes.com/library/tech/99/11/cyber/cyberlaw/19law.html (discussing suit filed by Visto Corp. against a spammer); SimpleNet, *SimpleNet Awarded Judgment in "Spam" Lawsuit*, *at* http://www.jmls.edu/cyber/docs/simple1.html (Apr. 15, 1998) (discussing SimpleNet's suit against VNZ Info. & Entm't Servs.) [hereinafter SimpleNet Article].

[161] *See* CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. at 1022.

[162] *See* RESTATEMENT (SECOND) OF TORTS § 217(b) (1965).

[163] *See id.* § 218; *see also* Am. Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d at 451–52; Am. Online, Inc. v. IMS, 24 F. Supp. 2d at 550; CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. at 1021; Thrifty-Tel, Inc. v. Bezenek, 54 Cal. Rptr. 2d 468, 473 (Ct. App. 1996); Dan L. Burk, *The Trouble with Trespass*, 4 J. SMALL & EMERGING BUS. L. 27, 28 (2000).

[164] *See, e.g.*, CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. at 1019, 1024 (discussing defendant's actual notice of Compuserve's objection to spamming and the defendant's continued trespass).

[165] *See* Am. Online, Inc. v. GreatDeals.Net, 49 F. Supp. 2d 851, 854 (E.D. Va. 1999); Blue Card Report, *supra* note 160, at 5; Bliss Complaint, *supra* note 160; Christian Complaint, *supra* note 160; Dayton Complaint, *supra* note 160; Global Complaint, *supra* note 160; Nat'l Health Complaint, *supra* note 160; Persaud Complaint, *supra* note 160; USA Home Complaint, *supra* note 160; Wrhel Complaint, *supra* note 160; Plaintiff's First Amended Complaint, Am. Online, Inc. v. Cyber Promotions, Inc. (E.D. Va. June 17, 1996) (No. 96-462) http://www.bna.com/e-law/docs/aolcyber.html [hereinafter Cyber Promotions Complaint].

[166] *See id*.

liver their messages.[167] Other ISPs have raised similar claims of unjust enrichment based upon spammers' misappropriation of their computing resources.[168]

Unauthorized use of a destination operator's SMTP server and other facilities can subject a spammer to liability under state and federal computer crime laws.[169] For example, the Federal Computer Fraud and Abuse Act[170] prohibits individuals from obtaining information or causing damage by intentionally accessing a computer without authorization,[171] providing for both criminal penalties[172] and a civil right of action for injured parties.[173] Many spam-related cases have involved requests for damages or injunctive relief based upon violations of state and federal computer crime laws.[174]

Spammers frequently use the destination operator's domain name or other service marks in message headers for various reasons, including attempts to disguise the actual origin of the spam, to evade filtering and blocking by the destination operator or its subscribers, and to cause complaints to be directed to the destination operator rather than to the spammer or its service providers. Destination opera-

[167] *See id*.

[168] *See, e.g.*, Earthlink Judgment, *supra* note 160; Bigfoot Complaint, *supra* note 160; Plaintiff's Complaint, Concentric Network Corp. v. Wallace (N.D. Cal. Oct. 2, 1996) (No. C-96 20829-RMW (EAI)), http://www.bna.com/e-law/docs/concentr.html [hereinafter Concentric Complaint].

[169] "Harvesting" of e-mail addresses from a destination operator's web site, chat system, or other facilities may also give rise to liability under computer crime laws. *See, e.g.*, Am. Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444, 450 (E.D. Va. 1998).

[170] 18 U.S.C. § 1030 (1994 & Supp. 1999).

[171] *See id*. § 1030(a)(2)(C), (a)(5)(C) (Supp. 1999).

[172] *See id*. § 1030(c) (Supp. 1999).

[173] *See id*. § 1030(g) (Supp. 1999).

[174] *See, e.g.*, Am. Online, Inc. v. GreatDeals.Net, 49 F. Supp. 2d 851, 854 (E.D. Va. 1999); Am. Online, Inc. v. Prime Data Sys. Inc., No. 97-1652-A, 1998 U.S. Dist. LEXIS 20226 (E.D. Va. Nov. 20, 1998); Am. Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d at 450–51; Am. Online, Inc. v. IMS, 24 F. Supp. 2d 548, 549 (E.D. Va. 1998); Hotmail Corp. v. Van$ Money Pie, Inc., 47 U.S.P.Q.2d (BNA) ¶ 1020 (N.D. Cal. Apr. 16, 1998); Blue Card Report, *supra* note 160; CN Order, *supra* note 158; Bliss Complaint, *supra* note 160; Christian Complaint, *supra* note 160; Dayton Complaint, *supra* note 160; Global Complaint, *supra* note 160; Nat'l Health Complaint, *supra* note 160; Persaud Complaint, *supra* note 160; USA Home Complaint, *supra* note 160; Wrhel Complaint, *supra* note 160; Earthlink Judgement, *supra* note 160; Web Complaint, *supra* note 160; Squeaky Complaint, *supra* note 160; Bigfoot Complaint, *supra* note 160; OAE Complaint, *supra* note 160; Concentric Complaint, *supra* note 168; Cyber Promotions Complaint, *supra* note 165; SimpleNet Article, *supra* note 160. A few of these cases (for example, *Bigfoot Partners, L.P. v. Cyber Promotions, Inc.*, *Concentric Network Corp. v. Wallace*, *America Online, Inc. v. Cyber Promotions, Inc.*) have also alleged violations of the Electronic Communications Privacy Act, 18 U.S.C. §§ 2701–2711 (1994 & Supp. 1999). *See* Bigfoot Complaint, *supra* note 160; Concentric Complaint, *supra* note 168; Cyber Promotions Complaint, *supra* note 165.

tors and other providers whose names are included in forged message headers frequently pursue various trademark and unfair competition claims against spammers.[175]

The theories discussed here represent those most frequently applied in cases brought against spammers by destination operators. Among other theories that have been raised in such cases are nuisance;[176] misappropriation of name or identity;[177] fraud, misrepresentation, or deceptive practices;[178] negligence;[179] and tortious interference with contractual relations.[180]

2. Relay Operators

Most spam-related litigation has been brought by large consumer-oriented ISPs which have been inundated with spam addressed to their subscribers. In a few spam cases, however, the plaintiffs have been operators of SMTP servers used by spammers to relay their messages elsewhere.[181] While relay operators can configure their servers to prevent recurrences of the problem, often the damage has already been done in terms of system outages, reputational injury, and the staff time needed to repair the damage and address complaints.[182]

[175] *See, e.g.*, Am. Online, Inc. v. Prime Data Sys. Inc., No. 97-1652-A, 1998 U.S. Dist. LEXIS 20226, at *8 (E.D. Va. Nov. 20, 1998); Am. Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d at 449–50; Am. Online, Inc. v. IMS, 24 F. Supp. 2d at 551–52; Hotmail Corp. v. Van$ Money Pie, Inc., 47 U.S.P.Q.2d (BNA) ¶1020 (N.D. Cal. Apr. 16, 1998); Blue Card Report, *supra* note 160; CN Order, *supra* note 158; Christian Complaint, *supra* note 160; Dayton Complaint, *supra* note 160; Global Complaint, *supra* note 160; Nat'l Health Complaint, *supra* note 160; Persaud Complaint, *supra* note 160; USA Home Complaint, *supra* note 160; Wrhel Complaint, *supra* note 160; Earthlink Judgment, *supra* note 160; Web Complaint, *supra* note 160; Bigfoot Complaint, *supra* note 160; OAE Complaint, *supra* note 160; Concentric Complaint, *supra* note 168; Cyber Promotions Complaint, *supra* note 165; Kaplan, *supra* note 160; SimpleNet Article, *supra* note 160.

[176] *See, e.g.*, Christian Complaint, *supra* note 160.

[177] *See, e.g.*, *id.*; Bigfoot Complaint, *supra* note 160.

[178] *See, e.g.*, Christian Complaint, *supra* note 160; Dayton Complaint, *supra* note 160; Bigfoot Complaint, *supra* note 160; Concentric Complaint, *supra* note 168; Cyber Promotions Complaint, *supra* note 165.

[179] *See, e.g.*, Dayton Complaint, *supra* note 160.

[180] *See, e.g.*, Concentric Complaint, *supra* note 168.

[181] *See infra* note 183.

[182] To at least some extent, the existence of open relays contributes to the spam problem by making it easier for spammers to cover their trail. *See* discussion *supra* note 58 and accompanying text. It is conceivable that destination operators and recipients of spam might someday seek to hold relay operators themselves liable for spam, particularly in instances where the identity of the spammer cannot be ascertained (or the spammer is judgment-proof) and the relay operator has refused previous requests to limit relaying. *Cf.* Ritchenya A. Shepherd, *Online Raids Pose Issue of Firms' Security*, NAT'L L.J., Mar. 6, 2000, at A1, A1, A13 (discussing potential liability of sites hijacked by hackers for use in

Relay operators have sued spammers using many of the same legal theories as destination operators.[183] Trespass and computer abuse are somewhat easier to prove in the case of third-party relaying because it is difficult to argue that relay operators implicitly consent to the use of their servers for routing messages that neither originate from nor are addressed to their own users. However, relaying through servers in foreign countries is increasingly common, partly because such servers are less likely to use current software that limits relaying[184] and partly because operators of such servers may be less likely to take action against United States-based spammers. Most relay victims—unlike large ISPs whose customers are targeted by spammers—are likely to find the expense of litigation prohibitive, particularly given the likelihood that a spammer will be elusive or judgment-proof.[185] Furthermore, the mere threat of litigation may be sufficient to send a spammer on its way to a different open relay, providing relay victims little incentive to incur the cost of protracted litigation.

attacking other sites).

[183] *See, e.g.*, Plaintiff's Complaint, Typhoon, Inc. v. Kentech Enters. (C.D. Cal. Aug. 20, 1997) (No. CV 97-6270 JSL (AIJx)) (alleging violations of Electronic Communications Privacy Act, false designation of origin and false description under the Lanham Act, misappropriation of computer services, misappropriation of name and identity, trespass to chattels, libel, unjust enrichment, and unfair competition), http://www.jmls.edu/cyber/cases/typhoon1.html [hereinafter Typhoon Complaint], *partial settlement entered*, No. CV 97-6270 JSL (AIJx) (C.D. Cal. Sept. 30, 1997) (consent judgment and permanent injunction), http://www.jmls.edu/cyber/cases/typhoon2.html; Plaintiff's First Amended Complaint, Strong Capital Mgmt., Inc. v. Smith (E.D. Wis. Apr. 14, 1997) (No. 97-C-0371) (alleging trademark infringement, false designation of origin, violations of Computer Fraud & Abuse Act, violations of Telephone Consumer Protection Act, computer crimes under state law, violations of state facsimile law, fraudulent representations, common-law trademark infringement and unfair competition, and trespass to chattels), http://www.jmls.edu/cyber/cases/strong/comp1.html.

[184] *See* CAUCE India, *Spam in India*, *at* http://www.india.cauce.org/spamindia.html (last visited Aug. 8, 2000); James Niccolai, *China Seen as a Growing Source of Spam*, INDUSTRY STANDARD, Apr. 4, 2000, http://www.thestandard.com/article/display/0,1151,13700,00.html; CAUCE India, *Spam in India*, *at* http://www.india.cauce.org/spamindia.html (last visited Aug. 8, 2000); *Porn Spam Sent in Name of School Riles 147,000 Users*, DAILY YOMIURI (Tokyo), Aug. 1, 1999, 1999 WL 17756027.

[185] Although it is unlikely prosecutors would be interested in most instances of unauthorized third-party relaying, criminal charges might be appropriate in the most extreme cases. *Cf.* John Borland, *ISP Seeks Criminal Charges against Spammer*, TECHWEB NEWS, Nov. 13, 1997 (referring to criminal prosecution sought by destination operator), *at* http://www.techweb.com/se/directlink.cgi?WIR1997111311.

3. Forgery Victims

Forgery of message headers can help shield a spammer from being inundated with bounced messages and complaints, but often the result is merely to shift these effects to an innocent third party whose e-mail address or domain name is borrowed by the spammer.[186] In at least one sense forgery can be more insidious than third-party relaying and other spam-related activities because there is little a forgery victim can do to prevent others from appropriating its identity.

Owners of domain names used in forged message headers have brought several lawsuits.[187] Among the claims that have been raised in these cases are trademark infringement,[188] unfair competition,[189] trespass to chattels,[190] computer abuse,[191] misappropriation of name and identity,[192] violation of publicity rights,[193] false light invasion of pri-

[186] It is possible to use an invalid or fictitious domain name, of course, or to omit a domain name entirely. However, some e-mail filters automatically check for valid domain names in headers (this is significantly easier than checking for valid e-mail addresses), and some people who actually read spam may pay more attention to a message that appears to originate from a valid address, so spammers tend to avoid using addresses that are obviously invalid.

Some spammers reportedly target forgery victims as an intentional reputation attack, but in most instances the use of a particular person's name or e-mail address is likely mere coincidence. *See, e.g.*, Seidl v. Greentree Mortgage Co., 30 F. Supp. 2d 1292, 1297–98 (D. Colo. 1998) (describing spammer's use of "nobody@localhost.com," apparently in the mistaken belief that it was an invalid address).

[187] *See, e.g.*, Classified Ventures, L.L.C. v. Softcell Mktg., Inc., 109 F. Supp. 2d 898 (N.D. Ill. 2000); Seidl v. Greentree Mortgage Co., 30 F. Supp. 2d 1292, 1297 (D. Colo. 1998); Plaintiff's Complaint, Juno Online Servs., L.P. v. Scott Allen Export Sales (S.D.N.Y. Nov. 21, 1997) (No. 97 Civ. 8694), http://www.jmls.edu/cyber/cases/juno/comp.html [hereinafter Juno Complaint]; Typhoon Complaint, *supra* note 183; Parker v. C.N. Enters., No. 97-06273 (Tex. Dist. Ct. Nov. 10, 1997) (order of final judgment), http://legal.web.aol.com/decisions/dljunk/parkero.html; Plaintiffs' Application for Injunctive Relief, Web Sys. Corp. v. Cyber Promotions, Inc., (Tex. Dist. Ct. 1997) (No. 97-30156), http://www.jmls.edu/cyber/cases/websys1.html [hereinafter Web Sys. Application]; Randy Barrett, *RustNet Nabs Spammers*, INTER@CTIVE WK., Sept. 5, 1997 (discussing RustNet's suit against spammers), *at* http://www.zdnet.com/intweek/daily/970905h.html; Janet Kornblum, *Web Firm Takes on Cyber Promotions*, CNET NEWS.COM, June 6, 1997, *at* http://news.cnet.com/news/0-1005-200-319513.html; Microsoft, *Q&A: Fighting Spam at MSN Hotmail*, *at* http://www.microsoft.com/PressPass/features/1999/09-22spam.asp (Sept. 22, 1999) (discussing *Microsoft Corp. v. Franpro, Inc.*, No. 99-079269R (BQRx) (C.D. Cal. filed Sept. 1999)) [hereinafter *Hotmail* Article].

[188] *See, e.g.*, *Classified Ventures*, 109 F. Supp. 2d at 900; *Hotmail* Article, *supra* note 187.

[189] *See, e.g.*, *Classified Ventures*, 109 F. Supp. 2d at 901; Juno Complaint, *supra* note 187; Typhoon Complaint, *supra* note 183.

[190] *See, e.g.*, *Seidl*, 30 F. Supp. 2d at 1298; Typhoon Complaint, *supra* note 183; Web Sys. Application, *supra* note 187; *Hotmail* Article, *supra* note 187.

[191] *See, e.g.*, *Hotmail* Article, *supra* note 187.

[192] *See, e.g.*, Juno Complaint, *supra* note 187; Typhoon Complaint, *supra* note 183.

[193] *See, e.g.*, *Seidl*, 30 F. Supp. 2d at 1298.

vacy,[194] unjust enrichment,[195] fraud,[196] misrepresentation,[197] deceptive practices,[198] and negligence.[199] Like third-party relay cases, header forgery cases generally involve relatively straightforward legal claims, but practical obstacles often prevent forgery victims from obtaining relief.[200]

4. Service Providers

The cases discussed thus far have involved claims based primarily upon tort law brought against spammers with whom the plaintiffs had no prior relationship. There have also been several disputes between spammers and their own service providers, within the United States[201] and elsewhere,[202] mainly involving contract claims.[203] In such cases,

[194] *See, e.g.*, *id*.

[195] *See, e.g.*, Juno Complaint, *supra* note 187; Typhoon Complaint, *supra* note 183.

[196] *See, e.g.*, Juno Complaint, *supra* note 187.

[197] *See, e.g.*, *id*.

[198] *See, e.g.*, Classified Ventures, L.L.C. v. Softcell Mktg., Inc., 109 F. Supp. 2d 898, 901 (N.D. Ill. 2000); Seidl v. Greentree Mortgage Co., 30 F. Supp. 2d 1292, 1298 (D. Colo. 1998).

[199] *See, e.g.*, Seidl v. Greentree Mortgage Co., 30 F. Supp. 2d 1292, 1298 (D. Colo. 1998); Web Sys. Application, *supra* note 187.

[200] *Cf. supra* text accompanying note 185. One United Kingdom-based ISP that was victimized by header forgery filed suit against the spammer in a United States court, and as a condition of settlement required the spammer to agree to limitations on its future spam-related activities, even those not involving the plaintiff ISP. This is reportedly the first case involving such a broad remedy. *See* Jean Eaglesham, *Internet Company Wins US Legal Fight on Junk E-Mails*, FIN. TIMES (London), Mar. 29, 2000, at 9; Jason Gonzalez, *Ruling Bars Spammer From Repeat Mailings*, IMARKETING NEWS, Apr. 24, 2000, *at* http://www.dmnews.com/archive/2000-04-24/7916.html.

[201] *See, e.g.*, Cyber Promotions, Inc. v. Apex Global Info. Servs., Inc., No. 97-5931, 1997 U.S. Dist. LEXIS 15344 (E.D. Pa. Sept. 30, 1997); *Cyber Promotions Sues WorldCom*, *at* http://www.jmls.edu/cyber/cases/cp-wc0.html (June 24, 1997) (discussing a spammer's suit against his ISP) [hereinafter *WorldCom* Article]; Kaplan, *supra* note 160 (discussing Visto's suit against a Visto user who spammed); *Hotmail* Article, *supra* note 187 (discussing Microsoft's suit against a Hotmail user who spammed).

A similar situation arose in another case, *Hall v. Earthlink Network, Inc.*, No. 98-CIV-5489 (S.D.N.Y. filed July 30, 1998), which involved an ISP that terminated service to a subscriber based upon a mistaken belief that he was responsible for spamming. *See* Hall Complaint, *supra* note 50; Metal Tiger Technologies, *Cyber Rights Litigation*, *at* http://metal-tiger.com/delinquent/litigation.html (last visited Aug. 8, 2000).

[202] *See, e.g.*, 1267623 Ont. Inc. v. Nexx Online, Inc., No. C-20546/99, 1999 Ont. Sup. C.J. LEXIS 465 (Ont. Super. Ct. J. June 14, 1999); I.D. Internet Direct Ltd. v. Altelaar, No. 99-CV-162738, 1999 Ont. Sup. C.J. LEXIS 320 (Ont. Super. Ct. J. May 3, 1999).

Virgin Net brought the first spam lawsuit in the United Kingdom in April of 1999 against a spammer, Adrian Paris, who settled a few weeks later. *See* Tim Richardson, *Virgin Spammer Settles out of Court*, REG. (London), May 26, 1999, http://www.theregister.co.uk/content/archive/4563.html; Jane Wakefield, *Virgin Sues Spam Pest*, ZDNET UK, Apr. 20, 1999, *at* http://www.zdnet.co.uk/news/1999/15/nsthe provider typically is permitted to terminate the spammer's service and the spammer may be enjoined from opening additional accounts with the provider,[204] although actual or even liquidated damages to the ISP should also be available in appropriate cases.[205]

Internet service providers normally require their customers to abide by terms of service that clearly prohibit most or all forms of spam,[206] but even a general reference to "netiquette" rules may suffice to support a provider's termination of a customer.[207] Because the

7833.html; John Willcock, *Virgin Takes Action to Stop "Spamming" on the Internet*, INDEP. (London), Apr. 19, 1999, LEXIS, News Library, Independent File; *Virgin Net Sues Customer*, WIRED NEWS, Apr. 20, 1999, *at* http://www.wired.com/news/news/technology/0,1282,19224,00.html.

[203] In another recent case, a domain name registrar sued a marketer for collecting domain registrants' names and contact information from the registrar's online database and using the information for solicitations, including spam. *See* Brief of Amicus Curiae ICANN, Register.com, Inc. v. Verio Inc. (S.D.N.Y. Sept. 22, 2000) (No. 00-Civ-5747 (BSJ)), http://www.icann.org/registrars/register.com-verio-amicus-22sep00.htm; Joanna Glasner, *Setting Limits for "Whois" Data*, WIRED NEWS, Aug. 4, 2000, *at* http://www.wired.com/news/politics/0,1283,38025,00.html; *REGISTER.COM: Lawsuit Alleges Verio Sent Unsolicited E-Mails, Calls*, WALL ST. J., Aug. 4, 2000, 2000 WL-WSJ 3039047.

[204] *See, e.g.*, authorities cited *supra* note 201–202.

[205] Provisions for liquidated damages for spam-related violations are becoming common in ISP service agreements. *See, e.g.*, Adam Pty Ltd, *Terms and Conditions*, *at* http://www.adam.com.au/service_terms.htm (last visited Apr. 21, 2000) (Austl. $5 per message or 39¢ per megabyte); Elecs. 2000, *Terms of Service (TOS) for All POP3 Electronics 2000 Users*, *at* http://electronics2000.com/pop3/ (last modified Jan. 1, 2000) ($100 per message); InterAccess, *Acceptable Use Policy*, *supra* note 24 ($20,000); Juno, *Guidelines*, *supra* note 23 ($200 per day); MSN Hotmail, *MSN Hotmail Terms of Service*, *at* http://www.hotmail.msn.com/cgi-bin/dasp/hminfo_shell.asp?content=tos&_lang=EN&id=2&ct=980651510 (last visited Aug. 8, 2000) ($5 per message); NUNet, Inc., *NUNet's Terms of Service Agreement*, *at* http://www.nni.com/tos.html (last visited Aug. 8, 2000) ($125 per hour for staff time, plus $0.50 per addressee); Salaam, *Salaam's Ummah.org Terms of Service (TOS)*, *at* http://config.ummah.org/signup.html (last visited Aug. 8, 2000) (£5 per message); StarHub Pte Ltd, *Terms & Conditions for StarHub Internet Services*, *at* http://regwww.mystarhub.com.sg/help/terms.html (last visited Aug. 8, 2000) (Sing. $10 per message); *cf. infra* note 266 and accompanying text (discussing statutory damage provisions).

[206] *See* Nora Macaluso, *Major ISPs Boot Spammers*, E-COMMERCE TIMES, Nov. 10, 2000, *at* http://www.ecommercetimes.com/news/articles2000/001110-1.shtml. A 1997 case involved a provider whose contract with a customer included a term explicitly *permitting* the customer to send unsolicited bulk e-mail. *See* Cyber Promotions, Inc. v. Apex Global Info. Servs., Inc., No. 97-5931, 1997 U.S. Dist. LEXIS 15344, at *2 (E.D. Pa. Sept. 30, 1997). When the provider found itself subjected to numerous denial-of-service, or "ping," attacks because of its unpopular customer, it terminated the customer's service notwithstanding the contract. *See id.* at *2. The court noted that the provider could have anticipated the attacks and was obligated to give thirty days' advance notice before terminating service, as required by the explicit terms of the parties' contract. *See id.* at *6, *10; *see also WorldCom* Article, *supra* note 201 (alleging similar facts in lawsuit filed by same customer against another service provider).

[207] *See* 1267623 Ont. Inc. v. Nexx Online, Inc., No. C-20546/99, 1999 Ont. Sup. C.J. LEXIS 465, at *7–*15 (Ont. Super. Ct. J. June 14, 1999); *see also* Wakefield, *supra*

backlash against spam is likely to affect all providers that are associated with a spammer, many providers prohibit their customers from spamming even if the provider's own facilities are not used to send the messages.[208]

Lawsuits may be relatively effective for large plaintiffs like America Online in combating relatively large, highly visible, and persistent spammers like the now-defunct "spam king," Cyber Promotions. But spammers are often much smaller operators—individuals who may use a succession of dial-up accounts with several different providers to advertise web sites or multi-level scams in exchange for commissions.[209] These spammers can be very difficult to trace—frequently they route their messages through mail servers in foreign countries—and most spammers do not have sufficient assets to justify a lawsuit, even if the havoc they wreak is substantial and measurable.

While most of the spam cases involve traditional litigation, the service provider cases may be prime candidates for alternative methods of dispute resolution ("ADR"). For example, Internet service providers might well begin including mandatory arbitration clauses in their service agreements, and parties with legitimate disputes might voluntarily submit to mediation or arbitration in order to avoid the costs of litigation. Unfortunately, the only widely reported application of ADR to the spam problem thus far has been acknowledged as a failure.[210]

note 202 (quoting Virgin Net terms that prohibited subscribers from "send[ing] material likely to cause annoyance, inconvenience or anxiety").

[208] *See, e.g.*, 1267623 Ont. Inc. v. Nexx Online, Inc., No. C-20546/99, 1999 Ont. Sup. C.J. LEXIS 465, at *16–*17 (Ont. Super. Ct. J. June 14, 1999); Access Nevada Internet Servs., *Access Nevada's Anti-Spam Policy*, *at* http://www.anv.net/antispam.shtml (last visited Aug. 8, 2000); @Home, *@Home Service Acceptable Use Policy*, *at* http://www.home.com/support/aup/ (last modified May 8, 2000); Erols Internet Servs., *Erols Internet Access Agreement*, *at* http://www.erols.com/erols/index/agreement.htm (last visited Aug. 8, 2000); InterAccess, *Acceptable Use Policy*, *supra* note 24; Juno, *Guidelines*, *supra* note 23; ReplyNet LLC, *ReplyNet's Terms of Service Agreement*, *at* http://www.reply.net/terms.html (last visited Feb. 6, 2001); Response-O-Matic, *Terms of Use*, *at* http://www.response-o-matic.com/legal.htm (last visited Aug. 8, 2000).

[209] *See* SCHWARTZ & GARFINKEL, *supra* note 2, at 36–38.

[210] The Virtual Magistrate Project was an experimental service initiated in 1996 by the Cyberspace Law Institute and operated by Villanova University School of Law. *See* Virtual Magistrate Project, *Virtual Magistrate Established for the Internet*, *at* http://www.vmag.org/docs/press/030496.html (Mar. 4, 1996). The project is now operated by Chicago-Kent College of Law but appears to be virtually defunct. *See The Virtual Magistrate*, *at* http://www.vmag.org/ (last visited Aug. 8, 2000); Timothy Wu, *Application-Centered Internet Analysis*, 85 VA. L. REV. 1163, 1198 & n.91 (1999); Timothy Wu, *When Law & the Internet First Met*, 3 GREEN BAG 2D 171, 176–77 (2000). The Virtual Magistrate's first case (and apparently its only one) was a complaint brought against America Online by one of its subscribers, seeking to force AOL to block or remove a posting by a third party, Email America. AOL agreed to submit the matter to arbitration, but Email America did not—and not surprisingly, the Virtual Magistrate held that AOL

B. Legislation

The expense of lawsuits, along with the uncertain status of the law regarding spam, has led to calls for legislation specifically designed to restrict or prohibit spam. Bills have been introduced in Congress[211] and in state legislatures, and more than a dozen states have already enacted anti-spam legislation of one form or another.[212] The

should remove the offending posting from its system. *See* Alejandro E. Almaguer & Roland W. Baggott III, Note, *Shaping New Legal Frontiers: Dispute Resolution for the Internet*, 13 OHIO ST. J. ON DISP. RESOL. 711, 727–33 (1998); Virtual Magistrate Project, *Virtual Magistrate Issues Its First Decision Recommends that AOL Remove a Subscriber Message Offering Millions of Email Addresses For Sale*, *at* http://www.vmag.org/docs/press/052196.html (May 21, 1996). As it turned out, AOL could not "remove" the posting, since it was merely an e-mail message that was delivered through AOL's system. *See* Almaguer & Baggott, *supra*, at 732–33; Wendy R. Leibowitz, *Internet Mediators: "We're Idle,"* NAT'L L.J., Aug. 12, 1996, at A7. Critical commentary on the project has generally been unfavorable, primarily due to its handling of the *Tierney* matter. *See, e.g.*, Almaguer & Baggott, *supra*, at 730–36; Leibowitz, *supra*, at A7; David J. Loundy, *Virtual Magistrate Becomes a Reality, Sort of*, CHI. DAILY L. BULL., June 16, 1996, http://www.loundy.com/CDLB/Virtual-Magistrate.html; Mark Voorhees, *A "Good" Case, Not an "Ideal" Case: Virtual Justice: The No-Show Case Showcases Promise and Peril of Magistrate Project*, INFO. L. ALERT, June 3, 1996, 1996 WL 8913605. *See generally* Ethan Katsh & Janet Rifkin, *An Online Ombuds Office on the Internet: Interim Report to the National Center for Automated Information Research*, *at* http://www.ombuds.org/ncair3.html (Aug. 26, 1996) (expressing doubt whether online mediation is well-suited to resolving spam-related disputes).

[211] *See* Unsolicited Electronic Mail Act of 2001, H.R. 95, 107th Cong.; Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2000, S. 2542, 106th Cong.; Netizens Protection Act of 1999, H.R. 3024, 106th Cong. (1999); Unsolicited Commercial Electronic Mail Act of 2000, H.R. 3113, 106th Cong.; Can Spam Act, H.R. 2162, 106th Cong. (1999); E-Mail User Protection Act, H.R. 1910, 106th Cong. (1999); Internet Freedom Act, H.R. 1686, 106th Cong. § 104 (1999); Internet Growth and Development Act of 1999, H.R. 1685, 106th Cong. § 201; Inbox Privacy Act of 1999, S. 759, 106th Cong.; Unsolicited Commercial Electronic Mail Choice Act of 1997, S. 771, 105th Cong.; Netizens Protection Act of 1997, H.R. 1748, 105th Cong.

[212] *See* CAL. BUS. & PROF. CODE §§ 17538.4, .45 (Deering Supp. 2000) (California); 815 ILL. COMP. STAT. ANN. 511/1, 511/5, 511/10, 511/15 (West Supp. 2000) (Illinois); IOWA CODE ANN. §§ 714E.1, .2 (West Supp. 2000) (Iowa); LA. REV. STAT. ANN. § 14:73.6 (West Supp. 2000) (Louisiana); NEV. REV. STAT. ANN §§ 41.705-.735 (Michie Supp. 1999) (Nevada); N.C. GEN. STAT. §§ 14-453, -458, 1-539.2A (1999) (North Carolina); R.I. GEN. LAWS §§ 6-47-2, 11-52-1, -4.1, -6 (Supp. 1999) (Rhode Island); TENN. CODE ANN. §§ 47-18-2501, -2502 (Supp. 1999) (Tennessee); Virginia Computer Crimes Act, VA. CODE ANN. §§ 18.2-152.1–.15 (Michie 1996 & Michie Supp. 2000) (Virginia); WASH. REV. CODE ANN. § 19.190.010–.050 (West 1999 & West Supp. 2001) (Washington); W. VA. CODE ANN. §§ 46A-6G-1 to -5 (Michie 1999) (West Virginia); Colorado Junk Email Law, ch. 388, 2000 Colo. Sess. Laws 2031 (to be codified at COLO. REV. STAT. §§ 6-2.5-101 to -105, 13-6-105, -403) (Colorado); Act of June 23, 1999, No. 99-160, 1999 Conn. Pub. Acts 446 (Connecticut); Act of July 2, 1999, ch. 135, 72 Del. Laws 7 (1999) (to be codified at DEL. CODE tit. 11, §§ 931(12)–(17), 937, 938) (Delaware); Act of Apr. 17, 2000, ch. 423, 2000 Idaho Sess. Laws 1373 (to be codified at IDAHO CODE § 48-603E) (Idaho); Act of June 27, 2000, ch. 763, § A, 2000 Mo. Laws 735, 749 (to be codified at MO. REV. STAT. §§ 407.1300–.1340) (Missouri); Act of June 8, 1999, ch.

United States Senate passed a spam bill in May of 1998,[213] and the House of Representatives passed a bill with stronger anti-spam provisions in 2000,[214] neither of which were enacted into law. Other countries and the European Union have also considered imposing statutory restrictions on spam.[215] The legislative responses to spam thus far have ranged in substance from mere disclosure requirements[216] all the way to outright prohibition of unsolicited bulk or commercial e-mail messages.[217]

1. Prohibition

In the United States, Delaware has enacted what appears to be the most restrictive spam law.[218] Sending unsolicited bulk commercial e-mail constitutes a violation of Delaware's computer crime law.[219] The law applies to messages sent into Delaware from outside the state if the sender knew that there was a "reasonable possibility" that the recipient was in Delaware.[220]

337, 1999 Okla. Sess. Laws 1515 (to be codified at OKLA. STAT. tit. 15, § 776.1–.4) (Oklahoma); Act of June 13, 2000, No. 25, §1, 2000 Pa. Legis. Serv. 91 (to be codified at 18 PA. CONS. STAT. § 5903(a.1), (l), (m)) (Pennsylvania).

[213] *See* Anti-Slamming Amendments Act, S. 1618, 105th Cong. (1998).

[214] *See* Unsolicited Commercial Electronic Mail Act of 2000, H.R. 3113, 106th Cong. This bill was recently reintroduced to the 107th Congress. *See* Unsolicited Electronic Mail Act of 2001, H.R. 95, 107th Cong.

[215] *See* discussion *infra* Part IV.B.1 and accompanying notes.

[216] *See* NEV. REV. STAT. ANN § 41.730 (Michie Supp. 1999).

[217] *See* Act of July 2, 1999, ch. 135, § 1, 72 Del. Laws 7 (1999) (to be codified at DEL. CODE tit. 11, §§ 931(12)–(17), 937, 938).

[218] *See id*.

[219] *See id*. (to be codified at DEL. CODE tit. 11, § 937(a)) (providing that a crime is committed when one "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"). "Bulk" is not defined in the statute, although messages "sent between human beings" are exempted. *See id*. Similarly, "unsolicited" is not defined, but the statute exempts messages that are sent at the recipient's request, by an organization to its members, or with a pre-existing business relationship. *See id*.

[220] The statute provides:

> For the purposes of this section, conduct occurring outside of the State shall be sufficient to constitute this offense if such conduct is within the terms of Section 204 of this title, or 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.

Id. (to be codified at DEL. CODE tit. 11, § 937(d)).

The Netizens Protection Act of 1997,[221] one of the first two spam-related bills introduced in the United States Congress,[222] would have broadened the federal law that prohibits unsolicited facsimile advertisements to include advertisements transmitted by electronic mail.[223] None of the recent federal bills include an outright prohibition of spam.[224]

The European Union does not prohibit unsolicited commercial e-mail, but permits individual member states to do so.[225] Finland,[226] Germany,[227] and Italy[228] all have laws prohibiting UCE, while Austria prohibits both UCE and UBE,[229] and other European countries are

[221] H.R. 1748, 105th Cong. (1997).

[222] The Unsolicited Commercial Electronic Mail Choice Act of 1997, S. 771, 105th Cong., was introduced one day earlier.

[223] *See supra* notes 154–157 and accompanying text (discussing applicability of current fax advertising law to e-mail).

[224] The Netizens Protection Act was reintroduced in 1999, but the later version merely included disclosure and opt-out requirements. *See* H.R. 3024, 106th Cong. (1999). Legislation introduced in early 1999 would have authorized the FTC to enact regulations governing unsolicited commercial e-mail as a deceptive act or practice, although it seems unlikely that the FTC would have used this authority to prohibit UCE entirely. *See* Protection Against Scams on Seniors Act of 1999, H.R. 612, 106th Cong. § 202; Telemarketing Fraud and Seniors Protection Act, S. 699, 106th Cong. § 202(a) (1999) (companion bill to H.R. 612).

[225] *See* Common Position Adopted by the Council with a View to the Adoption of a Directive of the European Parliament and of the Council on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market, 2000 O.J. (C 128) 32, 36, 40–42, 47, http://europa.eu.int/comm/internal_market/en/media/eleccomm/composen.pdf [hereinafter Directive on Electronic Commerce]. Prior EU directives require marketers to comply with "opt-out" requests. *See* Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector, art. 12, 1998 O.J. (L 024) 1, http://europa.eu.int/eur-lex/en/lif/dat/1997/en_397L0066.html; Directive 97/7/EC on the European Parliament and of the Council of 20 May 1997 on the Protection of Consumers in Respect of Distance Contracts, art. 10, 1997 O.J. (L 144) 19, http://europa.eu.int/eur-lex/en/lif/dat/1997/en_397L0007.html [hereinafter Directive 97/7/EC]; Directive 95/46/EC on the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, art. 14(b), 1995 O.J. (L 281) 31, http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html.

[226] *See* EuroCAUCE, *Finland*, *at* http://www.euro.cauce.org/en/countries/c_fi.html (last visited Aug. 8, 2000) (citing 1999 amendment to Data Security Act).

[227] *See* EuroCAUCE, *Germany*, *at* http://www.euro.cauce.org/en/countries/c_de.html (last visited Aug. 8, 2000) (citing Unfair Competition Law and trespass provisions in Federal Civil Code); *see also* cases cited *supra* note 158.

[228] *See* EuroCAUCE, *Italy*, *at* http://www.euro.cauce.org/en/countries/c_it.html (last visited Aug. 8, 2000) (citing Legislative Degree of May 22, 1999).

[229] *See* §§ 101, 104(3)(23) TKG BGBl 188/1999, http://www.tkc.at/www/RechtsDB.nsf/d2bebf4c91dc898cc12567e8002c1cb2/5376142e8598c2de412567e8004d944f!OpenDocument (last visited Jan. 16, 2001) (displaying the relevant sections of the Austrian tele-

considering whether to enact similar restrictions.[230] Neither Australia nor Canada, two other countries generally regarded as having much stronger privacy laws than the United States, have laws that prohibit spam.[231]

communications law ("Telekommunikationsgesetz"), pertaining to unsolicited e-mail); EuroCAUCE, *Austria*, *at* http://www.euro.cauce.org/en/countries/c_at.html (last visited Aug. 8, 2000).

[230] The United Kingdom is in the process of implementing Directive 97/7/EC, *supra* note 225, and is currently considering an opt-in regulation that would prohibit most UCE sent to United Kingdom residents from within the United Kingdom and possibly elsewhere. *See* U.K. Dep't of Trade & Indus., *Implementation of EU Directive 97/7/EC on the Protection of Consumers in Respect of Distance Contracts: A Further Consultation Paper: Annex A*, *at* http://www.dti.gov.uk/CACP/ca/policy/distanceselling/annex_a.htm (Nov. 1999); U.K. Office of Fair Trading, *Problems with Online Shopping?*, *at* http://www.oft.gov.uk/html/shopping/noframes/watchout.html (last modified Apr. 5, 2000). *But see* Colin Lloyd, *Dear U.S. Direct Marketer: Colin Lloyd on the Vicissitudes of Privacy and E-Mail*, DM NEWS, Apr. 17, 2000, LEXIS, News Library, DMNews File (citing rumors that the United Kingdom will favor an opt-out regime for unsolicited e-mail). *See generally* EuroCAUCE, *United Kingdom*, *at* http://www.euro.cauce.org/en/countries/c_uk.html (last visited Aug. 8, 2000) (noting arguments against UCE under existing United Kingdom laws).

In 1999, the French Data Processing and Liberties Commission published a report on unsolicited e-mail, but the report focused primarily on the propriety of various methods of collecting e-mail addresses rather than the practice of sending unsolicited bulk or commercial messages. *See* Comm'n Nationale de l'Informatique et des Libertés, *Prospection Non Sollicitée sur Internet et "spamming": la Commission Nationale de l'Informatique et des Libertés Rappelle la Règle du Jeu [Unsolicited Advertising on the Internet and "Spamming": the National Commission of Data Processing and Freedoms Points Out the Rule of the Game]*, *at* http://www.cnil.fr/actu/communic/ (Oct. 28, 1999) [hereinafter CNIL, *Spamming*].

The Danish Consumer Ombudsman was unable to reach an agreement on the issue with industry representatives in 1998, while a 1999 position paper issued by the consumer ombudsmen of Denmark, Finland, Norway, and Sweden states that prior consent is needed for e-mail solicitations. *See* EuroCAUCE, *Denmark*, *at* http://www.euro.cauce.org/en/countries/c_dk.html (last visited Apr. 12, 2000); Nat'l Consumer Agency, *The Nordic Consumer Ombudsmen Want to Secure Proper Trading and Marketing on the Internet*, *at* http://www.fs.dk/uk/misc/p990106u.htm (Jan. 6, 1999); Nat'l Consumer Agency, *The Nordic Consumer Ombudsmen's Position Paper to Trading and Marketing on the Internet and in Similar Communication Systems*, *at* http://www.consumer.dk/uk/acts/nord_gui.htm (Dec. 30, 1998); Nat'l Consumer Agency, *News from the Danish Consumer Ombudsman: Collapse of Internet Negotiations*, *at* http://www.fs.dk/uk/misc/p980928u.htm (Sept. 30, 1998).

[231] Australia's Department of the Treasury recently published a draft report on best practices for electronic commerce, including three proposed alternative provisions on unsolicited e-mail, one of which ("Opt In") would effectively constitute a prohibition on spam. *See* Austl. Dep't of Treasury, *Building Consumer Sovereignty in Electronic Commerce: A Best Practice Model for Business*, at 5, http://www.ecommerce.treasury.gov.au/publications/BuildingConsumerSovereigntyInElectronicCommerce-AbestPracticeModelForBusiness/ecommerce.pdf (Dec. 1999). The Australian Internet Industry Association has endorsed an opt-in regime. *See* Internet Indus. Ass'n, *Opt-Out Spam Is Out of Bounds*, *at* http://www.iia.net.au/news/000211.html (Feb. 20, 2000).

Canada's new privacy law imposes substantial restrictions on the use and collection of personal information, but does not include any provisions specific to unsolicited e-mail.

2. Enforcement of Anti-Spam Policies

ISPs and other destination operators generally have policies that govern the use of their facilities for various purposes, and nearly all of them prohibit spamming in particular. Several jurisdictions have considered enforcing such policies as a more flexible, and perhaps more palatable, alternative to enacting an outright ban on spam. Giving legal force to providers' policies is consistent with the trespass perspective: if placing an SMTP server on the Internet implicitly authorizes others to use the server to deliver e-mail messages to users who are affiliated with the server, then announcing conditions on the use of the server withdraws that implicit authority when the conditions are not satisfied.[232] The difficult questions in such an approach lie in determining the circumstances under which policies should be enforced—in particular, determining what form of notice ought to be required before a provider's policies can be enforced with respect to a particular spammer.

Several methods of providing constructive notice of such policies have been proposed. First, a provider may choose to post its policies on the web—preferably, where they can be easily located by someone who knows nothing more than the prospective recipient's e-mail address.[233] Second, a provider may configure its SMTP server to transmit a brief reference to its policies during every session, before it will receive a message.[234] A third approach would be for providers to regis-

See Personal Information Protection and Electronic Documents Act, Bill No. C-6 (2000) (Can.), http://www.privcom.gc.ca/english/02_06_e.htm (enacted Apr. 13, 2000).

[232] *See supra* Part IV.A.1 and accompanying notes (discussing trespass claims by destination operators).

[233] Thus, for example, one planning to transmit an unsolicited message to "user@example.com" could access the web page at http://www.example.com/ and look for a reference to e-mail policies. Many destination operators currently post their policies in this manner. *See, e.g.*, Tom Geller, *Suespammers.org*, *at* http://www.suespammers.org/ (last visited Aug. 8, 2000) ("The suespammers.org Web and Mail servers are located in California. You are hereby forbidden to send unsolicited commercial e-mail or unsolicited bulk mail of any kind to a suespammers.org address. (California BPC, Section 17538.45)."); *NetEase Internet Access Service*, *at* http://www.netease.net/ (last visited Apr. 30, 2000) ("The netease.net Web and Mail servers are located in Tennessee. In accordance with Tennessee Code Annotated, Title 47, Chapter 18 you are hereby forbidden to send unsolicited commercial e-mail or unsolicited bulk mail of any kind to a netease.net address. Anyone that send un-solicited e-mail to netease.net users will be fined to the maximum allowed amount of $10 per message or $5,000 per day."); *WA-STATE-RESIDENT.COM*, *at* http://www.wa-state-resident.com/ (last modified Jan. 31, 2000) ("Unsolicited bulk e-mail may not be sent to any address at WA-STATE-RESIDENT.COM without the recipient's permission.").

[234] *See* CAUCE, *CAUCE's "SMTP Banner Notification" Proposal*, *at* http://www.cauce.org/proposal/ (last visited Aug. 8, 2000) (suggesting that recipient sites

ter their policies with a central authority, such as a state or federal government agency; spammers could be required to consult a central registry of providers' policies before sending unsolicited messages.[235]

Louisiana law prohibits sending unsolicited bulk e-mail if the sender uses a provider's facilities to transmit the messages in violation of the provider's policies;[236] the law does not specify whether the sender must have actual notice of the policies.[237] California will enforce a destination operator's policies prohibiting unsolicited commercial e-mail if the sender has actual notice thereof.[238] Several other states will enforce particular aspects of providers' policies, but not to the extent of a complete prohibition on UCE or UBE.[239]

Some of the bills introduced in the last session of the United States Congress would have also given force to providers' anti-spam policies had they been enacted. The Internet Growth and Development Act of 1999[240] would have enforced policies that prohibit UCE if the sender had actual notice of the policies.[241] The Netizens Protec-

could include "NO UCE" or "UCE POLICY AT _____" in the "SMTP banner," or initial greeting message transmitted at the beginning of every SMTP session).

[235] For example, one bill introduced in the United States Congress would have prohibited sending UCE to e-mail addresses containing a domain name whose owner had previously notified the FTC of its election not to receive such messages. *See* Inbox Privacy Act of 1999, S. 759, 106th Cong. § 2(b), (c). A similar approach was proposed in a 1998 New Hampshire bill. *See* H.R. 1633, 1998 Gen. Ct., 155th Sess. (N.H. 1998) (authorizing registration of "restricted solicitation electronic mail provider[s]").

[236] *See* LA. REV. STAT. ANN. § 14:73.6(A) (West Supp. 2000).

[237] *See id.* Since the Louisiana law imposes criminal sanctions for violating a provider's policies, it seems likely that actual notice will be required.

[238] *See* CAL. BUS. & PROF. CODE § 17538.45(f)(3)(A)(i) (Deering Supp. 2000). An amendment to the California statute would have created an official state registry of providers with UCE policies; registration would serve as an alternative to actual notice. *See* Assemb.B. 2704, 1999–2000 Leg., Reg. Sess. (Cal. 2000). However, it was vetoed by the Governor. *See* Cal. Legis. Servs., *Current Bill Status*, *at* http://www.leginfo.ca.gov/pub/99-00/bill/asm/ab_2701-2750/ab_2704_bill_20000914_status.html (last modified Sept. 11, 2000).

[239] *See, e.g.*, R.I. GEN. LAWS §§ 11-52-1(15)(e)(2), -4.1(7) (Supp. 1999) ((unlawful to send UBE with forged headers in violation of a provider's policies)); VA. CODE ANN. §§ 18.2-152.2, .4(A)(7) (Michie Supp. 2000) (same); Act of June 23, 1999, No. 99-160, § 1(a)(14)(B), (b)(7), 1999 Conn. Pub. Acts 446, 448–49 (same); N.C. GEN. STAT. § 14-458(a)(6) (1999) (unlawful to send UBCE with forged headers in violation of a provider's policies); W. VA. CODE ANN. §§ 46A-6G-1(1), -2 (Michie 1999) (unlawful to send UBE in violation of a provider's policies if the message fails to identify the sender or has forged headers, a false or misleading subject line, or sexually explicit content); *see also* TENN. CODE ANN. §§ 47-18-2501, -2502 (Supp. 1999) (defining use "without authority" to include violations of an e-mail provider's policies, though statute places no restrictions on use "without authority").

[240] H.R. 1685, 106th Cong. (1999).

[241] *See id.* § 201.

tion Act of 1999[242] would have enforced anti-spam policies but only against a provider's own customers.[243] Three other bills would have enforced anti-UCE policies based upon various forms of constructive notice—web posting,[244] SMTP banner notification,[245] or a centralized registry.[246]

If a law is enacted that enforces providers' anti-spam policies and one or more of these forms of constructive notice is deemed adequate, the practical result will be roughly equivalent to imposing a legal prohibition on spam, since nearly all destination operators already have anti-spam policies and nearly all likely will take advantage of the constructive notice provision.

3. Opt-Out Procedures

Most of the responses to spam share as a common objective the desire to give individuals the ability to control whether they receive bulk or commercial e-mail messages. A prohibition on spam—or a law giving destination operators the ability to ban spam from their systems—would accomplish this objective with an "opt-in" rule: marketers would be permitted to send e-mail only to persons who explicitly opt in to receive it. In an opt-out system, on the other hand, senders may communicate with everyone except those who have explicitly opted out.

Several proposed statutes would implement various opt-out systems. For example, spammers might be required to include instructions for submitting opt-out requests, possibly even with a toll-free phone number, and then would be subject to penalties for ignoring opt-out requests.[247] Or, ISPs might be required to maintain opt-out lists of their own users, or a state or federal agency might maintain an opt-out list of e-mail addresses or entire domains that have opted out of receiving spam.[248]

[242] H.R. 3024, 106th Cong. (1999).

[243] *See id*. § 3.

[244] *See* Unsolicited Commercial Electronic Mail Act of 2000, H.R. 3113, 106th Cong. § 5(b)(2)(B)(i); Can Spam Act, H.R. 2162, 106th Cong., § 2(d)(4)(C)(i) (1999).

[245] *See* Can Spam Act, H.R. 2162, 106th Cong. § 2(d)(4)(C)(ii), (iii) (1999).

[246] *See* Inbox Privacy Act of 1999, S. 759, 106th Cong. § 2(b), (c).

[247] *See, e.g.*, Unsolicited Electronic Mail Act of 2000, H.R. 3113, 106th Cong. § 5(a); Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2000, S. 2542, 106th Cong. § 4(a); Inbox Privacy Act of 1999, S. 759, 106th Cong. § 2(d); Netizens Protection Act of 1999, H.R. 3024, 106th Cong. § 2(a) (1999).

[248] *See* Unsolicited Electronic Mail Act of 1999, H.R. 3113, 106th Cong. § 4(a) (original version of the bill), *available at* http://thomas.loc.gov/cgi-bin/query/C?c106:./temp/~c106PruMtl; *see also* Inbox Privacy Act of 1999, S. 759, 106th Cong. § 2(c); H.R. 1633,

The European Union is currently considering a proposal that would establish national opt-out registries, and companies would be prohibited from sending spam to those listed in the registries.[249] Residents of the State of Washington can add their e-mail addresses to an online registry of Washington residents, designed to provide spammers with notice that they are protected by the state's spam statute, although the legal effect of the registry is not entirely clear.[250] Many other states have enacted legislation requiring spammers to honor individual opt-out requests,[251] but none has yet adopted a centralized opt-out registry for Internet users, or even domain-specific registries to be maintained by destination operators.

4. Content Regulations

An alternative to regulating the conditions under which unsolicited e-mail messages may be sent is to regulate the information contained in such messages. Usually such restrictions are aimed at message headers,[252] although laws that apply only to commercial

1998 Gen. Ct., 155th Sess. (N.H. 1998). Domain-wide opt-out is equivalent to a destination operator's policy that prohibits spam. *See supra* note 78 and accompanying text.

[249] *See* CNIL, *Spamming*, *supra* note 230; Directive on Electronic Commerce, *supra* note 225, at 33; *see also* authorities cited *supra* note 225.

[250] *See* Wash. Ass'n of Internet Service Providers, *WAISP Registry Page*, *at* http://registry.waisp.org/ (last modified May 3, 1999). The Washington statute prohibits using false headers and misleading subject lines in unsolicited commercial e-mail messages if the sender knows, or has reason to know, that the recipient is a Washington resident. *See* WASH. REV. CODE ANN. § 19.190.020 (West Supp. 2001). The WAISP Registry presumably is intended to satisfy the constructive knowledge requirement, although the statute seems to recognize constructive knowledge only when confirmation of residency is available upon request from the registrant of the domain name contained in the recipient's e-mail address. *See id.* § 19.190.020(2); *cf.* Attorney Gen. of Wash., *Junk E-Mail: Protect Yourself* ("As long as the location of a Washington e-mail address is available to the would-be spammer, whether or not they actually check all possible sources of this information, they are prohibited from sending unsolicited e-mail in violation of the law to a Washington resident."), http://www.wa.gov/ago/junkemail/protect.html (last visited Aug. 8, 2000).

[251] *See, e.g.*, CAL. BUS. & PROF. CODE § 17538.4(c) (Deering Supp. 2000); IOWA CODE ANN. § 714E.1(2)(e) (West Supp. 2000); R.I. GEN. LAWS § 6-47-2(c) (Supp. 1999); TENN. CODE ANN. § 47-18-2501(c) (Supp. 1999); Colorado Junk Email Law, ch. 388, § 1, 2000 Colo. Sess. Laws 2031, 2033 (to be codified at COLO. REV. STAT. § 6-2.5-103(5)); Act of Apr. 17, 2000, ch. 423, § 1, 2000 Idaho Sess. Laws 1373, 1374 (to be codified at IDAHO CODE § 48-603E(3)(d)).

Legislation introduced at the federal level also would have required spammers to honor opt-out requests. *See* Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2000, S. 2542, 106th Cong., § 4(b); Unsolicited Commercial Electronic Mail Act of 2000, H.R. 3113, 106th Cong. § 5(a)(2); Inbox Privacy Act of 1999, S. 759, 106th Cong. § 2(a)(1); Netizens Protection Act of 1999, H.R. 3024, 106th Cong. § 2(a)(2); E-Mail User Protection Act, H.R. 1910, 106th Cong. § 2(a)(3) (1999).

[252] *See supra* note 18 (discussing message headers).

messages—particularly those that prohibit the use of misleading subject lines—can affect the body of a message as well as its header.

Many jurisdictions prohibit the use of forged or incomplete message headers in unsolicited bulk or commercial e-mail messages.[253] The theory behind this approach presumably is that requiring accurate routing information and related data in message headers makes it easier both to block or filter spam and to trace it for the purpose of complaining to spammers' service providers.[254]

The use of misleading subject lines is prohibited in some states for similar reasons.[255] Misleading subject lines such as "RE: your message" are used by spammers to induce recipients to read spam rather than discarding it unread, and prohibiting this practice could make manual filtering slightly easier.

Labeling of commercial messages seems to be a much more direct means of enabling recipients and destination operators to filter

[253] *See, e.g.*, Illinois Electronic Mail Act, 815 ILL. COMP. STAT. ANN. 511/10(a)(i) (West Supp. 2000)); IOWA CODE ANN. § 714E.1(2)(b) (West Supp. 2000); LA. REV. STAT. ANN. § 14:73.6(B) (West Supp. 2000); N.C. GEN. STAT. § 14-458(a)(6) (1999); R.I. GEN. LAWS § 11-52-4.1(7) (Supp. 1999); VA. CODE ANN. § 18.2-152.4(A)(7) (Michie Supp. 2000); WASH. REV. CODE ANN. § 19.190.020(1)(a) (West Supp. 2001); W. VA. CODE ANN. § 46A-6G-2(1) (Michie 1999); Colorado Junk Email Law, ch. 388, § 1, 2000 Colo. Sess. Laws 2031, 2032 (to be codified at COLO. REV. STAT. § 6-2.5-103(1)–(3)); Act of June 23, 1999, No. 99-160, § 1(b)(7), 1999 Conn. Acts 446, 449; Act of July 2, 1999, ch. 135, § 1, 72 Del. Laws 7, 8 (1999) (to be codified at DEL. CODE tit. 11, § 937(b)); Act of Apr. 17, 2000, ch. 423, § 1, 2000 Idaho Sess. Laws 1373, 1373–74 (to be codified at IDAHO CODE § 48-603E(3)); Act of June 8, 1999, ch. 337, § 1, 1999 Okla. Sess. Laws 1515, 1515 (to be codified at OKLA. STAT. tit. 15, § 776.1(A)); *see also* Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2000, S. 2542, 106th Cong. § 4(c); Inbox Privacy Act of 1999, S. 759, 106th Cong. § 2(e); E-Mail User Protection Act, H.R. 1910, 106th Cong. § 2(a)(2) (1999); Internet Freedom Act, H.R. 1686, 106th Cong. § 104(1) (1999) (amending 18 U.S.C. § 1030(a)(5)).

[254] In addition, some jurisdictions specifically prohibit the use of unrelated third parties' domain names or other information in message headers. *See, e.g.*, Illinois Electronic Mail Act, 815 ILL. COMP. STAT. ANN. 511/10(a)(i) (West Supp. 2000)); IOWA CODE ANN. § 714E.1(2)(a) (West Supp. 2000); R.I. GEN. LAWS § 6-47-2(d) (Supp. 1999); WASH. REV. CODE ANN. § 19.190.020(1)(a) (West Supp. 2001); W. VA. CODE ANN. § 46A-6G-2(1) (Michie 1999); Colorado Junk Email Law, ch. 388, § 1, 2000 Colo. Sess. Laws 2031, 2032 (to be codified at COLO. REV. STAT. § 6-2.5-103(3)); Act of Apr. 17, 2000, ch. 423, § 1, 2000 Idaho Sess. Laws 1373, 1373 (to be codified at IDAHO CODE § 48-603E(3)(a)); *see also* Can Spam Act, H.R. 2162, 106th Cong. § 3 (1999).

[255] *See, e.g.*, Illinois Electronic Mail Act, 815 ILL. COMP. STAT. ANN. 511/10(a)(i) (West Supp. 2000)); WASH. REV. CODE ANN. § 19.190.020(1)(b) (West Supp. 2001); W. VA. CODE ANN. § 46A-6G-2(2) (Michie 1999); *see also* Netizens Protection Act of 1999, H.R. 3024, 106th Cong. § 2(a)(3)(B). West Virginia's law also contains an additional content-based restriction: unsolicited bulk e-mail messages may not contain "sexually explicit materials." *See* W. VA. CODE ANN. § 46A-6G-2(4) (1999).

spam,[256] and a few jurisdictions have already adopted labeling requirements. Nevada, the first state to enact a spam law, requires merely that unsolicited commercial e-mail messages must be "readily identifiable" as such,[257] but at least two other states require that the advertising label "ADV:" appear at the beginning of the subject line in such messages.[258] Some states even require more specific labels for unsolicited messages with sexually explicit content.[259]

5. Other Statutory Provisions

Finally, some jurisdictions impose other sorts of statutory restrictions on spam-related practices. For example, many states prohibit the sale or distribution of software that is designed to facilitate the falsifycation of routing information in e-mail message headers, enabling spammers to cover their tracks.[260] Data protection laws in some coun-

[256] *See* Lessig & Resnick, *supra* note 93, at 424, 427–28.

[257] *See* NEV. REV. STAT. ANN. § 41.730(1)(c) (Michie Supp. 1999); *see also* Unsolicited Commercial Electronic Mail Act of 2000, H.R. 3113, 106th Cong. § 5(a)(3)(A) (requiring that UCE be clearly and conspicuously identifiable as such).

[258] *See, e.g.*, CAL. BUS. & PROF. CODE § 17538.4(g) (Deering Supp. 2000); TENN. CODE ANN. § 47-18-2501(c) (Supp. 1999); Colorado Junk Email Law, ch. 388, § 1, 2000 Colo. Sess. Laws 2031, 2032–33 (to be codified at COLO. REV. STAT. § 6-2.5-103(4)).

[259] *See, e.g.*, CAL. BUS. & PROF. CODE § 17538.4(g) (Deering Supp. 2000) (requiring "ADV:ADLT" at beginning of subject line in messages advertising material available only to adults); TENN. CODE ANN. § 47-18-2501(e) (Supp. 1999) (same as California statute); Act of June 13, 2000, No. 25, §1, 2000 Pa. Legis. Serv. 91, 93 (to be codified at 18 PA. CONS. STAT. 5903(a.1)) (requiring "ADV-ADULT" at beginning of subject line in advertising messages containing explicit sexual materials).

[260] *See, e.g.*, 720 ILL. COMP. STAT. ANN. 5/16D-3(a-5) (West Supp. 2000); LA. REV. STAT. ANN. § 14:73.6(B) (West Supp. 2000); R.I. GEN. LAWS § 11-52-4.1(8) (Supp. 1999); TENN. CODE ANN. § 47-18-2501(g) (Supp. 1999); VA. CODE ANN. § 152.4(B) (Michie Supp. 2000); W. VA. CODE ANN. § 46A-6G-4 (Michie 1999); Act of June 23, 1999, No. 99-160, § 1(c), 1999 Conn. Acts 446, 449; Act of July 2, 1999, ch. 135, § 1, 72 Del. Laws 7, 8 (1999) (to be codified at DEL. CODE tit. 11, § 937(c)); Act of June 8, 1999, ch. 337, § 1, 1999 Okla. Sess. Laws 1515, 1516 (to be codified at OKLA. STAT. tit. 15, § 776.1(E)); *see also* Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2000, S. 2542, 106th Cong. § 4(d); E-Mail User Protection Act, H.R. 1910, 106th Cong. § 2(a)(4) (1999); Internet Freedom Act, H.R. 1686, 106th Cong. § 104(1) (1999) (amending 18 U.S.C. § 1030(a)(5)). The software regulated by these statutes is commonly known as "spamware." While "spamware" describes a broad range of programs intended for use in sending unsolicited bulk e-mail, *see* Nick Nicholas, *Spamware Defined*, *at* http://mail-abuse.org/rbl/spamware.htm (last modified Feb. 2, 2000), the statutes that regulate such software tend to be relatively narrow in scope. *See, e.g.*, VA. CODE ANN. § 152.4(B):

> It shall be unlawful for any person knowingly to sell, give or otherwise distribute or possess with the intent to sell, give or distribute software which (i) is primarily designed or produced for the purpose of facilitating or enabling the falsification of electronic mail transmission information or other routing information; (ii) has only limited commercially significant purpose or use other than to facilitate or enable the falsification of electronic mail transmission information or other rout-

tries regulate the collection, use, and transfer of personal information that may include e-mail addresses,[261] and legislation has been proposed in the United States Congress to restrict the ability of spammers to harvest e-mail addresses from domain name registration records.[262]

Many ISPs attempt to block incoming spam, in part because Internet users tend to blame their own ISP for spam that they receive.[263] Many of the enacted and proposed laws explicitly permit destination operators and ISPs to block spam,[264] and there have even been proposals to require ISPs to offer spam-filtering services to their subscribers, or to solicit and record their subscribers' preferences with regard to receiving unsolicited messages.[265]

6. Enforcement Mechanisms

A variety of enforcement mechanisms appear in spam-related legislation. Many statutes confer a civil right of action upon individuals or destination operators who receive unsolicited e-mail messages that violate statutory requirements or who are injured as a result of receiving such messages. Because it is generally difficult to measure and prove actual damages—and probably because actual damages are likely to be quite small—many of these laws provide for liquidated or statutory damages in lieu of actual damages.[266] Several jurisdictions provide for

> ing information; or (iii) is marketed by that person or another acting in concert with that person with that person's knowledge for use in facilitating or enabling the falsification of electronic mail transmission information or other routing information.

See id.

[261] *See, e.g.*, Personal Information Protection and Electronic Documents Act, Bill No. C-6 (2000) (Can.), http://www.privcom.gc.ca/english/02_06_e.htm (enacted Apr. 13, 2000); *see also supra* Part IV.B.1 and accompanying notes (discussing European legislation aimed at prohibition of spam).

[262] *See, e.g.*, Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2000, S. 2542, 106th Cong. § 6(a).

[263] *See* Gartner Group, *supra* note 11, at 8.

[264] *See, e.g.*, 815 ILL. COMP. STAT. ANN. 511/10(f), (g) (West Supp. 2000); IOWA CODE ANN. § 714E.1(6)(b) (West Supp. 2000); LA. REV. STAT. ANN. § 14:73.6(D) (West Supp. 2000); VA. CODE ANN. § 18.2-152.4(D) (Michie Supp. 2000); WASH. REV. CODE ANN. § 19.190.050 (West 1999); W. VA. CODE ANN. § 46A-6G-3 (Michie 1999); Colorado Junk Email Law, ch. 388, § 1, 2000 Colo. Sess. Laws 2031, 2034 (to be codified at COLO. REV. STAT. § 6-2.5-104(5)); Act of June 23, 1999, No. 99-160, § 1(e), 1999 Conn. Acts 446, 449; Act of Apr. 17, 2000, ch. 423, § 1, 2000 Idaho Sess. Laws 1373, 1374 (to be codified at IDAHO CODE § 48-603E(6)); Act of June 27, 2000, ch. 763, § A, 2000 Mo. Laws 735, 749 (to be codified at MO. REV. STAT. § 407.1340).

[265] *See* Inbox Privacy Act of 1999, S. 759, 106th Cong. § 2(c)(3)(C).

[266] *See, e.g.*, CAL. BUS. & PROF. CODE § 17538.45(f) (Deering Supp. 2000) (an e-mail service provider whose UCE policy is violated may recover actual monetary losses or liquidated damages of $50 per message, up to a maximum of $25,000 per day, plus attorney's

criminal penalties or other governmental enforcement mechanisms in addition to or in place of private actions.[267]

fees); 720 ILL. COMP. STAT. ANN. 5/16D-3(b)(4), (5) (West Supp. 2000) (same as Connecticut statute); 815 ILL. COMP. STAT. ANN. 511/10(c), (d) (West Supp. 2000) (an injured person may recover actual damages or $10 per message, up to a maximum of $25,000 per day, plus attorney's fees); IOWA CODE ANN. § 714E.1(3)(a), (3)(b), (4) (West Supp. 2000) (an e-mail service provider may recover actual damages, $10 per message, or $25,000, plus attorney's fees; any other injured person may recover actual damages, $10 per message, or $500, plus attorney's fees; a recipient may also seek injunctive relief); NEV. REV. STAT. ANN. § 41.730(2) (Michie Supp. 1999) (a recipient may recover actual damages or $10 per message, plus attorney's fees, and may seek injunctive relief); N.C. GEN. STAT. § 1-539.2A(a) (1999) (same as Connecticut statute); R.I. GEN. LAWS § 6-47-2(h) (Supp. 1999) (a recipient may recover $100 for each violation plus attorney's fees); R.I. GEN. LAWS § 11-52-6(a), (b), (c) (Supp. 1999) (an e-mail service provider may recover actual damages, $500 per message, or $25,000 per day, plus attorney's fees; any other injured person may recover actual damages or $500 per message, up to a maximum of $25,000 per day, plus attorney's fees; punitive damages may also be available); TENN. CODE ANN. § 47-18-2501(i) (Supp. 1999) (an e-mail service provider may recover actual damages, $10 per message, or $5000 per day, plus attorney's fees; any other injured person may recover actual damages or $10 per message, up to a maximum of $5000 per day, plus attorney's fees); VA. CODE ANN. § 18.2-152.12(B), (C) (Michie Supp. 2000) (same as Connecticut statute); WASH. REV. CODE ANN. § 19.190.040 (West 1999) (same as Missouri statute); W. VA. CODE ANN. § 46A-6G-5(b), (c), (e) (Michie 1999) (an interactive service provider may recover actual damages, $10 per message, or $25,000 per day, plus attorney's fees; a recipient may recover actual damages or $1000, plus attorney's fees; punitive damages and injunctive relief may also be available); Colorado Junk Email Law, ch. 388, § 1, 2000 Colo. Sess. Laws 2031, 2033–34 (to be codified at COLO. REV. STAT. § 6-2.5-104) (a recipient or e-mail service provider may recover actual damages plus a civil penalty of $10 per message, plus attorney's fees); Act of June 23, 1999, No. 99-160, § 2(b),(c), 1999 Conn. Acts 446, 449–50 (an e-mail service provider may recover actual damages, $10 per message, or $25,000 per day, plus attorney's fees; any other injured person may recover actual damages or $10 per message, up to a maximum of $25,000 per day, plus attorney's fees); Act of Apr. 17, 2000, ch. 423, § 1, 2000 Idaho Sess. Laws 1373, 1374 (to be codified at IDAHO CODE § 48-603E(4)) (a recipient may recover actual damages, $100 per message, or $1000); Act of June 27, 2000, ch. 763, § A, 2000 Mo. Laws 735, 749 (to be codified at MO. REV. STAT. § 407.1330) (an interactive service provider may recover actual damages or $1000; a recipient may recover actual damages or $500); Act of June 8, 1999, ch. 337, § 2, 1999 Okla. Sess. Laws 1515, 1516 (to be codified at OKLA. STAT. tit. 15, § 776.2(B), (C)) (same as Connecticut statute).

[267] *See, e.g.*, CAL. PENAL CODE § 502(d)(4) (Deering Supp. 2000) (violation may be punishable by fine, imprisonment, or both); 720 ILL. COMP. STAT. ANN. 5/16D-3(a-5), (b)(1) (West Supp. 2000) (defining offense of computer tampering, a misdemeanor); IOWA CODE ANN. § 714E.2 (West Supp. 2000) (authorizing attorney general to seek injunctive relief and civil penalties, and to bring action for damages for the benefit of injured consumers); LA. REV. STAT. ANN. § 14:73.6(C) (West Supp. 2000) (violation punishable by fine of not more than $5000); N.C. GEN. STAT. § 14-458(b) (1999) (violation constitutes computer trespass, a misdemeanor or felony, depending upon extent of damage); TENN. CODE ANN. § 47-18-1604 (1995) (violation punishable by civil penalty of $100); VA. CODE ANN. § 18.2-152.4(C) (Michie Supp. 2000) (violation constitutes computer trespass, a misdemeanor or felony, depending upon intent and injury); Act of June 23, 1999, No. 99-160, § 1(d), 1999 Conn. Acts 446, 449 (violation constitutes a misdemeanor or felony, depending upon intent and injury); Act of June 23, 1999, No. 99-160, § 3, 1999 Conn. Acts 446, 450 (authorizing attorney general to bring action for damages for benefit of injured pri-

C. Limitations of Legal Approaches

Lawsuits and targeted legislation can ameliorate the spam problem by imposing costs and other disincentives on spammers, but it is very unlikely that legal approaches alone will be successful in eradicating spam.

1. Enforcement Problems

Jurisdictional barriers, together with practical issues of enforcement and circumvention, are probably the most significant limitations of legal responses to spam. Unlike most other forms of communication, electronic mail generally is unaffected by state and even national boundaries.[268] Furthermore, many e-mail addresses provide no indication of the addressee's physical location, and even an e-mail address that does include a geographic identifier frequently can be used from anywhere in the world.[269] Some spam-related laws include specific jurisdictional provisions—for example, providing that a state can exert long-arm jurisdiction over a person who sends e-mail into the state or uses a server located in the state.[270] But even if such an exercise of

vate parties); Act of July 2, 1999, ch. 135, § 1, 72 Del. Laws 7, 7–9 (1999) (to be codified at DEL. CODE tit. 11, §§ 937, 938) (defining crimes of "un-requested or unauthorized electronic mail" and "failure to promptly cease electronic communication upon request"); Act of June 8, 1999, ch. 337, § 1, 1999 Okla. Sess. Laws 1515, 1515 (to be codified at OKLA. STAT. tit. 15, § 776.1(B)) (violation punishable by civil penalty of up to $500); Act of June 13, 2000, No. 25, §1, 2000 Pa. Legis. Serv. 91, 93 (amending 18 PA. CONS. STAT. § 5903(h) and to be codified at 18 PA. CONS. STAT. § 5903(l)) (violation constitutes a misdemeanor or felony, with additional fine or imprisonment for attempt to evade prosecution).

[268] A fax marketer operating from offshore in order to evade a country's laws would likely sustain substantial long distance telephone charges; international telemarketing and direct mail are similarly subject to higher costs than domestic communications (although at least in the case of telemarketing, these costs may be offset by lower labor costs). The already negligible marginal cost of e-mail communications, on the other hand, is normally entirely independent of the physical locations of the sender and the recipient. National laws regulating unsolicited faxes and other forms of telephone and direct mail marketing are thus more likely to be effective than those regulating unsolicited e-mail.

[269] It can be difficult or impossible to determine where a particular message originated (even if the sender's e-mail address appears in the message), and a sender generally cannot determine the location of a recipient if the only information he or she has is the recipient's e-mail address.

[270] *See, e.g.*, CAL. BUS. & PROF. CODE § 17538.4(d) (Deering Supp. 2000); 815 ILL. COMP. STAT. ANN. 511/10(b) (West Supp. 1999); IOWA CODE ANN. § 714E.1(5) (West Supp. 2000); N.C. GEN. STAT. § 1-75.4(4)(c) (1999); R.I. GEN. LAWS § 6-47-2(a), (d), (g) (Supp. 1999); TENN. CODE ANN. § 47-18-2501(f) (Supp. 1999); VA. CODE ANN. § 8.01-328.1(B) (Michie 2000); WASH. REV. CODE ANN. § 19.190.020(1), (2) (West Supp. 2001); W. VA. CODE ANN. §§ 46A-6G-2, -5(d) (Michie 1999); Colorado Junk Email Law, ch. 388, § 1, 2000 Colo. Sess. Laws 2031, 2034 (to be codified at COLO. REV. STAT. § 6-2.5-105); Act of June 23, 1999, No. 99-160, § 4, 1999 Conn. Acts 446, 450 (amending CONN. GEN. STAT. § 52-59b(a)); Act of July 2, 1999, ch. 135, § 1, 72 Del. Laws 7, 8 (1999) (to be

jurisdiction comports with constitutional requirements,[271] it may be difficult to locate and subsequently to enforce a judgment on someone in another state or country. Indeed, it is certainly conceivable that spammers will begin making use of "spam havens"[272]—jurisdictions with spam-friendly laws—just as many spammers now use "bulk-friendly" ISPs.[273] Legislation may fare somewhat better at addressing spamming by legitimate mainstream businesses, particularly brick-and-mortar companies seeking to communicate with potential customers in their own geographic area, but this type of advertising probably represents only a very small proportion of present-day spam.

2. Lack of Uniformity

Linking spam rules to legal jurisdictions has another potential drawback: an inevitable lack of uniformity. Perhaps the best example to date is in the two conflicting labeling schemes that have been enacted by various states. Under Pennsylvania law, it is a misdemeanor to send an e-mail message containing "explicit sexual materials" unless the first nine characters in the subject line are "ADV-ADULT"[274]; but the laws of California and Tennessee require messages intended only for adults to contain "ADV:ADLT" as the first eight characters in the

codified at DEL. CODE tit. 11, § 937(d)); Act of June 8, 1999, ch. 337, § 3, 1999 Okla. Sess. Laws 1515, 1516–17 (to be codified at OKLA. STAT. tit. 15, § 776.3).

[271] While sending a single e-mail message into a jurisdiction probably is insufficient to subject the sender to long-arm jurisdiction, a spammer who sends hundreds or thousands of unsolicited messages into a state may well have sufficient contacts with the state to support personal jurisdiction. *See, e.g.*, Cybersell, Inc. v. Cybersell, Inc., 130 F.3d 414, 415 (9th Cir. 1997) (finding no jurisdiction over non-resident defendant who maintained a passive web page advertising its services); Cody v. Ward, 954 F. Supp. 43 (D. Conn. 1997) (finding jurisdiction over a non-resident defendant who made fraudulent representation to plaintiff in Connecticut via phone and e-mail); EDIAS Software Int'l L.L.C. v. BASIS Int'l Ltd., 947 F. Supp. 413 (D. Ariz. 1996) (finding jurisdiction over non-resident defendant based on substantial contacts with Arizona, including contact via phone, fax and e-mail).

[272] *See* Lessig & Resnick, *supra* note 93, at 428. Interestingly, an offshore data haven that announced its launch in mid-2000 claimed it would serve as a sanctuary for anything but spamming and child pornography—at least in the case of spamming, apparently because of the company's fear of technical rather than legal reprisals. *See* HavenCo, *Acceptable Use Policy*, *at* http://www.havenco.com/legal/aup.html (last modified June 2, 2000); Declan McCullagh, *A Data Sanctuary Is Born*, WIRED NEWS, June 4, 2000, *at* http://www.wired.com/news/business/0,1367,36749,00.html.

[273] *See Internet Spam Industry FAQ, ver. 1.0, at* http://world.std.com/FAQ/Internet/abuse/Spam-Industry-FAQ.txt (Jan. 21, 1998); *The Spamhaus Project*, *at* http://www.spamhaus.org/ (last visited Aug. 8, 2000).

[274] *See* Act of June 13, 2000, No. 25, §1, 2000 Pa. Legis. Serv. 91, 93 (to be codified at 18 PA. CONS. STAT. § 5903(a.1)).

subject line.[275] One solution is to incorporate some sort of "Internet standards" by reference in a statute,[276] but this approach raises problems of notice and accountability, among others.

3. Narrow Approach

A lack of flexibility is another problem with legislative attempts to curtail spam. The war between spammers and anti-spammers has frequently been described as an arms race,[277] with each side constantly developing new weapons. A statute that attempts to incorporate these weapons—for example, a particular labeling method or opt-out system—is likely to be obsolete before it takes effect because of the rapid advancement in technology. On the other hand, while the application of existing common law theories to spam provides a degree of flexibility that is not available in highly targeted legislation, the unintended consequences that may result from stretching the law in such a manner may outweigh the benefits of avoiding legislation.[278]

4. Legitimization of Spam

Another objection to legislative approaches is that a partial solution, one that regulates spam without prohibiting it altogether, will merely serve to legitimize spam. For example, if the law requires spam to be labeled and to include opt-out instructions, the stigma presently attached to spam will begin to disappear. Although it will be easier and less costly to filter out or delete each individual piece of spam, the overall volume of spam will likely increase exponentially as more

[275] *See* CAL. BUS. & PROF. CODE § 17538.4(g) (Deering Supp. 2000); TENN. CODE ANN. § 47-18-2501(e) (Supp. 1999).

[276] *See, e.g.*, Unsolicited Commercial Electronic Mail Act of 2000, H.R. 3113, 106th Cong. § 5(b)(2)(B)(ii) (permitting a provider's notice of its UCE policy to be published "in accordance with a technological standard adopted by an appropriate Internet standards setting body (such as the Internet Engineering Task Force) and recognized by the [FTC] by rule as a fair standard").

[277] *See, e.g.*, Cranor & LaMacchia, *supra* note 9, at 79; John Markoff, *Internet Is Expanding Arms Race with Junk E-Mail*, N.Y. TIMES, Mar. 17, 1998, at D1; Barry D. Bowen, *Controlling Unsolicited Bulk E-Mail*, SUNWORLD, Aug. 1997, *at* http://www.sunworld.com/swol-08-1997/swol-08-junkemail.html; Eamonn Sullivan, *The "Star Wars" Phase of Anti-Spam Tools*, PC WK., Mar. 13, 1998, http://www.zdnet.com/zdnn/content/pcwk/1511/293774.html.

[278] *See* Burk, *supra* note 162, at 54–55 (criticizing application of the trespass to chattels doctrine to spam cases, and referring to "a sort of legal mission creep that allows a common law doctrine to mutate from the cure for an isolated problem to the pathology in a broad body of caselaw").

mainstream businesses begin to use it, and the aggregate costs that spam imposes may well increase.[279]

5. Constitutional Concerns

Finally, a very real problem with legislative responses to spam is that an effective anti-spam statute is likely to be challenged on constitutional grounds. For example, state courts in California and Washington have held those states' anti-spam statutes unconstitutional under the Commerce Clause because they place a burden on interstate commerce.[280] And despite the fact that most spam is commercial speech, many commentators and advocates have raised First Amendment objections to governmental regulation of spam.[281]

Conclusion

Neither technical measures nor legal approaches have succeeded in eliminating spam, and self-regulation and other informal efforts have fared even worse. Technical responses to spam have been largely ineffectual and impose substantial costs that ultimately are passed on to Internet users, while frequently interfering with legitimate communications. Lawsuits may have driven a few spammers out of business, but they rarely afford an adequate remedy and have done little to change spammers' behavior. No jurisdiction has yet enacted truly comprehensive anti-spam legislation, but it seems unlikely that even well-drafted legislation will be capable of solving the problem.

[279] *See* discussion *supra* note 86 (discussing self-regulation and stigma). Political realities make it especially likely that such a counterproductive partial solution may result from the legislative process, as has occurred in Nevada and elsewhere. *See, e.g.*, Mark Grossman, *Spam: A Tasteless Part of Cyberspace*, LEGAL TIMES, Nov. 24, 1997, LEXIS, News Library, Legal Times File (describing Nevada spam law as "watered-down"); Peter Lewis, *Locke Signs "Spam" Bill to Reduce Junk E-Mail*, SEATTLE TIMES, Mar. 26, 1998, 1998 WL 3145243 (quoting California attorney David Kramer calling Nevada's spam law "worse than no law at all").

[280] *See* Ferguson v. Friendfinder, No. 307309 (Cal. Super. Ct. June 2, 2000) (order sustaining defendant's demurrer without leave to amend) (finding CAL. BUS. & PROF. CODE § 17538.4 unconstitutional); State v. Heskel, No. 98-2-25480-7 SEA (Wash. Super. Ct. Mar. 10, 2000) (order granting defendant's summary judgment) (finding the Washington spam law, found at WASH. REV. CODE §§ 19.190.020, .030, unconstitutional), http://www.wa-state-resident.com/agheck02.htm. The Louisiana spam law has also been challenged, although the case was dismissed on procedural grounds. *See* Fox v. Reed, No. 99-3094, 2000 U.S. Dist. LEXIS 3318 (E.D. La. Mar. 16, 2000) (dismissing case raising various constitutional challenges to LA. REV. STAT. § 14:73.6 based on plaintiff's lack of standing).

[281] *See Developments*, *supra* note 37, at 1622–34 (discussing First Amendment objections to application of common-law trespass doctrine to unsolicited noncommercial e-mail); authorities cited *supra* note 2.

The responses to spam that have been implemented to date have done little more than heighten the level of uncertainty that surrounds spam. Internet users flock from one ISP to another in attempts to escape spam, and this churn squeezes profitability for ISPs.[282] Responsible marketers for the most part are trying to avoid even the appearance of spam, but they face challenges in deciding when it is appropriate to use e-mail even when communicating with existing customers.[283]

Coordination of technical and legal mechanisms seems to be the most promising approach to the spam problem. The first step must be to agree upon the ultimate objective: it is quite easy to declare "get rid of spam," but the definition of spam is sufficiently controversial that this first step may be the most difficult.[284] Technical and legal measures can then be used in a complementary fashion—for example, technical measures can be designed so that one must break the law (or subject oneself to liability) in order to circumvent them,[285] while those who evade or ignore legal controls could be subjected to blackholing and other technical responses.

Yet it is probably unrealistic to expect that the consensus required for such coordination can be achieved. More likely, the technical arms race between spammers and anti-spammers will escalate, and more and more innocent bystanders will be caught in the crossfire. States and countries will continue enacting an increasingly diverse set of spam-related statutes, and traditional legal theories will be stretched and distorted even further in efforts to address spam and other forms of "network abuse." The news is not all bad; there have been advances in collaborative filtering by companies such as Brightmail, and some recent legislation seems to incorporate at least a rough comprehension of the underlying technology. Nonetheless, a coordinated solution to the problem of spam remains elusive at best.

[282] *See* Gartner Group, *supra* note 11, at 8, 11.

[283] *See, e.g.*, Elizabeth Weise, *Spamming by the Book Is Still Junk from "the Slime Pit,"* USA TODAY, Nov. 3, 1999, at 5D.

[284] *See supra* Part I.A.

[285] See, for example, the discussion of a "not spam" labeling protocol, *supra* note 93.