VIRGINIA JOURNAL OF LAW & TECHNOLOGY

SPRING 2005	UNIVERSITY OF VIRGINIA	VOL. 10, NO. 5

Solving the Inbox Paradox:
An Information-Based Policy Approach to Unsolicited E-mail Advertising

DEREK E. BAMBAUER†

ABSTRACT

Unsolicited commercial e-mail continues to challenge users, Internet service providers, and other stakeholders despite regulatory interventions aimed at eliminating it. This Paper argues that these issues persist because spam is, fundamentally, an information phenomenon, yet current regulatory efforts fail to analyze it in its complexity. Because some consumers find the information in spam relevant and in some cases even sufficiently valuable to make purchases based on it, regulators must account for this value or risk undercutting their own efforts. The Paper proposes an information-based analytical framework, and evaluates the technological characteristics of the e-mail channel and the informational characteristics of unsolicited advertising. By suggesting a more nuanced approach to spam, it moves beyond the standard assumptions of the debate to propose key goals for regulation and four alternatives for preserving information value while curbing spam's abuses. The Article offers a new model to analyze the policy goals and constraints for information in a networked environment, focusing on spam to make the approach concrete and relevant to all readers. Spam affects nearly every Internet user; this Paper seeks to change how we think about its problems as a first step in reform.

† Fellow, Berkman Center for Internet & Society, Harvard Law School. J.D., Harvard Law School, 2004. A.B., Harvard College, 1996. The author welcomes comments via e-mail at dbambaue@cyber.law.harvard.edu.

TABLE OF CONTENTS

I. INTRODUCTION[1]

¶ 1 Everyone hates spam, but some people buy from it. This contradiction highlights the legal policy challenge of unsolicited e-mail advertising—namely, how to preserve its benefits while stanching the deluge of useless messages in users' inboxes. Spam is a misunderstood phenomenon, and this confusion hampers reform efforts. Fundamentally, spam is an information problem:[2] unsolicited advertising provides value to some Internet users, but it is too often fraudulent,[3] poorly targeted, and offensive.[4] Accordingly, this Paper examines spam from an information-based perspective. It elucidates shortcomings of current theoretical and practical approaches to spam's problems, and then offers a new analytical framework that suggests different methods for reform.

¶ 2 This analysis incorporates two key insights. First, it considers the relevant information in the context of its medium: Internet e-mail's architecture makes untargeted mass advertising inexpensive and difficult to prevent. Second, it recognizes that spam works—it provides value to some recipients, who demonstrate this fact by responding to unsolicited e-mail ads with purchases.[5] Some unsolicited e-mail advertising provides

1. I thank Terry Fisher, Jonathan Zittrain, Urs Gasser, John Palfrey, Dan Hunter, Diane Cabell, Kara Zivin Bambauer, Thinh Nguyen, Mark Young, and the participants in the Harvard-Yale Cyberscholars Working Group for comments, suggestions, and critiques of drafts of this paper.

2. *See* Urs Gasser, *What is Information Law -- what could it be? in* INFORMATION LAW IN ENVIRONMENTS 7, 10 (Urs Gasser ed., 2002) ("Information Law is concerned with the legal apprehension of people's information relations, or to put it more precisely: the comprehensive regulation of subjective rights to information and their enforcement.").

3. *See* Press Release, Fed. Trade Comm'n, FTC Measures False Claims Inherent in Random Spam (Apr. 29, 2003), *at* http://www.ftc.gov/opa/2003/04/spamrpt.htm (finding that in a random sample of 1000 unsolicited commercial e-mail messages, 66% contained false information in the subject line, "From" information, or message text).

4. *See* Deborah Fallows, Pew Internet & American Life Project, *Spam: How It Is Hurting Email and Degrading Life on the Internet* 1, Oct. 22, 2003, *at* http://www.pewinternet.org/reports/toc.asp?Report=102 (finding 76% of surveyed users are "bothered by offensive or obscene content of spam").

5. *See id.* at 25 (reporting that "7% of [surveyed] emailers report that they have ordered a product or service that was offered in an unsolicited email" and that "[o]ne-third of emailers have pursued an offer in an unsolicited email by clicking on a link to find further information"); *see also* Jennifer Wolcott, *You Call it Spam, They Call it a Living*, THE CHRISTIAN SCIENCE MONITOR, Mar. 22, 2004, at 12 (estimating that 8% of recipients respond to spam); *cf.* Eric J. Sinrod, *Net Ads Are Hated, But They Work; Room for Improvement*, USA TODAY, Sept. 7, 2004, *available at* http://www.usatoday.com/tech/columnist/ericjsinrod/2004-09-07-sinrod_x.htm (citing a Ponemon Institute study finding that while 80% of surveyed users state that Internet pop-up ads "always annoy," 31% of respondents "responded to a product or promotional offer made from an Internet advertisement," and 7% made a purchase or used a particular service based on such an ad).

information valuable to some consumers, not only by providing them with an outlet for commerce, but by helping them satisfy and shape their consumption preferences. With these twin recognitions, an information-based perspective changes the policy focus from preventing spam (likely a difficult or impossible task) to improving it. In short, we seek to regulate spam to alter the information dynamic of unsolicited commercial e-mail.

¶ 3 This Paper begins by looking at the technical architecture of Internet e-mail, which creates opportunities for inexpensive advertising, focus points for exerting regulatory controls,[6] and challenges for policymakers trying to implement reforms. Next, it reviews current regulatory approaches and proposals using the four-part framework outlined by the New Chicago School. This section examines these regulatory methods' capabilities and drawbacks, and suggests that their approaches fail primarily because they misconstrue spam's problems. The next section proposes an information-based analytical scheme that clarifies spam's puzzle, and finally the Paper turns to reform proposals based on this model and its insights.

II. THE TECHNOLOGICAL CONTEXT OF SPAM

¶ 4 One must understand how Internet electronic mail works to understand why spam exists, the information problems it creates, and how it challenges regulation. E-mail was one of the earliest Internet applications;[7] originally, it contemplated users sending messages directly to each other's screens (a rudimentary "instant messaging" capability) in addition to each other's mailboxes.[8] Internet pioneer Jon Postel formalized the technical specifications for transferring e-mail with the Simple Mail Transfer Protocol (SMTP) in 1981.[9] The Internet Engineering Task Force (IETF)[10] adopted SMTP as one of its Requests for Comments (de facto standards for Internet applications) in RFC 821. Exploring SMTP helps explain spam's characteristics and introduces some technical targets for regulation.

A. SMTP

¶ 5 SMTP is an application protocol that relies on the TCP/IP-based Internet infrastructure.[11] An Internet e-mail exchange that conforms to SMTP's RFC 821 is often compared to a conversation[12] between two parties, the sender and the receiver (described

6. *See* Jonathan Zittrain, *Internet Points of Control*, 44 B.C. L. REV. 653, 656–59 (2003).
7. *See generally* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 102 (1999).
8. *See* Jonathan B. Postel, *RFC 821: Simple Mail Transfer Protocol*, § 3.4 (Aug. 1982), *available at* http://www.ietf.org/rfc/rfc0821.txt.
9. *Id.*
10. *See* Internet Engineering Task Force (IETF), *Overview of the IETF*, *at* http://www.ietf.org/overview.html (last visited Feb. 16, 2005).
11. *See* LESSIG, *supra* note 7, at 101–02.
12. *See, e.g.*, ALAN SCHWARTZ & SIMSON GARFINKEL, STOPPING SPAM, at 47, 50 (1998) (describing SMTP as an Internet "protocol [that] is a script for a structured conversation" and giving an example of "what the [SMTP] conversation looks like").

by RFC 821 as a "lock-step" exchange[13]). The sender has information (an e-mail message) it wants to transfer to the receiver. Simple Mail Transfer Protocol defines how the sender and receiver communicate to transfer this information—in essence, the protocol creates a set of conversational and grammatical rules for exchanging e-mail between computers.[14] The SMTP exchange is highly structured and ordered; when the sender makes a statement, the receiver must respond before the sender can "talk" (make another statement) again.[15] After each of the sender's statements, the receiver either accepts the information or rejects it with an error code that indicates the problem.[16] The SMTP conversation has the following steps:

¶ 6 1. Creating a connection—The sending computer contacts the receiving computer to establish a connection. To find out which computer should receive the e-mail, the sending computer examines the relevant message. An e-mail message contains addresses for one or more recipients; each address consists of a local part and a domain (in the form "<localpart@domain>").[17] The sending server's responsibility is to route the message to each recipient's domain; delivery to the user's mailbox is up to the computers in that domain. For each recipient, the sending server determines which computer can receive mail for their domain by consulting the Domain Name System (DNS).[18] (Most SMTP implementations support use of either A (address) or MX (mail exchange) DNS records to locate a domain's receiving computer.[19]) The sending computer retrieves one or more DNS records that list computers designated by a domain as able to receive e-mail for it; the records contain the IP address for each computer.[20] Next, the sending computer attempts to contact one of these computers at its IP address on TCP port 25.[21] If the

13. Postel, *supra* note 8, § 2 (stating that "[t]he dialog is purposely lock-step, one-at-a-time").

14. *See id.* RFC 2821 formally supersedes RFC 821. *See* J. Klensin, ed., *RFC 2821: Simple Mail Transfer Protocol* (Apr. 2001), *available at* http://www.ietf.org/rfc/rfc2821.txt. However, implementation of RFC 2821 in commercial e-mail products has been relatively slow. *See, e.g.*, IBM, *Fix List for Lotus Notes and Lotus Domino Release 5.0.10 Maintenance Release (MR)*, *available at* http://www-1.ibm.com/support/docview.wss?rs=0&q1=domino+2821&uid=swg27002754 (last modified Dec. 4, 2002) (noting that the Domino SMTP listener task now supports RFC2821).

15. Postel, *supra* note 8, § 2.

16. *Id.* §§ 4.2 (listing SMTP replies and stating that "[e]very command must generate exactly one reply") and 4.3 (noting the "communication between the sender and receiver is intended to be an alternating dialogue, controlled by the sender" where "the sender issues a command and the receiver responds with a reply" and the "sender must wait for this response before sending further commands").

17. *Id.* § 4.1.2.

18. *See* P. Mockapetris, *RFC 1035: Domain Names – Implementation and Specification*, §§ 2.2, 3.3.9 (Nov. 1987), *at* http://www.ietf.org/rfc/rfc1035.txt (explaining common DNS-host configuration and data structure for the MX record type).

19. *See id.*; *see also* R. Braden, ed., *RFC 1123: Requirements for Internet Hosts -- Application and Support* 48–49 (Oct. 1989), *available at* http://www.ietf.org/rfc/rfc1123.txt (requiring SMTP messages to have canonicalized domain names for senders and recipients, and defining canonicalized domain names as identifying a host directly (A record) or as an MX name).

20. *See, e.g.*, Lotus, *The Domain Name System (DNS) and SMTP Mail Routing*, *at* http://www-12.lotus.com/ldd/doc/domino_notes/Rnext/help6_admin.nsf/0/b775815941c92ddf85256c1d00394f23 (last visited Feb. 16, 2005) (describing how the Lotus Domino SMTP server retrieves and processes MX and A records to route e-mail).

21. IP addresses designate computers, while TCP ports designate applications on a computer. Conceptually, this is similar to mailbox numbers in an apartment building—the street (IP) address helps the postal service locate the building, and apartment numbers (TCP ports) ensure letters are delivered to the

receiving domain's computer accepts connections on port 25, it identifies itself as an SMTP service,[22] and the two computers establish a connection.

¶ 7 2. Establishing the SMTP conversation—The sending computer tells the receiving computer it wishes to communicate using SMTP by sending an initial statement with the SMTP statement "HELO" (or, for applications supporting extended SMTP commands, "EHLO") followed by an argument that is typically the sending server's fully-qualified domain name or IP address.[23] The receiving computer signals its willingness to begin the conversation by responding with an "OK" code.[24]

¶ 8 3. Defining the message sender—The sending server indicates an e-mail address for the message's sender with the statement "MAIL FROM" and an argument that gives the sender's address—for example, "MAIL FROM:<jdoe@law.harvard.edu>".[25] If the receiving computer accepts messages from this sender, it responds with an "OK" code.[26]

¶ 9 4. Defining the message recipients—The sending server specifies the recipient's address with the statement "RCPT TO" and an argument that gives the address—for example, "RCPT TO:<jsmith@fas.harvard.edu>".[27] If the receiving computer accepts messages for this recipient, it responds with an "OK" code.[28] Importantly, the sending server can indicate multiple recipients by using multiple "RCPT TO" statements at this stage. In other words, rather than transferring one message for each recipient, the sending server can transfer a single message with a list of recipients.[29] This efficiency

---

correct recipients. By default, a sending SMTP server contacts the receiving server on TCP port 25 at its IP address. Internet Assigned Numbers Authority, *Port Numbers*, *at* http://www.iana.org/assignments/port-numbers (last modified Feb. 8, 2005) (listing TCP and UDP ports 25 as well-known ports effectively reserved to SMTP). While software vendors, senders, or recipients are free to establish SMTP communications on other ports, the network effect of near-universal adoption of port 25 makes doing so impractical. *Cf.* J. Saltzer, D. Reed, & D. Clark, *End-to-End Arguments in System Design*, 2 ACM TRANSACTIONS IN COMPUTER SYSTEMS 277 (Nov. 1984), *available at* http://web.mit.edu/Saltzer/www/publications/endtoend/endtoend.pdf.

22. *See* Postel, *supra* note 8, § 3.5.

23. *See id.* ("In the HELO command the host sending the command identifies itself; the command may be interpreted as saying 'Hello, I am <domain>.'"). The purpose is "to ensure that the hosts are communicating with the hosts they think they are." *Id.* This initial statement tells the receiving computer who the sending computer is, or at least who it claims to be.

24. *See id.*; *see also id.* § 4.2.1 (defining the OK response as "220 <domain> Service ready").

25. *See id.* § 3.1. The "MAIL FROM" statement identifies the sender and provides a return e-mail address in case the receiving computer needs to send an error notification—for example, if the message cannot be delivered because the recipient's mailbox is full.

26. *See id.* (stating that if "accepted, the receiver-SMTP returns a 250 OK reply" in response to the MAIL FROM statement).

27. *See id.*

28. *See id.* (stating that if "accepted, the receiver-SMTP returns a 250 OK reply" in response to the RCPT TO command, but if "the recipient is unknown the receiver-SMTP returns a 550 Failure reply").

29. *See id.* (noting that the RCPT TO "step of the procedure can be repeated any number of times"). Thus, to transfer a message for multiple recipients, the sending computer would specify one recipient's address with a RCPT TO statement, wait for a response, and then specify the next recipient with another RCPT TO statement (repeating this process as needed). In practice, the number of recipients per message is limited by the size of the buffer in which the receiving computer stores recipient address information during the SMTP conversation. *See id.* § 4.5.3 (stating that the "maximum total number of recipients that must be buffered is 100").

makes sending e-mail, including spam, less expensive.

¶ 10 SMTP provides flexibility in specifying recipients, which in turn creates opportunities for concealing a message's origin. Today, most receiving servers accept messages only for recipients in "their" domains—a harvard.edu server, for example, will not accept messages for a recipient in another domain, such as yahoo.com. In the past, however, many servers accepted messages for recipients in other domains, forwarding the messages to their eventual destination. This "good neighbor" practice is known as SMTP relaying[30] and provides a haven for spam.[31] Relaying conceals a message's true origin, helping spammers evade filters and blacklists that try to block their e-mail. For example, assume servers in the domain spam.net send large volumes of spam messages. Internet Service Providers[32] ("ISPs") configure their SMTP servers not to accept mail from spam.net servers. However, the senders at spam.net discover that the SMTP server mail.harvard.edu supports relaying. They send all their messages (destined for various recipient domains) to the mail.harvard.edu server, which then forwards them to the relevant destinations. Since the messages appear to originate from the harvard.edu domain, the destination domains likely accept (at least initially) this e-mail from the mail.harvard.edu server, so the spam bypasses the blocks implemented for the spam.net domain.[33]

¶ 11 A server that supports SMTP relaying is quickly included on spam blacklists.[34] While administrators increasingly configure SMTP servers to prevent relaying, some viruses and worms take advantage of improperly secured computers to set up relays to send spam.[35] For example, broadband provider Comcast estimates that only 100 million of the 800 million daily messages on its network originate from the company's servers; the remaining 700 million come from compromised computers (known as "zombies")

30. *See id.* §§ 3.2 (forwarding) and 3.6 (relaying).

31. *See* Associated Press, *Your Computer Could Be a "Spam Zombie,"* CNN.COM, Feb. 18, 2004, *at* http://www.cnn.com/2004/tech/ptech/02/17/spam.zombies.ap/ (stating that "[open relays] are typically mail servers at ISPs . . . carelessly configured so that anyone on the Internet can send mail through them without needing a password" and noting that "[t]he relays make messages appear to have come from an ISP, not the spammer"); *see also* WEBOPEDIA, *Open Relay*, *at* http://www.webopedia.com/term/o/open_relay.html (last modified Dec. 2, 2003) (defining open relay as "an SMTP e-mail server that allows a third party to relay e-mail messages, i.e., sending and/or receiving e-mail that is not for or from a local user. . . . [A] downside of open relay technology is the proliferation of its usage by spammers looking to obscure or even hide the source of the large-volume e-mails they send").

32. For convenience, this paper uses the term "ISP" to denote any entity that receives e-mail on behalf of users; thus, traditional providers such as AOL and Earthlink are ISPs, as are companies that receive mail for employees, schools that receive mail for students, and government agencies that receive mail for officials.

33. The destination domains could still refuse to accept messages from a sender whose MAIL FROM domain includes spam.net, but spammers would likely use a false return address. Using this false address bypasses some spam filters and prevents angry recipients from retaliating against the true sender. *See* WEBOPEDIA, *Open Relay*, *supra* note 31.

34. *See, e.g.*, Spam-Blockers.com, *at* http://www.spam-blockers.com/spam-blacklists.htm.

35. *See, e.g.*, Symantec Security Response, *Backdoor.Hogle*, *at* http://securityresponse.symantec.com/avcenter/venc/data/backdoor.hogle.html (last modified Nov. 26, 2003) (describing a Trojan Horse that functions as "a proxy SMTP server that may be used as an anonymous spam relay").

used as relays by spammers.[36] Comcast found that blocking access to port 25 for computers sending suspiciously large volumes of e-mail reduced the amount of spam by twenty percent.[37] Thus, the receiving computer's decision to accept delivery for a given recipient (or, more accurately, a given Internet domain) has important consequences.

¶ 12 5. Transferring the message contents—Next, the sending computer prepares to transfer the message's contents with the statement "DATA."[38] If the receiving computer is ready to accept this data, it responds with a reply code.[39] After this reply, the sending computer transfers the contents (including the body, subject, date, and other relevant information), signaling the receiving computer when finished.[40] Once data transfer is complete, the receiving server normally returns an "OK" code and the conversation ends.[41] The sending computer can disconnect[42] or begin a new SMTP conversation for another message with the "MAIL FROM" statement.[43]

¶ 13 The rigid SMTP protocol is simple in content and requirements. It minimizes information that must be included in the exchange and leaves functions such as authentication to other protocols and applications.[44] This simple architecture makes SMTP easy to implement and use, but results in a number of problems.

B. Problems of E-mail Architecture

1. Trust

¶ 14 Spam takes advantage of the trust built into RFC 821.[45] SMTP defines how computers communicate to send and receive e-mail, but not whether they should do so. When two computers use SMTP to transfer e-mail, their default behavior is to accept

36. Jim Hu, *Comcast Takes Hard Line Against Spam*, CNET NEWS.COM, June 10, 2004, *at* http://news.com.com/2100-1038_3-5230615.html (describing the estimate from a Comcast engineer).

37. *See id*.

38. *See* Postel, *supra* note 8, § 3.1.

39. *See id*. (stating that if "accepted, the receiver-SMTP returns a 354 Intermediate reply and considers all succeeding lines to be the message text").

40. *See id*. (noting that "SMTP indicates the end of the mail data by sending a line containing only a period").

41. *See id*.

42. *See id*. § 3.5 (defining the "QUIT" command); *see also id*. § 4.1.1 (requiring that the receiving computer not close the connection after the "QUIT" command until it sends a reply, and that the sending computer not close the connection before issuing "QUIT" and receiving a reply).

43. *See id.* § 3.1 (noting that MAIL FROM "tells the SMTP-receiver that a new mail transaction is starting and to reset all its state tables and buffers, including any recipients or mail data").

44. Authentication between SMTP senders and receivers, and encryption of SMTP communications, are addressed through other protocols such as Transport Layer Security (TLS). *See* P. Hoffman, *SMTP Service Extension for Secure SMTP over Transport Layer Security* (Feb. 2002), *at* http://www.ietf.org/rfc/rfc3207.txt?number=3207 (defining "an extension to the SMTP . . . service that allows an SMTP server and client to use TLS (Transport Layer Security) to provide private, authenticated communication over the Internet").

45. *See* Paul Festa, *End of the road for SMTP?* CNET NEWS.COM, Aug. 1, 2003, *at* http://news.com.com/2100-1038-5058610.html?tag=nl (quoting the author of SMTP's predecessor standard as stating that Internet mail began in "a trusted situation" with relatively few senders and recipients, and the e-mail "protocols were developed on the basis of that trust").

each other's representations about which domain each signifies, who a message is from, and to whom it should be sent.[46] Spammers exploit this underlying trust to target recipients, hide their own identities, and conceal their tracks.

¶ 15 SMTP's trusting infrastructure is an historical artifact. When Jon Postel defined SMTP, the Internet consisted of a small group of connected computers whose users were almost exclusively military personnel or computer scientists at academic institutions.[47] In that small, relatively homogeneous community, norms worked well to control e-mail: unwanted messages could be regulated through social sanctions; context, familiarity, and technical expertise made falsification difficult; and the network's limited purpose provided little incentive to fake identity or routing path. E-mail standards incorporated the background assumptions inherent in this community and context.[48] As the community expanded, and as the Internet shifted from a strictly academic medium to a widely commercial one, assumptions of trust became increasingly untenable and risky. Like spyware, viruses, and denial of service attacks, spam exists because it can exploit both the implicit trusting model of Internet communications and the patchwork solutions intended to introduce greater caution.

2. Standards

¶ 16 Internet e-mail rests on a set of open standards; this reliance constitutes both a great strength and an inherent weakness of the medium. E-mail standards are defined and maintained by the IETF, a non-profit organization dedicated to creating universally accessible protocols for Internet uses.[49] Open standards reduce coordination costs for vendors and help assure interoperability—for example, a Lotus Domino SMTP server can transfer mail to a Microsoft Exchange SMTP server without incident since both implement RFC 821. A software company that wants to create a new e-mail server or client does not need to obtain a license for the core technologies involved. Electronic mail follows the classic pattern of network effects: as more people use e-mail, its value increases, since there are more potential recipients of communications and more information flowing through the system.[50] This in turn drives more people to communicate over e-mail, creating a positive feedback loop.

¶ 17 Spam, however, parasitizes this valuable e-mail characteristic. E-mail standards such as RFC 821 become relatively stable, inert "facts"—problems that the standards cause or fail to address are solved through adaptation (addressed through other

46. *Id.*; s*ee generally* Postel, *supra* note 8.

47. *See* Festa, *supra* note 45.

48. For example, SMTP assumes that recipients want messages—the default behavior is to accept connections and mail.

49. *See* IETF, *supra* note 10.

50. *See* Lawrence B. Solum & Minn Chung, *The Layers Principle: Internet Architecture and the Law*, 79 NOTRE DAME L. REV. 815, 833 (2004) (noting that the "value of an application like SMTP (e-mail) is a function, in part, of the number of adopters; the more users of e-mail, the more valuable it is. For some applications, there may be a tipping point, at which the number of adopters reaches critical mass resulting in a discontinuous and large increase in value from networking effects . . ."); *see also* STAN J. LIEBOWITZ, RE-THINKING THE NETWORK ECONOMY: THE TRUE FORCES THAT DRIVE THE DIGITAL MARKETPLACE 13 (Am. Mgmt. Ass'n 2002).

applications) rather than through modification of the standards themselves.[51] Standards lose flexibility in part because changes in standards must accommodate the "installed base" of systems that rely on and behave according to the current version.[52] This backwards compatibility issue affects all successful software and Internet technologies due to the changes not anticipated in earlier versions which risk disruption to existing users.[53]

¶ 18 Open-standards-based technology faces a second problem: it cannot compel adoption of changes. Proprietary vendors can force (gradually or immediately) users to move to newer versions that include the changes (a process known as migration, which aptly reflects the level of effort often involved). If Microsoft changes how its Windows operating system works, users will be compelled to accede to that change as Microsoft ends support for older versions and conditions added functionality on the new technology.[54] E-mail software, however, is produced by a large number of vendors who rely on the underlying standards. Migration becomes more difficult because vendors face a first-mover disadvantage: software versions implementing the changed standard may be incompatible with older versions, and users will not fully benefit from features in the changed standard until it is broadly adopted.[55] Thus, change requires vendor coordination—a process that imposes costs and delays.[56]

¶ 19 Thus far, e-mail software vendors have not sought to fix the spam problem within SMTP; rather, their solutions treat the protocol as a given. The IETF offers protocols that add security features to SMTP, but these have not been widely adopted.[57] Anti-spam proposals such as Caller-ID for E-mail and Sender Policy Framework (SPF) work through the DNS rather than changing SMTP.[58] The backwards-compatibility challenge

---

51. *See* LIEBOWITZ, *supra* note 50, at 33 (discussing coordination problems).

52. *See* Festa, *supra* note 45 (noting that "rewriting SMTP from the ground up would be prohibitively difficult because of the protocol's global user base, which is estimated to be in the hundreds of millions").

53. *See id*. (quoting the chair of the Anti-Spam Working Group for the Reseaux IP Europeans (RIPE), a consortium of European Internet service providers, as stating that the "difficulty of changing the transfer technology as a way of managing unsolicited bulk e-mail is the installed base"); *see generally* LIEBOWITZ, *supra* note 50, at 32–35.

54. *Cf. Windows 98 Support Ending*, CBSNEWS.COM, Dec. 13, 2003, *at* http://www.cbsnews.com/stories/2003/12/13/tech/main588381.shtml (describing Microsoft's plan to end support for its Windows 98 operating system and quoting a CBS News technology consultant as stating that "Microsoft is basically saying, 'Upgrade or you're out of luck'"). *But cf*. STUART MCCLURE ET AL., HACKING EXPOSED: NETWORK SECURITY SECRETS & SOLUTIONS 135, 434 (1999) (writing that "in a key concession to backward compatibility, Microsoft hamstrung the security of the SAM [Windows NT Security Accounts Manager] by using a hashing (one-way encryption) algorithm left over from NT's LanManager roots," pointing out that the "weaker LanManager hashing algorithm has been reverse-engineered," and noting that Windows 2000 also includes passwords hashed with the LanManager algorithm).

55. *Cf*. LESSIG, *supra* note 7 (discussing how server administrators are slow to update Sendmail versions unless they have a compelling reason to do so, such as a security scare).

56. A similar example is the transition from Internet Protocol version four to version six (IPv4 to IPv6). *See* Microsoft Corp., *IPv6 Transition Technologies* (November 12, 2002), *at* http://www.microsoft.com/windowsserver2003/techinfo/overview/ipv6coexist.mspx

57. *See* Hoffman, *supra* note 44.

58. *See infra* Section III.B.

and the need for widespread, if not universal, adoption of any solution, along with the notoriously slow pace of IETF processes, impede the effort to revise SMTP to help solve the spam problem.[59]

3. Cost

¶ 20 Senders use Internet mail's low cost and easy access to send information to recipients who have not requested it. This disclosure may increase the recipient's welfare if the information is valuable or decrease it if the data is fraudulent or useless. E-mail reverses the normal cost pattern of communication—sending is cheap relative to receiving.[60] Thus, advertisers enjoy a lower threshold level of revenue necessary to offset the cost of using e-mail. From a social welfare perspective, this means that senders (who choose the amount of communication) internalize relatively little of the total costs of unsolicited e-mail advertising; hence, they send much more e-mail than is optimal. The externality from e-mail advertising is thus relatively large.

¶ 21 E-mail creates low costs for a sender. An advertiser using e-mail faces the following costs:

- Hardware cost (computer workstation, SMTP server, etc.)
- Internet access (ISP fee, T1 lease, etc.)
- Acquisition of recipient addresses (creating an "opt-in" list, purchasing bulk lists)
- Composition of message contents (employee time, graphics software, etc.)
- Mechanism to capture revenue (Web site e-commerce functionality, phone number for orders, etc.)
- Risk (expected harm from civil or criminal liability, reputational costs, etc.)

¶ 22 Most of these costs are fixed (hardware, addresses, revenue capture) and others are generally low (Internet access, message creation). Thus, sending additional spam incurs trivial marginal costs. Even if marginal revenue is low, spammers have an incentive to send more messages to cover fixed initial investments. Thus, an advertiser who transmits spam tends to send a lot of it.

¶ 23 Recipients bear the majority of e-mail's costs for two reasons. First, most recipients receive e-mail through an ISP. ISPs unwittingly act as spam aggregation points—they receive spam for many users from many senders. Thus, ISPs pass the costs of processing this large e-mail volume on to recipients since there is currently no feasible way to charge senders. *USA Today* cites research estimating that end users pay an additional two dollars per month in ISP fees simply to cover spam costs.[61] Second, the

59. *See* Saul Hansell, *4 Big Internet Providers File Suits To Stop Leading Senders of Spam*, N.Y. TIMES, Mar. 11, 2004, at A1 (stating that many "spam experts argue that the single most effective method for reducing spam would be to modify the technical protocols used to send e-mail so that it would be easy to verify the identity of the sender of a message").

60. Contrast, for example, the investment required by senders of broadcast television or newspaper communications with the investment required by their recipients.

61. *As spam multiplies, so do its costs to consumers*, USA TODAY, Apr. 30, 2003, at 12A. The U.S. Senate cited this article in a report accompanying its version of CAN SPAM. S. Rep. No. 108–102 (2003).

architecture of Internet e-mail[62] generates a cost-multiplier effect for aggregators, such as ISPs, due to recipient processing. For example, if a spammer sends one message to 100 recipients at a particular ISP, he bears only the cost of one e-mail. The ISP accepts transfer of one message over SMTP, but then incurs the cost of delivering 100 e-mails—one to each recipient's mailbox.

¶ 24 Recipients typically bear the following costs:

- Hardware cost (personal computer for recipients, SMTP / POP[63] servers for ISPs, message storage such as hard drives or storage area networks, etc.)
- Internet access (T-3[64] lease for ISPs, ISP fee for users, etc.)
- Message processing or filtering (use of blacklists by ISPs, use of filters by ISPs or end users, time to read and delete messages by end users, risk of missing desired messages due to volume of unwanted ones, etc.)
- Risk (reputational costs for ISPs that deliver spam to their end users,[65] potential harm to end users from fraudulent messages (such as "phishing" ones[66]), etc.)
- Psychological effects on users, such as from viewing pornographic spam[67] or from the annoyance of managing large volumes of unwanted mail.[68]

¶ 25 Recipients, unlike senders, face non-trivial marginal costs for additional messages. ISPs in particular must devote considerable storage space, processing (by computers and personnel), and reputation investments to deal with spam. Users must download and then delete unwanted messages, and may open messages containing offensive material. As the spam volume increases, the risk of missing non-spam messages in one's inbox increases. Increasing marginal costs derive from two sources. First, SMTP makes delivery less efficient than transfer. Second, end users must determine which messages have value and which do not. This is a cost that senders (who know the content, purpose, and context of their messages) do not face.

---

62. *See supra* Section II.A.

63. Post Office Protocol (POP) defines a method of downloading e-mail messages from an ISP's server to a recipient's computer workstation. *See* J. Myers & M. Rose, *Post Office Protocol – Version 3* (May 1996), *at* http://www.ietf.org/rfc/rfc1939.txt?number=1939.

64. ISPs connect to Internet backbones via T-3 lines, which typically provide data transfer rates of 43 Mbps (megabits per second). *See* WEBOPEDIA, *T-3 carrier*, *at* http://www.webopedia.com/term/t/T_3_carrier.html (last modified Feb. 8, 2002).

65. Users tend to blame their ISP, in addition to the sender, for delivering spam to them. David E. Sorkin, *Technical and Legal Approaches to Unsolicited Electronic Mail*, 35 U.S.F. L. REV. 325, 378 n.263 (2001).

66. *See* WEBOPEDIA, *Phishing* (defining phishing as "[t]he act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft"), *at* http://www.webopedia.com/term/p/phishing.html; *see also* John Leyden, *Fear of phishing hits e-commerce*, REGISTER, May 5, 2004, *at* http://www.theregister.co.uk/2004/05/05/phishing_fears_survey/ (describing a study by software developer Cyota finding that 74% of online account holders "were less likely to shop online because of phishing").

67. *See* Fallows, *supra* note 4, at 29–31.

68. *Id*. at 24, 28.

4. Low Transaction Costs of E-mail Commerce

¶ 26 Advertising through e-mail has a medium-specific characteristic important to information analysis: the tight link in time, location, and transaction cost between the information conveyed (the ad) and the opportunity to act upon it (the transaction). Most e-mail clients enable users to click links embedded in messages, launching a Web browser program that loads the Web site indicated by the link's URL.[69] This makes reacting to advertising through e-mail cheap, fast, and easy—users can point, click, and buy. This speed offers both convenience and risk. E-mail messages and associated Web sites may lack or mimic context clues that make it harder for users to determine a product's true characteristics or quality—indeed, the practice of "phishing" for valuable personal data relies on users' willingness to interact with Internet forms that resemble those of legitimate banks or merchants.[70] This risk is increasingly real—research firm Gartner Group estimated in May 2004 that of adults in the United States, 57 million had received a phishing e-mail, 11 million had clicked on a link in a phishing message, and 1.8 million had disclosed personal information.[71] The Federal Deposit Insurance Corporation (FDIC) reported that nearly 2 million Internet users in the United States were victims of unauthorized bank account transfers between April 2003 and April 2004.[72] Phishers take advantage of low Internet transaction costs to create, and lure users to, Web sites that mimic legitimate e-commerce and financial sites, down to exact copies of corporate logos and falsified security measures such as the Secure Sockets Layer (SSL) encryption that protects online transactions.[73]

¶ 27 The minimal effort and cost of sharing personal information or entering into a commercial transaction online favor impulse buying and impede reflection or calculation. Other commercial media, by contrast, necessarily separate the advertising and point-of-sale contexts. Television commercials, catalogs, newspaper ads, and radio jingles all require consumers to switch to another medium to carry out a purchase (whether through a phone order, Web site, or retail store). This separation imposes both financial costs (phone charges, gas, etc.) and time costs (travel time, activating Internet access, opportunity cost, etc.). These costs, though, may have a hidden benefit: consumers gain time and space to reflect upon a decision before carrying it out. E-mail advertising

---

69. *See, e.g.*, Microsoft Corp., *OLEXP: How to Configure Outlook Express to Open Links in E-mail Messages in a New Browser Window*, *at* http://support.microsoft.com/default.aspx?scid=kb;en-us;256953 (last modified June 28, 2004); *see also* WEBOPEDIA, *URL*, *at* http://www.webopedia.com/term/u/url.html (last modified Jan. 8, 2004) (defining URL).

70. *See* Munir Kotadia, "*Phishing*" *Scams Luring More Users*, CNET NEWS.COM, Apr. 19, 2004, *at* http://news.com.com/2100-7355_3-5194807.html (noting that a company monitoring corporate e-mail traffic found 215,643 phishing e-mails by March 2004 and defining phishing as a scam where "unsuspecting users receive official-looking e-mails that attempt to fool them into disclosing online passwords, user names and other personal information," and where victims typically "click on a link that directs them to a doctored version of an organization's Web site").

71. Leslie Walker, *Internet Snagged In the Hooks of "Phishers*," WASH. POST, July 29, 2004, at E1.

72. Fed. Deposit Ins. Corp. (FDIC), *Putting an End to Account-Hijacking Identity Theft* 11 (Dec. 14, 2004), *at* http://www.fdic.gov/consumers/consumer/idtheftstudy/identity_theft.pdf.

73. *Id.*; *see* Citibank, *Learn About Spoofs*, *at* http://www.citibank.com/domain/spoof/learn.htm (last visited Sept. 13, 2004) (explaining how to detect phishing sites and messages, and describing Citibank's practices regarding e-mail communication).

provides easy impulse buying, with its concomitant benefits and risks. Thus, spam reduces transaction costs by combining product information with a purchase mechanism.

¶ 28 E-mail's standards-based architecture creates four challenges to controlling spam: overcoming built-in trust, dealing with standards resistant to change, managing an unusual cost structure, and addressing easy impulse buying by users. Next, we explore how current spam initiatives try, but fail, to overcome these problems.

III. CURRENT APPROACHES TO CONTROLLING SPAM

¶ 29 Current proposals and methods for controlling spam cover all four of the possible regulatory modalities envisioned by the New Chicago School: architecture, laws, markets, and norms.[74] However, these approaches do not solve the problem, and their lack of efficacy derives in large part from an imprecise understanding of spam's informational context. Thus, the New Chicago analytical schema and the proposed information-based framework operate at different levels. The four-part New Chicago taxonomy sets forth different techniques for controlling or regulating behavior. This model does not address whether regulation is appropriate or what goals it should seek to achieve; the information-based framework undertakes this level of analysis. This section briefly reviews the New Chicago schema and then examines major current regulatory initiatives and their respective capabilities and shortcomings.

A. Regulatory Framework

¶ 30 Lawrence Lessig divides methods of regulating behavior into four categories: laws, social norms, markets, and architecture.[75] This framework is known as the New Chicago approach.[76] These four modalities interact with and shape each other and, in total, constrain human behavior.[77] Legal regulation forbids or requires certain actions and enforces its dictates with ex post sanctions for disobedience.[78] Direct action—prescribing or proscribing behavior—can be supplemented with indirect effects created through laws altering the other modalities. For example, laws could forbid smoking (direct action) or impose a tax on cigarettes (indirect action that reduces demand through market price effects).[79] A "social norm is a 'rule that is neither promulgated by an official source, such as a court or a legislature, nor enforced by the threat of legal sanctions, yet is regularly complied with.'"[80] Social norms shape behavior through community sanctions;

74. *See* Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501, 507–10 (1999).

75. Lawrence Lessig, *The New Chicago School*, 27 J. LEGAL STUD. 661, 662–66 (1998).

76. *Id.* at 661.

77. *Id.* at 666 ("Norms might constrain, but law can affect norms (think of advertising campaigns); architecture might constrain, but law can alter architecture (think of building codes); and the market might constrain, but law constitutes and can modify the market (taxes, subsidy)."); *see* Lessig, *The Law of the Horse*, *supra* note 74, at 512.

78. Lessig, *The Law of the Horse*, *supra* note 74, at 507.

79. Lessig, *The New Chicago School*, *supra* note 75, at 671.

80. *Id*. at 662 n.7 (quoting Richard A. Posner, *Social Norms and the Law: An Economic Approach*, 87 AM. ECON. REV. 365 (1997)).

violators risk being criticized or shunned.[81] For example, ethnic jokes are legal, but humorists who employ them risk losing their audience.[82] Markets regulate through prices—if you cannot afford a subscription to the *Wall Street Journal*'s Web offerings, you cannot access its content.[83] To function, markets depend on the other modalities—laws must forbid theft for people to pay for computers rather than shoplift them, and trade in an item must be socially acceptable for a market (at least a public one) to exist.[84] Finally, architecture constrains people's choices.[85] Theft of buildings is difficult; theft of digital music is easy, unless the software code for the music implements restrictions such as digital rights management.[86] On the Internet, architecture is defined by software and hardware code that defines what actions are possible in a given context.[87]

¶ 31 These modalities create a toolbox for regulators. Most scholars believe that approaches to the problem of spam must be multi-modal to succeed; using only one of Lessig's tools will not work. By understanding the specific configuration of these four regulatory constraints for a given policy issue, policymakers can decide how to achieve a desired outcome.[88] In the Internet context, and particularly for spam, two modalities predominate: the architecture of software and hardware ("West Coast code") and the dictates of legal regulation ("East Coast code").[89] Accordingly, these are the first two areas examined in this survey of current attempts to control the behavior of spammers.

B. Technology

¶ 32 Spam has triggered a wide range of technological responses seeking to control or eliminate it, ranging from use of existing Internet features, to technological attacks on senders,[90] to additional functionality that vendors and ISPs must implement. The challenge of technological responses to spam is the need for consensus. Vendors or organizations implementing anti-spam measures face the problem of non-compliant senders, who may be spammers or legitimate entities who have not yet adopted the new control technology. For example, consider an ISP that implements a new feature that

81. *Id.* at 674.
82. *See id.* at 662.
83. *See* LESSIG, *supra* note 7, at 89 (noting that in cyberspace, "[p]ricing structures constrain access").
84. *See* Lessig, *The New Chicago School*, *supra* note 75, at 663; *see also* Lessig, *The Law of the Horse*, *supra* note 74, at 507 (stating that "the market is able to constrain in this manner only because of other constraints of law and social norms: property and contract law govern markets; markets operate within the domain permitted by social norms").
85. *See* LESSIG, *supra* note 7, at 89; *see also* Lessig, *The New Chicago School*, *supra* note75, at 663.
86. Lessig, *The Law of the Horse*, *supra* note 74, at 523–36.
87. *Id.* at 509–10.
88. *Id.* at 510 (stating that "to understand how a regulation might succeed, we must view these four modalities as acting on the same field, and understand how they interact").
89. LESSIG, *supra* note 7, at 53–54.
90. *See* Jan Libbenga, *Lycos screensaver to blitz spam servers*, REGISTER, Nov. 26, 2004, *at* http://www.theregister.co.uk/2004/11/26/lycos_europe_spam_blitz/ (reporting on a Lycos Europe screen saver program that launched denial of service attacks against Web sites selling products advertised through spam); *see also* Scarlet Pruitt, *Lycos pulls antispam screen saver from site*, COMPUTERWORLD, Dec. 3, 2004, *at* http://www.computerworld.com/softwaretopics/software/groupware/story/0,10801,98039,00.html (noting criticism of the Lycos tactic).

verifies a sender's identity. If a server that does not employ the new method tries to send e-mail to the ISP, how should the ISP react? Treating the sender as a spammer reduces e-mail volume and comports with the new method's intent, but risks rejecting legitimate messages from slow-adopting senders. This risk of "false positives" is particularly great early in a technology's adoption phase, as senders face a range of possibly incompatible choices for control methods. However, permitting the non-compliant sender to transfer mail undercuts the new precaution's power, increases the risk the ISP will accept spam, and requires employing additional processes to control spam effectively.

¶ 33 Current technological approaches conform to our earlier analysis by treating the underlying e-mail architecture as static—they do not seek wholesale changes to standards, but instead propose minor modifications. Thus, we can classify technological responses based on the point of the architecture they seek to control.[91]

1. Verifying the Sending Server

¶ 34 Many technological anti-spam methods verify the sending server's identity.[92] Microsoft provides a useful analogy: this check is like caller ID for telephone calls.[93] Like caller ID, verification techniques let the receiver know who seeks to contact them to share information. These approaches try to confirm, for example, that the mail server claiming to be smtp.harvard.edu is, in fact, a computer authorized to transfer mail for Harvard's Internet domain. The methods use the DNS for this check, whether through existing records (such as PTR, or "pointer," records[94]) or new ones (such as Microsoft's XML-based TXT records for Caller ID for E-mail[95]). The point of control[96] utilized by these methods limits their effectiveness—verifying the sending server's identity ensures that the *server* represents a given domain, but does not validate the *message's* sender or content. While verification proposals from e-mail vendors AOL, Microsoft, and Yahoo! have different implementations, they are all variants of the classic PTR lookup technique.

a. PTR Record Lookup

¶ 35 A standard technique for limiting spam involves verifying the sending server's identity by checking its IP address and hostname in the DNS. When a sending server

91. *See* Zittrain, *supra* note 6 at 656–59.

92. More specifically, these methods work at the initial SMTP conversation point in the e-mail transfer process—they verify the accuracy of the information exchanged in the SMTP connection and the HELO / EHLO statement.

93. *See infra* Section III.B.1.c.

94. For a definition of PTR records, see Cisco Systems, *Glossary – Cisco CNS Network Registrar User's Guide*, *at* http://www.cisco.com/en/US/products/sw/netmgtsw/ps1982/products_user_guide_chapter09186a00800ade6c.html#xtocid13 (last visited Oct. 13, 2004).

95. *See* Microsoft Corp., *Caller ID for E-mail: The Next Step to Deterring Spam* 5 (Feb. 12, 2004), *available at* http://download.microsoft.com/download/2/e/2/2e2850b8-2747-4394-a5a9-d06b5b9b1a4c/callerid_email.pdf (Feb. 12, 2004) (describing how "XML-encoded information stored in the TXT resource records in the '_ep' subdomain of a DNS domain in question is used" to determine the sending server's identity).

96. *Cf.* Zittrain, *supra* note 6 at 656–59 (discussing potential points of network control on the Internet).

contacts a receiving server to transfer e-mail over SMTP, it generally provides its "fully qualified domain name" (FQDN[97]), which includes the server's name and domain (such as mail.harvard.edu).[98] Knowing the sending computer's hostname (along with obtaining its IP address in the initial connection) allows the receiving server to compare the information provided to that listed in a PTR record in the DNS.[99] A PTR record lists the IP address and FQDN for a computer.[100] Thus, if a sending server claims to have the FQDN mail.harvard.edu with IP address 192.168.0.1, the receiving server can look up that IP address in the DNS. If the hostname listed in the corresponding PTR record is not mail.harvard.edu, the receiving server may conclude that the sending computer is impersonating the Harvard SMTP server.

¶ 36 PTR lookups reduce the likelihood of a spammer successfully impersonating a legitimate e-mail server. However, this technique has limitations. Looking up a PTR record in the DNS requires extra processing by the receiving computer and causes e-mail transfer to take additional time.[101] Additionally, passing this check verifies only that a server is properly listed in the DNS, not that its messages are legitimate. From an information perspective, PTR records offer limited value—they verify the identity of the intermediary transferring e-mail, but cannot provide information about the message's content or the sender's identity.

b. AOL Sender Policy Framework (SPF)

¶ 37 AOL has implemented a system known as Sender Policy Framework (SPF).[102] SPF

97. *See* WEBOPEDIA, *FQDN*, *at* http://www.webopedia.com/term/f/fqdn.html (last modified May 15, 2001) (stating that a "fully qualified domain name consists of a host and domain name, including top-level domain" and providing as an example "www.webopedia.com . . . [where] www is the host, webopedia is the second-level domain, and .com is the top level domain").

98. The EHLO / HELO statement in the SMTP conversation identifies the server's hostname or domain. Postel, *supra* note 8, § 3.5 (noting that "in the HELO command the host sending the command identifies itself; the command may be interpreted as saying 'Hello, I am <domain>'").

99. *See* Mockapetris, *supra* note 18; *see also* Microsoft Corp., *Description of Reverse DNS Lookups*, *at* http://support.microsoft.com/default.aspx?scid=kb;en-us;164213 (last modified Oct. 9, 2002) (describing how applications use PTR records); Tech Recipes, *DNS/BIND Resource Record: PTR Reverse Lookup Record*, *at* http://www.tech-recipes.com/modules.php?name=Recipes&rx_id=307 (last modified July 18, 2004) (stating that a "PTR (pointer) record maps an IP address to a hostname and fully qualified domain name").

100. *See* PAUL ALBITZ & CRICKET LIU, DNS AND BIND 65, 420 (3rd ed. 1998). The PTR record provides the same information as an A record, but in reverse order. The A record maps hostnames to IP addresses, while PTR records map IP addresses to hostnames. The difference is analogous to finding a person's phone number by looking up their name in a directory (A record), or finding which person holds a phone number by looking up the number in the directory (PTR record).

101. *See* IBM, *Restricting Inbound SMTP Connections*, *available at* https://publib-b.boulder.ibm.com/help/help6_admin.nsf/f4b82fbb75e942a6852566ac0037f284/beb2c6a47cdada2185256c1d00395bed?OpenDocument (last visited Feb. 16, 2005).

102. The technology was originally known as "Sender Permitted From," but changed to "Sender Policy Framework" in February 2004. *See* SMTP+SPF, *Frequently Asked Questions about SPF*, *at* http://spf.pobox.com/faq.html#senderpermittedfrom (last visited Oct. 13, 2004). Ming Weng Wong, the Chief Technology Officer of pobox.com, invented SPF. Byron Spice, *Drowning in Spam: New Anti-Spam Techniques Focus on Identifying Senders*, PITTSBURGH POST-GAZETTE, May 10, 2004, at A1, *available at* http://www.post-gazette.com/pg/04131/314021.stm.

employs DNS records that specify which mail servers may send e-mail for a given domain.[103] These records are analogous to the MX records used to determine which servers can receive e-mail for a domain. Receiving servers look up a connecting server's hostname and IP address in these DNS records to confirm its identity and its permission to send mail before allowing it to transfer messages.[104] Like PTR lookups, SPF allows receiving servers to verify a connecting computer's identity. This helps establish a sending domain's reputation for spam and reduces a spammer's ability to pretend to be a different server or domain.[105] SPF can also check whether a message has a valid return address—it compares the return address specified in the SMTP MAIL FROM statement to the domains for which the sending server has permission to transfer mail.[106] For example, if the MAIL FROM address is <jdoe@harvard.edu>, but the server that transferred the message is not listed in the DNS as authorized to send mail for the harvard.edu domain, SPF would conclude that the message was unauthorized and likely to be spam.[107]

¶ 38 Sender Policy Framework has considerable benefits. It is supported and implemented by one of the largest ISPs, helping establish its value, and more than 13,000 domains use it.[108] Technical experts view it as relatively easy to deploy.[109] Major advertisers and commercial message senders, such as Amazon.com and Google, have "already taken the steps necessary to verify their mail using S.P.F."[110] However, SPF suffers important drawbacks. Spammers can evade its restrictions by using a valid return address;[111] indeed, nearly one-sixth of spam senders in a recent study used SPF to increase the perceived legitimacy of their messages.[112] SPF does not protect against

---

103. *See* Paul Roberts, *AOL Tests New Spam-Blockers*, PCWORLD.COM, Jan. 22, 2004, *at* http://www.pcworld.com/news/article/0,aid,114411,00.asp.

104. SMTP+SPF, *Frequently Asked Questions* (noting that "SPF was designed to protect the envelope sender," including "the return-path that shows up in 'MAIL FROM,' and to a lesser extent the HELO argument that is supposed to be an FQDN").

105. Roberts, *AOL Tests New Spam-Blockers* (citing Eric Raymond, president of the Open Source Initiative).

106. *See* Spice, *supra* note 102. Note that the return address displayed in the "From:" field of a message can differ from the return address provided in MAIL FROM; spammers often falsify the "From:" information to deceive recipients into reading a message. This check of MAIL FROM constitutes a key difference from Microsoft's Caller ID for E-mail proposal (discussed *infra*), which examines the return addresses contained in the body of the message, not the SMTP conversation. *See* Gregg Keizer, *Microsoft To Merge Caller ID With SPF Anti-Spam Scheme*, INTERNETWEEK.COM, May 26, 2004, *at* http://www.internetweek.com/showArticle.jhtml?articleID=21100498.

107 *See How does it work?*, *in* SMTP+SPF, *supra* note 102.

108. Spice, *supra* note 102; *see also* SMTP+SPF, *Executive Summary*, *at* http://spf.pobox.com/execsumm.html (last visited Oct. 13, 2004) (listing well-known domains that implement SPF).

109. Spice, *supra* note 102 (quoting John R. Levine, co-chair of the IETF Anti-Spam Research Group).

110. Saul Hansell, *4 Rivals Almost United on Ways to Fight Spam*, N.Y. TIMES, June 23, 2004, at C1.

111. Spice, *supra* note 102.

112. Robert Lemos, *Study: Spammers Use E-mail ID to Gain Legitimacy*, CNET NEWS.COM, Sept. 8, 2004, *at* http://news.com.com/2100-1029-5357269.html (citing a study by e-mail service provider MX Logic of almost 10 million messages in August 2004); *see also* Press Release, MX Logic, MX Logic Reports 16 Percent of Spammers Adopt Sender Policy Framework (SPF) Email Authentication Scheme (Sept. 8, 2004), *at*

spammers hijacking legitimate computers to send messages without the actual owner's knowledge.[113] The technique also requires organizations that forward e-mail messages on behalf of recipients to implement changes in how they do so.[114] Organizations implementing SPF must decide how to handle messages from domains that do not use the system—blocking this e-mail traffic as spam could inadvertently prevent receipt of legitimate mail. Even the company whose Chief Technical Officer invented the technology admits that encryption is a more secure answer for verifying senders.[115] Thus, SPF is likely to be only one component of a solution.

c. Microsoft Caller-ID for E-mail

¶ 39 To control spam, Microsoft has proposed a system analogous to the caller ID system used to identify and screen incoming telephone calls.[116] Like SPF, Caller-ID for e-mail systems use DNS records to establish which servers may legitimately send e-mail for a given domain.[117] Organizations can list multiple servers permitted to send e-mail for their domains.[118] When a mail server receives a request from another SMTP server to transfer mail, it checks these records to verify that the connecting server is authorized to transfer messages for the domain it claims to represent. For example, administrators for the law.harvard.edu domain create a Caller-ID DNS record specifying that the server mail.law.harvard.edu, at IP address 192.168.0.1, is the only server authorized to send mail for the domain. Thus, when a mail server tries to transfer mail from addresses in the law.harvard.edu domain, the receiving server can check if that server's name and IP address match those listed in the Caller-ID record. If not, the destination can assume that the mail is not legitimate and reject it.

¶ 40 Microsoft's system creates procedures that identify which domain a message is from. Caller-ID for e-mail calls this the message's "purported responsible domain."[119] The system first calculates the "purported responsible address" for the e-mail by examining message headers; it then extracts from the purported responsible address the domain that sent the e-mail.[120] The message headers are contained within the body of the e-mail message (as defined by RFC 821), so the calculation of the purported responsible address and domain analyzes the message body, not the address presented during the

---

http://www.mxlogic.com/news_events/press_releases/09_08_04_SPF_CAN_SPAM.html (reporting on the same study).

113. Roberts, *supra* note 103; Stefanie Olsen, *AOL tests caller ID for e-mail*, CNET NEWS.COM, Jan. 22, 2004, *at* http://news.com.com/2100-1032_3-5145065.html.

114. *Does SPF break email forwarding?*, *in* SMTP+SPF, *supra* note 102.

115. *Does it protect the "From:" header field?*, *in id.* ("The best way to protect the header 'From:' is by using a cryptographic signature such as . . . (when it is released) Yahoo DomainKeys.").

116. *See generally* Microsoft Corp., *supra* note 95, for Microsoft's specification on the Caller ID system.

117. *Id.* at 3. These records for outbound SMTP servers are analogous to the MX records for inbound servers that list which servers accept mail for a domain. The Caller-ID records are published as TXT records in a special DNS subdomain, "_ep."

118. *See id.* at 7–8 (describing how organizations can structure the DNS records and can use address ranges to avoid listing each server's address individually).

119. *Id.* at 11–12.

120. *Id.*

SMTP conversation (RFC 821's "MAIL FROM" command).[121] Thus, using SPF's "[t]esting at the message level would allow administrators to block some spam before it's sent, while the content examination proposed by Caller-ID could be used to more deeply probe messages to detect phishing attacks."[122]

¶ 41 Microsoft has disclosed two patent applications covering the underlying technology for Caller-ID.[123] The patents are broad, covering both the Caller-ID technology and, potentially, methods such as e-postage.[124] The chairman of the IETF's Anti-Spam Research Group expressed concern that one of the claimed inventions is sufficiently broad to cover most anti-spam technologies, including authentication.[125] In response to criticism, Microsoft revised its patent applications to remove language that might have covered SPF.[126]

¶ 42 Caller-ID for e-mail is essentially an enhanced version of the PTR lookup method. Its benefits are that it allows senders to establish which servers may transfer mail for their domains and that it has the support of a leading e-mail and computer software vendor.[127] Caller ID's drawbacks are that it does not verify the authenticity of a message's content or a sender's identity and that it may be viewed as a proprietary solution controlled by Microsoft.[128] The system requires domains to create new DNS records.[129] Caller-ID also forces some configuration changes for e-mail servers so it can determine the purported responsible domain—for example, systems forwarding e-mail must modify a forwarded message's header to alert subsequent systems to the forward.[130] Caller ID for e-mail would reduce the problem of senders impersonating legitimate domains and mail servers,

---

121. *See, e.g.*, Paul Roberts, *Microsoft to enforce Sender ID checks*, INFOWORLD, July 22, 2004, *at* http://www.infoworld.com/article/04/07/22/HNmicrosoftid_1.html (noting that under the merged Sender ID, organizations "will be able to check for spoofing at the envelope level, as proposed by SPF, and in the message body, as proposed by Microsoft").

122. Keizer, *supra* note 106.

123. *See* Jim Wagner, *Exposed Sender ID Patents Up Debate*, INTERNETNEWS.COM, Sept. 20, 2004, *at* http://www.internetnews.com/dev-news/article.php/3409971 (reporting on the publication of Microsoft's patents and anti-spam advocates' response).

124. *See* U.S. Patent Application 20040181571 (disclosed Sept. 16, 2004) (covering "[r]educing unwanted and unsolicited electronic messages by preventing connection hijacking and domain spoofing"); U.S. Patent Application 20040181585 (disclosed Sept. 16, 2004) (covering "[r]educing unwanted and unsolicited electronic messages by exchanging electronic message transmission policies and solving and verifying solutions to computational puzzles").

125. *See* Wagner, *supra* note 123 (quoting ASRG chairman John Levine).

126. Stefanie Olsen, *Microsoft reworks antispam spec to silence critics*, CNET NEWS.COM, Oct. 25, 2004, *at* http://news.com.com/2100-1032_3-5426045.html.

127. *Cf.* Festa, *supra* note 45 (noting that "Microsoft--with its Hotmail Web mail service, its MSN mail service, and others under its control--could single-handedly give such a system [of verification] a sizeable implementation boost").

128. Paul Roberts, *Experts Question Microsoft's Caller ID Plans*, PCWORLD.COM, Mar. 5, 2004, *at* http://www.pcworld.com/news/article/0,aid,115095,00.asp. Microsoft claims patent rights in this technology, and states it will grant a royalty-free license, but only to entities that make Sender ID patents available on a reciprocal basis. Microsoft Corp., *Royalty-Free Sender ID Specification License Agreement* (Aug. 2004), *at* http://download.microsoft.com/download/b/d/3/bd3b5463-c461-409c-b29f-512218d3f3e6/SenderID_License-Agreement.pdf.

129. Microsoft Corp., *supra* note 95, at 5.

130. *Id.* at 13–14.

but would not address spam sent from these domains and servers.[131]

d. Sender ID

¶ 43 Recognizing the need for a verification technology, the IETF created a working group to examine the various options. This team, known as the MTA Authorization Records in DNS ("MARID") group,[132] began by examining SPF.[133] Microsoft, though, submitted Caller-ID for e-mail to MARID as a proposed part of the Internet standard.[134] MARID combined Caller-ID with SPF to form a hybrid technology known as Sender ID.[135] Initially, it appeared that this "partial truce" among competing technologies would ease the path to an authentication standard.[136] Microsoft adopted Sender ID with its Hotmail, MSN, and Microsoft.com mail systems, creating a strong incentive for companies to publish SPF and Caller-ID records for their mail servers.[137] However, Sender ID came under heated criticism because Microsoft filed a patent covering how to determine a message's purported responsible address, and refused to disclose what the patent application claimed.[138] Open source software advocates also worried that the licenses Microsoft sought from users of Sender ID conflicted with the GNU General Public License (GPL)[139] that governs use of their programs.[140]

¶ 44 In response, Microsoft altered its patent applications for Sender ID to remove claims language that could have covered SPF. In addition, the company announced that Sender ID would support publishing records either in SPF or in its Purported Responsible Address format.[141] AOL announced renewed support for Sender ID after Microsoft altered one of its patent applications for the technology, but did not commit to an

---

131. For example, Caller ID does not affect spam that originates from free e-mail services such as Hotmail and Yahoo! Mail.

132. Internet Engineering Task Force (IETF), *MTA Authorization Records in DNS (MARID) Charter*, *at* http://www.ietf.org/html.charters/OLD/marid-charter.html (last modified June 18, 2004).

133. Larry Seltzer, *MARID Proposal Presses On*, EWEEK, Aug. 2, 2004, *at* http://www.eweek.com/article2/0,1759,1629053,00.asp.

134. Jim Hu & Stephanie Olsen, *Microsoft to submit antispam standard*, CNET NEWS.COM, May 19, 2004, *at* http://news.com.com/Microsoft+to+submit+antispam+standard/2100-1032_3-5216255.html.

135. *See* J. Lyon & M. Wong, *Sender ID: Authenticating E-Mail* (Internet Draft, May 2005), *at* http://www.ietf.org/internet-drafts/draft-lyon-senderid-core-01.txt; *see also* Press Release, Microsoft Corp., Microsoft and Meng Wong to Merge Caller ID for E-Mail and SPF Anti-Spam Technology Proposals (May 25, 2004), *at* http://www.microsoft.com/presspass/press/2004/may04/05-25SPFCallerIDPR.asp.

136. Hansell, *4 Rivals Almost United on Ways to Fight Spam*, *supra* note 110 (quoting SPF author Meng Wong as calling the agreement "good news, because we now have a road map. . . . We can proceed with S.P.F. and Sender ID now and with Domain Keys as a second wave").

137. Roberts, *supra* note 121.

138. *See* Jim Wagner, *Microsoft Floats Sender ID Compromise*, INTERNETNEWS.COM, Sept. 8, 2004, *at* http://www.internetnews.com/dev-news/article.php/3405331.

139. For GNU's terms, see GNU Project, *GNU General Public License*, *at* http://www.gnu.org/copyleft/gpl.html (last modified Nov. 8, 2004).

140. *See also* Robert Lemos, *Apache, open source groups wary of Sender ID*, CNET NEWS.COM, Sept. 2, 2004, *at* http://news.com.com/Apache%2C+open-source+groups+wary+of+Sender+ID/2100-1013_3-5345317.html?tag=nl (discussing "[t]he Apache Foundation, an open-source development group," and its decision to pull its support from Sender ID due to Microsoft's licensing requirements).

141. *See* Olsen, *supra* note 126.

implementation date.[142]

¶ 45 Ultimately, an inability to reach consensus on how to deal with Microsoft's potential intellectual property claims to parts of Sender ID led the MARID group to decide that Microsoft's technology would not be a mandatory part of the standard.[143] Verification techniques that use the Microsoft technique can still comply with the standard, but the Microsoft approach becomes only one of several acceptable methods.[144] The dispute, and subsequent decision to adopt a multi-pronged approach to verification, risks undercutting adoption of the standard and dividing the anti-spam community into different camps.

¶ 46 The split over Sender ID forced the shutdown of the MARID working group and its efforts to arrive at a single authentication standard.[145] The group proposed "experimentation with multiple proposals and a subsequent review of deployment experience" before attempting to define a standard.[146] Verification technologies need consensus and widespread adoption to succeed; the Balkanization of techniques makes it increasingly unlikely that the MARID standard effort will succeed.

¶ 47 The Federal Trade Commission hosted a forum on authentication in November 2004 in an attempt to explore options and to create consensus.[147] However, the summit reinforced both the division among vendors over technical approaches and pessimism that authentication would solve the spam problem.[148] Participants cited authentication as a necessary first step, but indicated that the increasing use of hijacked "zombie" personal computers to send spam made the technique less effective as a remedial measure.[149]

2. Controlling the Connection: Blocking the Sending Server

¶ 48 ISPs can refuse SMTP connections from servers or domains viewed as suspect by using a process known as "blacklisting." Blacklisting attacks unwanted e-mail by blocking designated servers from transferring messages based on a belief or track record of sending (or vulnerability to sending) spam.[150] Like verification techniques,

142. *See* Jonathan Krim, *Microsoft Regains AOL's Support for Anti-Spam Technology*, WASH. POST, Oct. 26, 2004, at E5.

143. *See* Robert Lemos, *Microsoft e-mail proposal dealt setback*, CNET NEWS.COM, Sept. 13, 2004, *at* http://news.com.com/Microsoft+e-mail+proposal+dealt+setback/2100-1032_3-5364075.html.

144. *Id.*

145. *See* Jim Wagner, *IETF Shutters E-mail Working Group*, INTERNETNEWS.COM, Sept. 22, 2004, *at* http://www.internetnews.com/dev-news/article.php/3411461.

146. *Id.* (quoting Ted Hardie, an "area advisor of the IETF's Internet Engineering Steering Group").

147. *See* Fed. Trade Comm'n, *Email Authentication Summit*, *at* http://www.ftc.gov/bcp/workshops/e-authentication/index.htm (last visited Jan. 9, 2005).

148. *See* David McGuire, *E-Mail Firms Seek Spam Solution*, WASHINGTONPOST.COM, Nov. 9, 2004, *at* http://www.washingtonpost.com/wp-dyn/articles/A35958-2004Nov9.html (noting that MARID IETF chairman John Levine stated he would be "astonished if anything concrete came out of" the summit).

149. *See* Jonathan Krim, *E-mail Authentication Will Not End Spam, Panelists Say*, WASH. POST, Nov. 11, 2004, at E1.

150. *See* Spam-Blockers.com, *What is a Blacklist? SPAM Email Blacklists Directory*, *at* http://www.spam-blockers.com/SPAM-blacklists.htm (last visited Feb. 16, 2005) (describing a blacklist as a "database of known Internet addresses (or IP's) used by persons or companies sending spam" and linking

blacklisting operates on the control point of the initial SMTP connection. However, this method extends that control to its next logical step: deciding how to handle e-mail based on the sending server's identity. Blacklisting compares a server's hostname, domain, or IP address to a list of forbidden sources—if there is a match, the receiving server refuses to accept mail from the sending server.[151] In conjunction with verification techniques, blacklisting groups sending servers into two categories: allowed and forbidden senders. If a given server or domain becomes a significant source of spam, a receiving organization can implement a blacklist to block messages from that source.[152]

¶ 49 Two popular blacklists, the Mail Abuse Prevention System (MAPS) Realtime Blackhole List (RBL),[153] and the Open Relay Behavior-modification System (ORBS),[154] demonstrate the capabilities and challenges of this technique. Both ORBS and the RBL represent "a kind of vigilantism . . . an example of private people taking the law into their own hands" that constitutes "imperfect bottom-up regulation."[155] The RBL was founded by Paul Vixie,[156] the architect of Berkeley Internet Name Domain,[157] one of the most popular and influential DNS server applications. It began as an effort to block point sources of spam and expanded to block open relays, spam advertisers, and even entities providing payment processing to spammers. The RBL once invited lawsuits by describing how to sue MAPS on its Web site,[158] but after settling at least one claim, it adopted a lower profile and removed the relevant page from the site. In 2000, an estimated forty percent of e-mail servers used the RBL.[159] The RBL acknowledges that overblocking occurs—in 1998, Vixie stated that "It's heartbreaking for me to get e-mail from somebody's mother who can't send mail to her son at college because the school subscribes to the Black Hole List. . . . But I write them back and say: 'I'm sorry you're being inconvenienced. But your provider is spamming me. And they won't stop.'"[160]

---

to various blacklists). Blacklisting's counterpart is whitelisting, which switches the default rule used for connections. Blacklisting permits a server to transfer mail unless it is listed. Whitelisting forbids a server from transferring mail unless it is listed.

151. *See id.* (describing the process used by products implementing the MAPS Realtime Blackhole List to determine whether a connecting SMTP server has been blacklisted).

152. *See, e.g.*, MAPS, *MAPS RBL Overview*, *at* http://www.mail-abuse.com/services/mds_rbl.html (last visited Oct. 13, 2004) (describing the MAPS RBL Service as a technology for "identifying and blocking email from known spam sources, thereby greatly reducing the amount of unwanted email").

153. *Id.*

154. *See* Stewart Taggart, *Spam Blockers Pass It On*, WIRED NEWS, July 2, 2001, *at* http://www.wired.com/news/culture/0,1284,44876,00.html.

155. Lessig, *The Law of the Horse*, *supra* note 74, at 546–47.

156. *See* WIKIPEDIA, *Paul Vixie*, *at* http://en.wikipedia.org/wiki/Paul_Vixie (last modified July 13, 2004).

157. *See* Internet Systems Consortium, *ISC BIND*, *at* http://www.isc.org/index.pl?/sw/bind/ (last visited Feb. 16, 2005).

158. *See* Sorkin, *supra* note 65, at 349 n.113. Sorkin describes a second lawsuit filed by polling firm Harris Interactive against MAPS. Harris dropped the suit after several of the ISPs it sued discontinued use of MAPS. *See Jabs Traded, Slugfest Ends: Harris Discontinues Fight Against MAPS*, ATNEWYORK.COM, Sept. 14, 2000, *at* http://www.atnewyork.com/news/article.php/460571.

159. *See* Michelle Finley, *Other Ways to Fry Spam*, WIRED NEWS, Apr. 24, 2000, *at* http://www.wired.com/news/culture/0,1284,35776-2,00.html; *see also* Sorkin, *supra* note 65, at 348 n.106 (quoting other estimates that roughly one-third of mail servers use RBL).

160. Amy Harmon, *The American Way of Spam*, N.Y. TIMES, May 7, 1998, at G1.

¶ 50 The ORBS blacklist may have been even more controversial than RBL. The service, run by a New Zealand volunteer, compiled a publicly accessible file of open SMTP relays that companies used as a blacklist.[161] In 1998, ORBS listed the Massachusetts Institute of Technology's domain in its blacklist; MIT operated an open relay mail server controlled with methods of which the blacklist did not approve.[162] This led to a near "spam war" between MIT and an ORBS client, Hewlett-Packard, which abated only when ORBS' ISP decided that its blacklist violated the provider's network use policy.[163] ORBS shut down after two New Zealand companies won injunctions against the blacklist for including them in its database.[164]

¶ 51 While popular, blacklisting has several flaws. First, organizations implementing blacklists must compile a list of prohibited senders or subscribe to one such as RBL, incurring cost in either case.[165] Second, blacklists have been criticized for providing inadequate process for senders added to or removed from the list of barred sources.[166] MIT, for example, objected to being blacklisted by ORBS for operating an open mail relay when it used other techniques to control spam through its servers.[167] Third, criteria for inclusion in a blacklist are often amorphous—under the MAPS RBL definition, MasterCard could be included for providing payment processing services to a spam advertiser, and UUNet could be listed for providing DNS services to a site using spam to advertise its products. Fourth, blacklisting works best for senders who send a large *percentage* of spam, not simply a large *volume* of spam. Free e-mail services are increasingly popular with spammers;[168] indeed, Microsoft recently terminated free access to its Hotmail service from users with Outlook and Outlook Express e-mail clients due to "spammers going more and more after this particular protocol [that allows such access]."[169] However, blocking messages from the Hotmail or Yahoo! Mail services is untenable for most ISPs due to the high volume of legitimate messages that these senders route. This fact pressures blacklists not to include domains such as hotmail.com, since organizations implementing a blacklist blocking Hotmail would face immediate pressure from disgruntled users. Finally, blacklisting implements a definition of permissible e-

161. Taggart, *supra* note 154.
162. Lessig, *The Law of the Horse*, *supra* note 74, at 546–47.
163. *Id.* at 547.
164. Taggart, *supra* note 154.
165. Sorkin, *supra* note 65, at 349.
166. *See, e.g.*, *Blacklists vs. Spam*, BIZREPORT, May 16, 2003, *at* http://www.bizreport.com/article.php?art_id=4409 (describing challenges faced by a First Amendment Web site in removing its domain from blacklists); *see also* Saul Hansell, *How to Unclog the Information Artery*, N.Y. TIMES, May 25, 2003, at C1 (quoting former ICANN chair and current EFF director Esther Dyson as stating that "blacklists tend to be applied indiscriminately, and they are overbroad [and] amount to some sort of community censorship").
167. Lessig, *The Law of the Horse*, *supra* note 74, at 546–47 (noting that "MIT had measures to limit spam by policing the use of its 'third-party relay' facility," but its "methods were not the methods of ORBS, which made MIT an ORBS enemy").
168. Sorkin, *supra* note 65, at 351 n.123.
169. Matt Hicks, *MSN Ends Hotmail's Free Outlook Access*, EWEEK, Sept. 27, 2004, *at* http://www.eweek.com/article2/0,1759,1651948,00.asp (quoting Brooke Richardson, product manager for MSN's communication services). The protocol in question is WebDAV, a "set of HTTP extensions that allows for the reading and writing of documents through the Web" from clients such as Microsoft Outlook. *Id.*

mail marketing that does not comport with an information-based approach. The Spamhaus Block List, for example, will block *any* unsolicited bulk message.[170] As analyzed below, whether an e-mail message is consensual—whether the recipient indicates consent in advance to receive the information—does not determine whether that recipient realizes value from it. Blacklisting, then, is a tool that can be helpful in reducing spam, but it is a crude instrument.

¶ 52 Blacklisting's counterpart, whitelisting, is increasingly popular as an approach. Whitelisting solutions do not deliver a message to a recipient unless that recipient agrees to accept mail from that sender. Software vendors offer whitelist solutions for many popular messaging products.[171] Microsoft's Hotmail e-mail service uses whitelists.[172] Whitelists can operate in conjunction with programs such as bonded sender or payment at risk,[173] and may offer users more control over their communications generally. For example, in *The Accountable Internet: Peer Production of Internet Governance*, David Johnson, Susan Crawford, and John Palfrey propose a mixture of sender authentication technologies and whitelisting to allow each individual e-mail recipient to determine for herself the senders from whom she wants to accept messages.[174] Their goal is to permit individual users to exercise effective "Internet governance" by making decisions about who to trust and with whom to communicate. Users will permit "Internet connectivity 'by invitation only' . . . [to] radically affect the flow of wrongful or malicious messages."[175] Software programs such as Mailblocks implement this approach by allowing users to create lists of senders whose messages are accepted for delivery to their inboxes; other senders must respond to a challenge message to prove that they, not an automated spam program, sent the message.[176] Whitelisting, though, does present risks from an information-based perspective, since it is difficult for users to assess whether messages from unknown senders—even automated ones such as advertising bots—will provide value. In addition, whitelisting can break down if users extend their "Web of trust" too far, such as by trusting everyone whom another user trusts. Finally, whitelist e-mail

170. The Spamhaus Project, *Rationale & Listing Criteria*, *at* http://www.spamhaus.org/sbl/sbl-rationale.html (last visited Feb. 16, 2005) (stating that a sender may be blocked for transferring "bulk email verified to be unsolicited (spam)").

171. *See, e.g*, Corrigan Consulting, *Whitelist Based Anti-Spam Solution for Lotus Notes and Domino*, *at* http://www.corriganinc.com/Web.nsf/PublishedDetail/Spam?OpenDocument (last visited Feb. 16, 2005) (describing ClearMail, a whitelist spam solution for the Lotus Domino e-mail server).

172. *See* Jim Wagner, *Microsoft Joins IronPort Whitelist*, INTERNETNEWS.COM, May 5, 2004, *at* http://www.internetnews.com/infra/article.php/3349601.

173. *See infra* Section III.D.

174. David R. Johnson, Susan P. Crawford, & John G. Palfrey, Jr., *The Accountable Internet: Peer Production of Internet Governance*, 9 VA. J.L. & TECH. 9, ¶ 44, *at* http://www.vjolt.net/vol9/issue3/v9i3_a09-Palfrey.pdf (arguing that "decentralized decision-making can control or sharply curtail the spam problem, as long as sources of e-mail can either be accurately identified (authenticated as actually coming from the source listed in the headers) or known to be incapable of authentication . . . The new world of e-mail will consist of messages you would very likely want to receive—because sending an unwanted message might get the sender removed from the list of those you invite to communicate").

175. *Id.* ¶ 8.

176. *See* Wayne Porter, *Review: Mailblocks Challenge and Response Anti-Spam System*, *at* http://www.xblock.com/articles/article_show.php?id=43 (last visited Feb. 16, 2005). Mailblocks has recently been acquired by AOL.

systems require effort to maintain, and risk annoying senders.[177]

3. Checking the Sending Domain: DomainKeys

¶53 Yahoo!, along with e-mail software vendor Sendmail, uses a cryptographic approach to combat spam.[178] This system, DomainKeys, employs public-private key technology.[179] Public-private key cryptography uses a pair of encryption keys, one publicly available and one secret.[180] A message encrypted with the public key can be decrypted only with the private key, and vice-versa. With DomainKeys, an organization that sends e-mail messages, such as an ISP, creates a public key and a private key. It stores the public key for its domain in the DNS, and places copies of the private key on the e-mail servers that send messages to other domains.[181] The organization then signs all messages sent from its e-mail servers with the private key.[182] When an e-mail server in another domain receives a message purporting to be from the organization's domain, that server can verify the e-mail by checking the digital signature with the public key.[183] The receiving server collects the sending domain's public key from the DNS, and the digital signature and domain from the message headers.[184] It uses the public key to verify the message's digital signature. If the signature is valid, the server then compares the domain of the signing server to the domain listed in the message's From: header.[185] If the signature does not match the public key, or the domains do not match, the receiving server can treat the message as spam.[186] In addition, DomainKeys signs the entire e-mail message, allowing recipients to verify that its contents have not been altered and preventing spammers from copying signatures and re-using them for their own

177. *See, e.g.*, Jeff Ready, *The Big Squeeze: Closing Down the Junk E-mail Pipe – Internet*, COMPUTER TECH. REV., Dec. 2003, *available at* http://www.findarticles.com/p/articles/mi_m0BRZ/is_12_23/ai_112800714 (noting that whitelist "challenge responses can seriously annoy legitimate senders").

178. Press Release, Yahoo!, Sendmail and Yahoo! Mail Collaborate to Develop and Deploy DomainKeys (Feb. 24, 2004), *at* http://docs.yahoo.com/docs/pr/release1143.html; *see* Reuters, *New Standard Could Reduce Spam*, WIRED NEWS, May 18, 2004, *at* http://www.wired.com/news/business/0,1367,63513,00.html.

179. Yahoo! Anti-Spam Resource Center, *DomainKeys*, *at* http://antispam.yahoo.com/domainkeys (last visited Feb. 16, 2005).

180. *See generally* SIMON SINGH, THE CODE BOOK 384 (1999) (providing glossary definition of public-key cryptography); *see also id*. at 379–81 (describing the mathematics of one public-private key cryptographic system known as RSA encryption).

181. *See* Yahoo!, *supra* note 179; *see also* Juan Carlos Perez, *Yahoo Takes Aim at Spam*, PCWORLD.COM, Dec. 5, 2003, *at* http://www.pcworld.com/news/article/0,aid,113789,00.asp.

182. *Cf.* Am. Bar Ass'n, *Digital Signature Guidelines Tutorial*, *at* http://www.abanet.org/scitech/ec/isc/dsg-tutorial.html (last visited Oct. 13, 2004) (describing how digital signatures function).

183. *See* Yahoo!, *supra* note 179.

184. Mark Delany, *Domain-based Email Authentication Using Public-Keys Advertised in the DNS (DomainKeys)* § 3.7.3 (Internet Draft, March 25, 2005), *at* http://www.ietf.org/internet-drafts/draft-delany-domainkeys-base-02.txt. DomainKeys examines the From: or Sender: header in the message and compares the domain in that address to the domain in the digital signature.

185. *Id.* § 3.7.7 (stating that "it is not unreasonable to treat unauthenticated email as lacking any trust and having no positive reputation"); *see also* Yahoo! *supra* note 179.

186. *See* Hiawatha Bray, *Yahoo Pitches Antispam System; Newly Passed Bill Inadequate to Halt Junk Mail, Firm Says*, BOSTON GLOBE, Dec. 10, 2003, at D1.

messages.[187]

¶ 54 Yahoo! cites a number of benefits for the DomainKeys architecture. It establishes a reputation for sending domains—for example, receiving servers can reject unsigned messages purporting to be from domains that always sign their messages using DomainKeys, or reject signed messages from a domain frequently used to send spam.[188] The company encourages ISPs to share information about the spam volume of domains using DomainKeys, and notes that companies subject to phishing impersonation can employ DomainKeys to protect their users from fraudulent solicitations.[189] Thus, if Citibank (a frequent phishing target) signs its messages with DomainKeys, recipients can discard unsigned messages that claim to be from Citibank.

¶ 55 Yahoo! promises to make the DomainKeys source code available as an open source venture, which may assuage industry concerns about implementing a proprietary solution.[190] Yahoo! claims patent rights in the technology underlying DomainKeys, but offers a royalty-free, non-exclusive, sub-licensable license to make and use implementations of the system.[191] It is also producing a reference implementation of DomainKeys that can be used with messaging systems such as qmail.[192] In August 2004, the company submitted DomainKeys as an Internet draft to the IETF,[193] which is likely to create a working group to explore signing messages digitally.[194]

¶ 56 Because using encryption to determine a message's origin is widely acknowledged as the most technically sound approach,[195] DomainKeys has obvious technical advantages over other spam-fighting tools such as SPF. Yahoo! already includes DomainKey signatures in all outgoing messages sent from any of the 39 million users of its free e-mail service, [196] and Google has recently begun using DomainKeys in its free e-mail service GMail.[197] Along with support from messaging software vendor Sendmail,[198] this

187. *See* Yahoo!, *supra* note 179 (noting that the system "signs the entire message to allow the receiving server to also verify that the message wasn't tampered with or altered in transit. . . . [This] makes it impossible to reuse parts of a message from a trusted source to fool users into believing the email is from that source").

188. *Id*.

189. *Id*.

190. *See* Alex Salkever, *Yahoo's Risky Antispam Gambit*, BUSINESSWEEK ONLINE, Jan. 13, 2004, *at* http://www.businessweek.com/technology/content/jan2004/tc20040113_3442_tc047.htm.

191. Yahoo!, *Yahoo! DomainKeys Patent License Agreement v1.0*, *at* http://domainkeys.sourceforge.net/license/patentlicense1-0.html (last visited Feb. 16, 2005).

192. *See* Yahoo!, *supra* note 179.

193. *See* Delany, *Domain-based Email Authentication Using Public-Keys Advertised in the DNS (DomainKeys)* (Internet Draft, Aug. 2004), *at* http://www.ietf.org/internet-drafts/draft-delany-domainkeys-base-01.txt.

194. Anick Jesdanun, *Anti-Spam Effort Killed Amid Patent Row*, BIZREPORT, Sept. 27, 2004, *at* http://www.bizreport.com/news/8073/.

195. *See, e.g.*, SMTP+SPF, *supra* note 108.

196. Jim Hu, *Yahoo takes on spam, boosts e-mail storage*, CNET NEWS.COM, Nov. 15, 2004, *at* http://news.com.com/2102-1032_3-5450821.html.

197. Jim Hu, *Gmail jibes with Yahoo to fight spam*, CNET NEWS.COM, Oct. 18, 2004, *at* http://news.com.com/2102-1032_3-5415306.html.

198. Stefanie Olsen, *Yahoo, Sendmail to test antispam system*, CNET NEWS.COM, Feb. 24, 2004, *at* http://zdnet.com.com/2100-1104_2-5164279.html.

user community gives DomainKeys a further advantage since most domains will almost certainly want to communicate with Gmail and Yahoo! Mail users.

¶ 57 Like SPF and Caller ID, DomainKeys will not solve all of spam's problems; although it verifies that a message originates from a domain, its approach suffers several shortcomings. First, the system is vulnerable to server hijacking. More importantly, DomainKeys may have difficulty achieving the widespread cooperation and adoption required to succeed:[199] Yahoo! has already alienated other members of an anti-spam group by announcing DomainKeys as its preferred approach without consulting them.[200] In addition, cryptographic verification imposes performance costs that can be significant.[201] Currently, only Yahoo! has implemented DomainKeys on a widespread basis, and it is not clear when the technology will be available to other e-mail software vendors or ISPs.[202] Sendmail and qmail implementations of DomainKeys are in the works, but there is no indication of release dates for these products. Thus, while using cryptography to verify senders holds promise, DomainKeys still faces the potentially imposing hurdles of compatibility and computing cost.

4. Checking the Content: Filtering

¶ 58 Filtering software, which can be implemented by both ISPs and end users, evaluates a message's contents to determine whether to reject it as spam, generally searching for key words, such as "Viagra," that characterize spam.[203] Other filters implement statistical methods known as Bayesian analysis that use a probabilistic assessment of words in a message to detect spam.[204] Use of Bayesian filters increased[205] after an article by software programmer Paul Graham[206] touted their capabilities.

199. Perez, *supra* note 181.

200. Hiawatha Bray, *Tech Experts Say Spammers on the Run*, BOSTON GLOBE, Jan. 26, 2004, at C3.

201. *Id.* (stating that DomainKeys would require domains "to set up a complex new encryption system, with lots of computing power to encode and check billions of digitally signed messages"); *see also* SearchSecurity.com, *DomainKeys*, *at* http://searchsecurity.techtarget.com/sDefinition/0,290660,sid14_gci944600,00.html (last modified Jan. 18, 2004) (stating that "some critics believe if DomainKeys was broadly implemented it would lead to an unacceptable slowing of transmission due to the extra handling of each message") (emphasis omitted).

202. Spice, *supra* note 102.

203. *See generally* James Gleick, *Tangled Up in Spam*, N.Y. TIMES, Feb. 9, 2003, at 42 (discussing key word filtering).

204. *See, e.g.*, Neil Swidey, *Spambusters*, BOSTON GLOBE MAG., Oct. 5, 2003, at 15 (describing Bayesian analysis). Bayesian analysis offers the capability to refine a filter's analysis through classification of messages by users or administrators. *See* Robert Lemos, *Network Associates builds a better SpamKiller*, CNET NEWS.COM, Apr. 12, 2004, *at* http://news.com.com/2100-7355_3-5190209.html (stating that an "advantage is that Bayesian models are self-correcting, meaning that when data changes, so do the results"). *See generally* Paul Graham, *A Plan for Spam* (Aug. 2002), *at* http://www.paulgraham.com/spam.html (describing a Bayesian software filter's code and underlying analysis).

205. *See* Sue Mosher, *Bayesian Spam Filters*, WINDOWS NETWORK & .NET MAG., Feb. 18, 2003, *at* http://www.windowsitpro.com/Articles/Print.cfm?ArticleID=38059 (noting that "[m]uch of the buzz around this technique started with Paul Graham's August 2002 article 'A Plan for Spam'").

206. Graham, *A Plan for Spam*, *supra* note 204.

Bayesian filtering software is available for both personal computers[207] (for use by consumers) and servers[208] (for use by ISPs).

¶ 59 Filters effectively catch a great deal of spam, but suffer three major drawbacks: underinclusion, overinclusion, and questions of control. Underinclusive filters fail to detect some spam, primarily due to programming constraints (it is difficult for computer software to evaluate semantic meaning) and spammers' reactions to filtering. For example, if filters block messages with the term "Viagra," senders may shift to "V1agra," which the filter is less likely to detect but which appears similar to human readers. On the other hand, overinclusive filters remove desired messages as well as undesired ones. The e-mail marketing firm Return Path conducted research showing that seventeen percent of permission-based messages (where senders indicate advance consent to receive the e-mail) were blocked by spam filters.[209] This overblocking hurts users who want to receive these messages; the filter does not distinguish between commercial messages requested by users and unsolicited advertisements. Preventing overinclusion is difficult, since one user might request a given advertisement via e-mail and another would prefer to block it.[210]

¶ 60 Overinclusive filters may also block users' outbound messages.[211] For example, the ISP Comcast misconfigured a spam filter to try to block spammers from sending messages with falsified return addresses ending in .ru, the top-level domain for the Russian Federation.[212] Unfortunately, this error prevented Comcast broadband users from sending mail to users in that domain—the filter did not distinguish between Comcast users and external senders (spammers) in rejecting messages destined for Russian addresses.[213]

---

207. *See, e.g.*, Spammunition, *FAQ*, *at* http://www.upserve.com/spammunition/faq.asp (last visited Feb. 16, 2005) ("Spammunition is an add-in for [Microsoft] Outlook 2000 (and higher) that helps you fight spam. . . . [It] uses a Bayesian filtering technique to analyze the incoming mail you get."); Spam Bully, *Features & Screenshots*, *at* http://spambully.com/features.php (last visited Feb. 16, 2005) (describing a Bayesian filtering program for Microsoft Outlook and Outlook Express).

208. *See, e.g.*, Red Earth Software, *Policy Patrol Spam Filter*, *at* http://www.policypatrol.com/PolicyPatrolSpamFilter.htm (last visited Feb. 16, 2005) (describing a server-based Bayesian mail filtering program that "works with Exchange 2003, 2000 & 5.5, Lotus Domino and any other SMTP mail server").

209. Hiawatha Bray, *As War On Spam Heats Up, Many Valid E-mails Are Getting Lost*, BOSTON GLOBE, Feb. 18, 2004, at A14 (noting that overinclusiveness is a greater problem for smaller ISPs and receiving organizations that have less skill in configuring filters).

210. Overinclusive filters are less problematic at the user level since most filtering software for end users isolates, but does not immediately delete, spam messages. Users can also configure their filters to permit some messages but block others. For ISPs, though, checking each user's preferences before accepting transfer of a message would impose a prohibitive cost in performance.

211. *See, e.g.*, Paul Festa, *Comcast Goofs in Russian Spam Blockade*, CNET NEWS.COM (Mar. 2, 2004), *at* http://news.com.com/2102-1038_3-5168643.html (describing how Comcast blocked its broadband customers from sending mail to addresses in the .ru domain to "thwart spammers who were using the ISP's servers to send spam with spoofed return addresses ending in .ru, the Russian top level domain").

212. *Id.*

213. In essence, the misconfigured filter blocked all mail to .ru addresses, rather than rejecting only relayed mail for that domain and permitting Comcast users to send such messages. *Id.*

¶ 61 Finally, filtering may shift choices about whether to receive unsolicited information from the end user to entities such as an ISP or a filtering software company.[214] Like filters that regulate which Internet sites users can access,[215] spam filters can make control over information less transparent and less easily altered by individuals.[216]

¶ 62 A number of regulatory proposals and requirements for spam combine law with filtering. For example, the Federal Trade Commission requires all unsolicited adult messages to include the words "SEXUALLY-EXPLICIT" in the subject line[217], and the CAN SPAM Act of 2003 directs the Commission to consider recommending that every spam message contain a subject line identifier such as "ADV."[218] Standardized spam identifiers greatly aid filters in detecting and blocking these messages.[219]

¶ 63 The problem with this type of filtering requirement is that it has the inverse effect of that desired: legitimate marketers (who already have incentives to control unwanted e-mail advertising from reputation considerations) are more likely to comply than illegitimate ones. Spam filters are thus more likely to weed out compliant messages, decreasing the overall volume of spam but also reducing the value consumers gain from unsolicited advertising and increasing the share of unsolicited e-mail that is fraudulent or inaccurate. Filtering, then, is like TiVo—it filters out advertising in a way that may ultimately harm the underlying medium.[220]

5. Technology Summary

¶ 64 Overall, current technological methods for controlling spam are reactionary, not revolutionary—they work within the existing system of Internet e-mail standards rather than altering it. As such, they tend to be partial solutions to the problems inherent in the

---

214. *See, e.g.*, Fed. Trade Comm'n, *Label for Email Messages Containing Sexually Oriented Material*, 69 Fed. Reg 21,024, 21,025 (Apr. 19, 2004), *available at* http://www.ftc.gov/os/2004/04/040413adultemailfinalrule.pdf (noting the Center for Democracy and Technology's objection to its labeling requirement because labeling "is designed to promote filtering by the ISPs and takes control away from the end user," and responding that ISPs can compete based on the accuracy and level of filtering to meet this objection).

215. *See, e.g.*, *OpenNet Initiative*, *at* http://www.opennetinitiative.net/ (last visited Feb. 16, 2005) (describing research on Internet filtering in various countries).

216. *Cf.* Lawrence Lessig, *Law Regulating Code Regulating Law*, 35 LOY. U. CHI. L.J. 1, 10–13 (2003).

217. *See* Fed. Trade Comm'n, Press Release, *FTC Adopts Rule That Requires Notice That Spam Contains Sexually-Explicit Material* (Apr. 13, 2004), *at* http://www.ftc.gov/opa/2004/04/adultlabel.htm. Anti-spam company Brightmail found that most spam failed to comply with the FTC regulations during testing one week after the regulations went into effect. Declan McCullagh, *Porn Spammers Ignore New Rule*, CNET NEWS.COM, May 26, 2001, *at* http://news.com.com/2100-1028_3-5220850.html.

218. 15 U.S.C. § 7710(2) (2004) (requiring the FTC to create a report within 18 months of the Act's enactment and allowing the FTC to recommend compliance with IETF standards, use of "ADV," or no plan at all).

219. *See, e.g.*, Fed. Trade Comm'n, *supra* note 214, at 21,024 (noting that requiring spam with adult content to include a standardized identifier in its subject line "facilitates filtering").

220. *See* Jane Black, *Coming Soon: A Horror Show for TV Ads*, BUSINESSWEEK ONLINE, June 27, 2003, *at* http://www.businessweek.com/technology/content/jun2003/tc20030627_1133_tc119.htm (citing Forrester Research data projecting that when 30 million households have personal video recorders like TiVo, 76% of advertisers will cut television ad spending).

standards. Technology hasn't yet worked to curb spam. In reaction, U.S. regulators have turned to the second modality for shaping behavior—law—with a recent federal statute.

C. Law

¶ 65 In the United States, legal spam regulation began with private suits against spammers on claims such as trespass to chattels, trademark infringement, and computer fraud. State laws governing spam emerged slowly. Federal laws regulated spam indirectly, such as by prohibiting deceptive advertising, but only states had laws specifically covering unsolicited commercial e-mail until 2003.[221] This patchwork statutory coverage created a number of different, often conflicting legal regimes for unsolicited commercial e-mail messages: some states imposed an "opt-in" system,[222] others "opt-out;"[223] some required subject lines to begin with "ADV,"[224] others with different characters[225]; and many based their jurisdiction on whether a recipient was a state resident[226] (a characteristic difficult or impossible to discern from most e-mail addresses). This welter of regulations was simplified greatly in 2003 when the U.S. Congress passed a bill governing spam that pre-empts most state regulation. This federal legislation, known as the "CAN SPAM" Act, constitutes the major current legal constraint on unsolicited e-mail advertising in the U.S., and this analysis of spam regulation through law begins by reviewing its provisions.

1. The CAN SPAM Act of 2003

¶ 66 In December 2003, after nearly four years of proposals and debate, the U.S. Congress passed, and President George W. Bush signed, a bill regulating commercial e-mail.[227] Two key factors drove passage of the CAN SPAM Act of 2003. First, technology companies and e-mail service providers such as Microsoft, Time Warner, and AOL pushed strongly for legislation.[228] Second, marketing and advertising groups that opposed earlier national legislation dropped objections in the face of impending, more restrictive state legislation (which CAN SPAM pre-empted).[229] While CAN SPAM

---

221. *See, e.g.*, David E. Sorkin, *Spam Laws: Summary*, *at* http://www.spamlaws.com/state/summary.html (last visited Feb. 16, 2005) (listing spam laws of individual states but cautioning that CAN SPAM may preempt them).

222. *See, e.g.*, CAL. BUS. & PROF. CODE § 17529.2(b) (2003).

223. *See, e.g.*, R.I. GEN. LAWS § 6-47-2(b) (1999).

224. *See, e.g.*, UTAH CODE ANN. § 13-36-103(1)(b)(i) (2002) (repealed 2004).

225. *Compare* 18 PA. CONS. STAT. § 5903(a.1) (2004) (requiring messages containing "explicit sexual materials" to include "the term 'ADV-ADULT' at the beginning of the subject line") *with* 815 ILL. COMP. STAT. 511/10(a-15) (2003) (requiring unsolicited e-mail advertisements that contain information that may be possessed or purchased only by people over the age of 18 to "include 'ADV:ADLT' as the first 8 characters" of the subject line).

226. *See, e.g.*, WASH. REV. CODE § 19.190.020(1) (1999).

227. Jennifer Lee, *Bush Signs Law Placing Curbs on Bulk Commercial E-Mail*, N.Y. TIMES, Dec. 17, 2003, at C4.

228. Jennifer Lee, *House Accepts Revisions on Antispam Bill*, N.Y. TIMES, Dec. 8, 2003, at C10.

229. Chris Gaither, *Clearing Way for Legitimate E-mail? Marketers Hope Antispam Law Restores Industry's Reputation*, BOSTON GLOBE, Dec. 1, 2003, at C1 (stating that the marketing "industry argued against federal legislation, until states began passing laws trying to restrict unsolicited commercial e-mail"

criminalized certain commercial e-mail activities, it created less rigorous restrictions than many state laws by allowing advertisers to contact recipients until requested to stop (an "opt-out" approach) and by preventing lawsuits by individual users.[230]

¶ 67 CAN SPAM has five parts: criminal prohibitions, civil prohibitions, enforcement limitations, pre-emption of state e-mail laws, and provisions instructing the Federal Trade Commission ("FTC") to undertake further analysis. We examine each in turn.

a. Criminal Provisions

¶ 68 CAN SPAM creates new criminal offenses related to spam by adding Section 1037 to Title 18 of the U.S. Code. Section 1037 makes falsifying e-mail account information, spam relaying, and falsifying mail header information a criminal offense.[231] Specifically, the bill prohibits accessing without authorization[232] a computer[233] to send or relay multiple[234] commercial e-mail messages,[235] using a computer to relay commercial e-mail messages to deceive recipients or ISPs about the messages' origin,[236] materially falsifying[237] header information in sent commercial messages,[238] registering with false information five or more e-mail accounts or two or more domain names used by the

---

and that the "toughest [state law], scheduled to take effect in California on Jan. 1, prompted e-mail marketers to begin lobbying hard for a federal law to override the 37 state rules").

230. *Id.*

231. *See* CAN SPAM Act of 2003, Pub. L. No. 108-187, 117 Stat. 2699 (2003), *codified at* 15 U.S.C. § 7701 *et seq.* (2004). 18 U.S.C. § 1037(a) requires that the person knowingly take the specified actions and that the actions be in or affect interstate or foreign commerce.

232. 18 U.S.C. § 1037(a)(1).

233. 15 U.S.C. § 7702(13) defines the relevant computer through the term "protected computer" in 18 U.S.C. § 1030(e)(2)(B), which "means a computer . . . which is used in interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States."

234. 18 U.S.C. § 1037(d)(3) defines "multiple" as "more than 100 electronic mail messages during a 24-hour period, more than 1,000 electronic mail messages during a 30-day period, or more than 10,000 electronic mail messages during a 1-year period."

235. 15 U.S.C. § 7702(2) defines "commercial electronic mail message" as "any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service (including content on an Internet website operated for a commercial purpose)" except for "transactional or relationship message[s]." The FTC issued regulations defining "primary purpose" on Dec. 16, 2004. *See* Fed. Trade Comm'n, *Commission Actions for December 2004, at* http://www.ftc.gov/os/2004/12/index.htm; Fed. Trade Comm'n, *Definitions and Implementation Under the CAN-SPAM Act*, 70 Fed. Reg. 3110 (Jan. 19, 2005), *available at* http://www.ftc.gov/os/2005/01/050112canspamfrn.pdf. Section 7702(17) defines "transactional or relationship message" as having the primary purpose of completing a commercial transaction to which the recipient has agreed; providing warranty or safety information about a product or service; providing information about changes in terms, features, status, employment or employment benefits; providing periodic information about account balances; or delivering goods or services pursuant to a transaction to which the recipient has agreed.

236. 18 U.S.C. § 1037(a)(2).

237. *See id.* Section 1037(d)(2) defines "materially falsified" to mean "altered or concealed in a manner that would impair the ability of a recipient of the message, an Internet access service processing the message on behalf of a recipient, a person alleging a violation of this section, or a law enforcement agency to identify, locate, or respond to a person who initiated the electronic mail message or to investigate the alleged violation."

238. 18 U.S.C. § 1037(a)(3).

registrant to send commercial e-mail,[239] and falsely representing one's status as the registrant or owner of five or more IP addresses used to send commercial e-mail. Violators face fines; prison terms of one,[240] three,[241] or five[242] years; and forfeiture of proceeds from and property used in the crime.[243]

¶ 69 The Act directs the U.S. Sentencing Commission to consider increasing sentences for violators who obtained e-mail addresses through unauthorized harvesting from Web sites or online services;[244] used dictionary attacks[245] to obtain addresses;[246] knew the unlawful message advertised or contained a domain whose registrant used false registration information;[247] or committed child pornography, child sexual exploitation, fraud, identity theft, or obscenity offenses involving large volumes of e-mail.[248] The Sentencing Commission in turn proposed using the increased sentence guidelines for fraud for CAN SPAM violations.[249] Though the Electronic Frontier Foundation and the National Association of Criminal Defense Attorneys opposed this proposal as unduly harsh,[250] the Commission retained the link in its final guidelines for Congress.[251]

---

239. *Id.* § 1037(a)(4). Note that this provision requires the registrant to use more than one of the domain names or e-mail accounts to initiate the transmission of multiple commercial e-mail messages.

240. *Id.* § 1037(b)(3) (imposing up to a one-year sentence for CAN SPAM offenses not covered by the three- or five-year provisions).

241. *Id.* § 1037(b)(2) (imposing up to a three-year sentence for violations of 18 U.S.C. § 1037(a)(1) or violations of 18 U.S.C. § 1037(a)(4) involving twenty or more accounts, or ten or more domains names; message volumes greater than 2500 in twenty-four hours, 25,000 in thirty days, or 250,000 in one year; losses of $5000 or more in a one-year period; offenders gaining benefit of $5000 or more in a one-year period; or the defendant acting as organizer or leader in working with three or more other people to commit the offense).

242. *Id.* § 1037(b)(1) (imposing up to a five-year sentence for violations in furtherance of a felony or when the defendant has a previous conviction for a violation of 18 U.S.C. § 1037, 18 U.S.C. § 1030 (the Computer Fraud and Abuse Act), or state laws involving unauthorized access to a computer or transmission of multiple commercial e-mail messages).

243. *Id.* § 1037(c)(1).

244. 18 U.S.C. § 1037(b)(1)(B).

245. *See* WEBOPEDIA, *Dictionary Attack*, *at* http://www.pcwebopedia.com/term/d/dictionary_attack.html (last modified Feb. 19, 2004) (defining dictionary attack as a method of breaking password-based security systems by "systematically test[ing] all possible passwords beginning with words that have a higher possibility of being used, such as names and places").

246. 15 U.S.C. § 7704(b)(1).

247. *Id.* § 7702(4).

248. *Id.* § 7703(b).

249. U.S. Sentencing Comm'n, *Sentencing Guidelines for United States Courts*, 69 Fed. Reg. 2169, 2172–73 (Jan. 14, 2004).

250. Paul Festa, *Legal Experts Urge Spam Leniency*, CNET NEWS.COM, Mar. 17, 2004, *at* http://news.com.com/2100-1028_3-5174098.html.

251. U.S. Sentencing Comm'n, Press Release, *Sentencing Commission Toughens Requirements for Corporate Compliance and Ethics Programs* (Apr. 13, 2004), *at* http://www.ussc.gov/press/rel0404.htm (stating that the "Commission created a sentence enhancement of approximately 25 percent if a defendant improperly obtains e-mail addresses for the purpose of spamming and an automatic application of an additional 25 percent sentence increase for mass marketing" and that "additional sentencing increases based on the amount of loss and number of victims also will apply"); *see also* Paul Festa, *Stiff Spam Penalties Urged*, CNET NEWS.COM, Apr. 14, 2004, *at* http://news.com.com/2100-1028_3-5191651.html (quoting a representative for the National Association of Criminal Defense Lawyers as saying, "[T]his is just junk mail. This doesn't even kill trees").

¶ 70 Finally, entities sending e-mail with sexually-oriented material must indicate the content in the subject line (as specified by the FTC[252]) and ensure that such messages display only this indicator, instructions on accessing content, and the opt-out mechanism when first opened,[253] unless the recipient consented in advance to receiving the message.[254] Violations are punishable by fines or up to five years in prison.[255]

b. Civil Prohibitions

¶ 71 In addition to criminal prohibitions, CAN SPAM establishes civil liability to regulate commercial e-mail. Initiating[256] a commercial, transactional, or relationship e-mail message with materially[257] false or misleading headers,[258] or using a subject line the sender knows is likely to mislead the recipient,[259] is unlawful. Senders must include a conspicuous means for recipients to request not to receive future messages at that address.[260] This "opt out" mechanism must function for at least thirty days after the message is sent in order to give recipients time to make such a request.[261] When a recipient opts out, the sender (or her agent) must not send commercial e-mail within the request's scope after ten business days of receiving the request, nor can the sender transfer or share the recipient's e-mail address except in compliance with specific legal

252. 15 U.S.C. § 7704(d)(3) (requiring the FTC to consult with the U.S. Attorney General to specify "clearly identifiable marks or notices to be included in or associated with commercial electronic mail that contains sexually oriented material" in the Federal Register within 120 days of the law's enactment). The FTC proposed requiring that the subject line for such messages begin with the mark "'SEXUALLY-EXPLICIT-CONTENT: '." Fed. Trade Comm'n, *supra* note 214. .After considering comments, the FTC modified its approach. As of May 19, 2004, the Commission will require all "commercial e-mail that includes sexually oriented material" to exclude such material from the subject line, include the mark "SEXUALLY-EXPLICIT: " in the subject in the ASCII character set, and ensure that the message displays only a limited set of information (not including sexually oriented material) when first opened, unless the recipient gave prior consent to receive the message.

253. 15 U.S.C. § 7704(d)(1)(B). This requirement responds to an FTC finding that 17% of pornographic offers in a random sample of 1000 commercial e-mail messages contained adult imagery, and over 40% of these messages had falsified subject line or "From" information. *See* Label for E-mail Messages Containing Sexually Oriented Material 3 n.2 (proposed Jan. 28, 2004), *at* http://www.ftc.gov/os/2004/01/canspamfrn.pdf (citing Fed. Trade Comm'n, *False Claims in Spam* 13 (Apr. 30, 2003), *available at* http://www.ftc.gov/reports/spam/030429spamreport.pdf).

254. 15 U.S.C. § 7704(d)(2).

255. *Id.* § 7704(d)(5).

256. Section 7702(9) defines "initiating" a commercial e-mail message as "to originate or transmit such message or to procure the origination or transmission of such message," but does not include "actions that constitute routine conveyance of such message." Thus, "more than one person may be considered to have initiated a message."

257. Section 7704(a)(6) defines "materially" as "alteration or concealment of header information in a manner that would impair the ability of an Internet access service processing the message on behalf of a recipient, a person alleging a violation of this section, or a law enforcement agency to identify, locate, or respond to a person who initiated the electronic mail message or to investigate the alleged violation, or the ability of a recipient of the message to respond to a person who initiated the electronic message."

258. Section 7704(a)(1)(A) defines "materially misleading" to include using relaying that fails to identify the sending computer or using a fraudulently obtained e-mail address, domain name, or IP address.

259. 15 U.S.C. § 7704(a)(2).

260. *Id.* § 7704(a)(3).

261. *Id.*

requirements.[262] Commercial e-mail senders must clearly identify messages as advertisements and must include the sender's valid physical postal address.[263] The Act bans sending commercial e-mail to recipients whose addresses were obtained through dictionary attacks or through automated means from a site that states it will not make e-mail addresses available to anyone for the purpose of sending mail.[264] Using scripts to create multiple accounts to send e-mail that violate the Act is specifically prohibited,[265] as is relaying e-mail through another computer without authorization.[266] Either actual or statutory damages are available, with a limit of $250 per statutory violation and a cap of $2 million.[267] A court may multiply damages as much as threefold for aggravated violations,[268] or reduce damages if the defendant took adequate precautions.[269] Plaintiffs may also recover attorneys' fees.[270]

¶ 72 CAN SPAM also regulates how entities can advertise through e-mail, even if they are not the message's sender.[271] It is unlawful to promote (or to allow another to promote) a business, product, or service through a commercial e-mail message that violates the Act if one knows (or should know) of the promotion, receives or expects economic benefit from the promotion, and takes no reasonable action either to prevent the message or to detect and report it to the FTC.[272] Third parties providing services to someone who violates this prohibition are liable only if they have a majority interest in the violator's business, or if they know the message violates CAN SPAM and receive or expect to receive an economic benefit from the solicitation.[273] Only the FTC may enforce this part of CAN SPAM.[274]

c. Enforcement

¶ 73 CAN SPAM's enforcement provisions have been among the most criticized parts of the legislation.[275] The FTC is the primary enforcer of the Act's provisions.[276] Other

262. *Id.* § 7704(a)(4).

263. *Id.* § 7704(a)(5) (exempting senders from this requirement if a recipient agreed to receive the message).

264. *Id.* § 7704(b)(1).

265. *Id.* § 7704(b)(2).

266. *Id.* § 7704(b)(3).

267. *Id.* § 7706(f)(3). The $2 million cap does not apply to § 7704(a)(1) violations.

268. *Id.* § 7706(f)(3)(C). The court may increase the total award to as much as three times the normal maximum if the defendant acted willfully and knowingly, or if the defendant committed one of the aggravating violations defined in § 7704(b), such as dictionary attacks, scripted creation of accounts, or harvesting e-mail addresses.

269. *Id.* § 7706(f)(3)(D). Reduction is permitted if the defendant implemented "commercially reasonable practices and procedures designed to effectively prevent such violations" or if the violation occurred despite commercially reasonable efforts to maintain such precautions.

270. *Id.* § 7706(f)(4).

271. The Act accomplishes this by holding that the advertising entity "initiates" the message along with the sender. *See id.* § 7702(9).

272. *Id.* § 7705(a).

273. *Id.* § 7705(b).

274. *Id.* § 7705(c).

275. *See, e.g.*, Declan McCullagh, *Bush OKs spam bill--but critics not convinced*, CNET NEWS.COM (Dec. 16, 2003), *at* http://news.com.com/2100-1028-5124724.html?tag=nl (quoting Ray Everett-Church,

government agencies enforce provisions affecting their respective regulated industries, such as the Securities Exchange Commission (with respect to brokers and dealers)[277] and the Department of Transportation (with respect to air carriers)[278]. State officials, including state attorneys general, and state agencies can sue in federal court to enjoin violations or recover monetary damages for violations of §§ 7704(a)(1), (a)(2), or (d), or patterns or practices violating §§ 7704(a)(1)–(3).[279] However, state officials initiating suit must notify federal regulators (such as the FTC), who retain the right to intervene, remove the suit, and/or file appeals.[280] In addition, if federal regulators prosecute or bring a civil action for CAN SPAM violations, such a suit trumps state action, and state officials may not sue any defendant named in the federal action for violations alleged in the complaint.[281]

¶ 74 Internet access services[282] may also sue for an injunction or damages if "adversely affected" by violations of §§ 7704(a)(1), (b), or (d), or by a pattern or practice violating §§ 7704(a)(2)–(5).[283] CAN SPAM allows recovery of either actual or statutory damages. Statutory damages are calculated by multiplying the number of violations (the number of messages transmitted or attempted) by either $100 (for § 7704(a)(1) violations) or $25 (for other violations of § 7704) up to a maximum of $1 million.[284] Once again, an adjudicating court may increase damages (up to threefold) based on aggravating circumstances,[285] decrease damages based on the defendant's precautions,[286] and award costs, including attorneys' fees.[287] The Act expressly avoids regulating the lawfulness of Internet access services' e-mail policies.[288]

d. Pre-emption

¶ 75 The CAN SPAM Act pre-empts any state law or regulation "that expressly

---

Chief Privacy Officer at anti-spam firm ePrivacyGroup.com, as believing that there is not "enough enforcement to make spammers think twice about engaging in the practice").

276. 15 U.S.C. § 7706(a).

277. *See id.* § 7706(b)(3).

278. *See id.* § 7706(b)(7).

279. *Id.* § 7706(f)(1). See *supra* notes 253–66 and accompanying text for definitions of offenses under 15 U.S.C. § 7704 (2004).

280. 15 U.S.C. § 7706(f)(5).

281. *Id.* § 7706(f)(8).

282. "Internet access service" is defined in § 7702(11) by referring to 47 U.S.C. § 231(e)(4) (codified as part of the Child Online Protection Act), which defines the term as "a service that enables users to access content, information, electronic mail, or other services offered over the Internet." The term "may also include access to proprietary content, information, and other services as part of a package of services offered to consumers," but excludes "telecommunications services."

283. 15 U.S.C. § 7706(g)(1).

284. *Id.* § 7706(g)(3). Note that CAN SPAM defines a violation based on each "separately addressed message" transmitted or attempted to be transmitted over the access service's facilities or to an e-mail address obtained by the service; presumably, therefore, one message with multiple recipients would be treated as a single violation.

285. *Id.* § 7706(g)(3)(C).

286. *Id.* § 7706(g)(3)(D).

287 *Id.* § 7706(g)(4).

288 *See id.* § 7707(c); *see also* Sorkin, *supra* note 65, at 372–74 (discussing state laws prohibiting violations of Internet service providers' spam policies).

regulates the use of electronic mail to send commercial messages," but permits enforcement "to the extent that any such statute, regulation, or rule prohibits falsity or deception in any portion of a commercial electronic mail message or information attached thereto."[289] State laws "not specific to electronic mail," such as "trespass, contract, or tort law," as well as laws that "relate to acts of fraud or computer crime," are not pre-empted,[290] but most state laws regulating spam did not survive the adoption of CAN SPAM.[291]

e. Further Study

¶ 76 CAN SPAM deferred certain issues by requiring the FTC to study and report on them. These include a "do-not-e-mail" registry similar to the "do-not-call" registry;[292] an analysis of the Act's effectiveness, including how technical and market developments may change it, recommendations for foreign commercial e-mail, and recommendations for protecting consumers from obscene e-mail;[293] a report on rewarding people who supply information about violations;[294] and a report on requiring commercial e-mail to include an identifier in its subject line.[295] The Act specifically blocks the FTC from rulemaking that mandates how entities must comply with the opt-out, identification, and postal address requirements for commercial e-mail.[296]

¶ 77 To date, the FTC has issued two of the required studies. First, it rejected creating a "do-not-e-mail" registry, arguing that such a registry "would fail to reduce the amount of spam consumers receive, might increase it, and could not be enforced effectively."[297] In essence, the FTC stated that the registry would worsen, not improve, spam problems; it "determined that spammers would most likely use a Registry as a mechanism for verifying the validity of email addresses and, without authentication, the Commission

289. 15 U.S.C. § 7707(b)(1).

290. *Id.* § 7707(b)(2).

291. *See, e.g.*, Andy Sullivan, *Maryland Governor Signs Tough Anti-Spam Law*, REUTERS, May 26, 2004, *available at* http://msnbc.msn.com/id/5069723/ (reporting on the adoption of the Maryland Spam Deterrence Act after a "previous Maryland law [that] allowed customers to sue spammers directly . . . was voided by the national Can Spam Act").

292. *See* 15 U.S.C. § 7708(a) (requiring the FTC to report a plan and timetable, and any applicable concerns, about the "do-not-e-mail" registry within six months of the enactment of CAN SPAM); *cf.* Telemarketing Sales Rule, 16 C.F.R. § 310.4(b) (2004) (making it an abusive practice to call a person whose phone number appears in the "do-not-call" registry); *Mainstream Mktg. Servs. et al. v. FTC*, 358 F.3d 1228 (10th Cir. 2004) (upholding the "do-not-call" registry as a valid commercial speech regulation within the FTC and FCC's statutory authority). The Act permits the FTC to implement the "do-not-e-mail" plan only after nine months have passed since the Act's enactment. 15 U.S.C. § 7708(b).

293. *See* 15 U.S.C. § 7709.

294. *See id.* § 7710(1) (requiring the report within nine months of the Act's enactment).

295. *See id.* § 7710(2) (requiring the report within eighteen months of the Act's enactment and allowing the FTC to recommend compliance with IETF standards, use of "ADV," or no plan at all).

296. *Id.* § 7711(b) (forbidding the FTC from requiring senders "to include any specific words, characters, marks, or labels in a commercial electronic mail message, or to include the identification required by [§ 7704(a)(5)(A)] in any particular part of such a mail message").

297. Fed. Trade Comm'n, Press Release, *New System to Verify Origins of E-Mail Must Emerge Before "Do Not Spam" List Can Be Implemented, FTC Tells Congress* (June 15, 2004), *at* http://www.ftc.gov/opa/2004/06/canspam2.htm.

would be largely powerless to identify those responsible for misusing the Registry."[298] FTC chairman Timothy Muris said that "any do-not-spam registry would be so open to abuse by spammers that he would not sign up for it."[299] The Commission instead supported development of more robust domain-level authentication techniques for verifying senders, and announced it would hold an "Authentication Summit" in November to spur this effort.[300] Depending on the outcome of authentication efforts, the FTC stated that it would consider mandating adoption of an authentication system, and might revisit the option of a registry if the spam problem persisted despite effective authentication.[301]

¶ 78 Second, the FTC evaluated the prospects of a bounty system, as required under CAN SPAM and as urged by scholars such as Lawrence Lessig.[302] The Commission recommended that any such system be limited to "insiders with high-value information," rather than open to any bounty hunter, and that eligibility for rewards be restricted to "imposition of a final court order, rather than to collection of civil penalties."[303] The FTC noted that some violations of CAN SPAM, such as failure to include a valid physical postal address, are obvious and readily identifiable by the government; thus, a reward-based system to identify these violations would incur needless cost.[304] However, information on less obvious violations (such as the use of open relays) or on the spammer's identity would be more valuable since it is harder for the government to obtain.[305] The Commission argued that "cybersleuths," or private parties who "expend[] personal time and effort to track down information about spammers," are unlikely to provide admissible evidence of a spammer's identity since they lack subpoena power and can rarely establish a sender's knowledge or culpability.[306] The FTC also seemed to believe that the existence of volunteer spam-fighting groups reduced the need to pay

298. Fed. Trade Comm'n, *National Do Not Email Registry: A Report to Congress* 6 (June 2004), *available at* http://www.ftc.gov/reports/dneregistry/report.pdf.

299. Amit Asaravala, *FTC Says No to Antispam Registry*, WIRED NEWS, June 15, 2004, *at* http://www.wired.com/news/technology/0,1282,63862,00.html.

300. *Id.*; *see also* Fed. Trade Comm'n, Press Release, *FTC, NIST to Host E-mail Authentication Summit* (Sept. 15, 2004), *at* http://www.ftc.gov/opa/2004/09/emailauth.htm.

301. Fed. Trade Comm'n, *supra* note 298, at ii.

302. *See, e.g.*, Lawrence Lessig, *Code Breaking: A Bounty on Spammers*, CIO INSIGHT, Sept. 16, 2002, *at* http://www.cioinsight.com/article2/0,1397,1454839,00.asp (proposing a requirement that spam messages be labeled and that "the first person to track down a spammer violating the labeling requirement . . ., upon providing proof to the Federal Trade Commission, be entitled to $10,000 to be paid by the spammer"); Amit Asaravala, *With This Law, You Can Spam*, WIRED NEWS, Jan. 23, 2004, *at* http://www.wired.com/news/business/0,1367,62020,00.html?tw=wn_story_related (quoting Stanford Law School professor Lawrence Lessig as supporting a bounty hunter system in saying that a "spammer needs to realize that there are 50,000 entities on the Net willing to track him down"). Professor Lessig famously offered to resign his position at Stanford if the bounty system were implemented but did not reduce spam. *See, e.g.*, *Lofgren Calls for Tagging Spam*, SILICON VALLEY/SAN JOSE BUS. J., Apr. 28, 2003, *available at* http://sanjose.bizjournals.com/sanjose/stories/2003/04/28/daily7.html.

303. Fed. Trade Comm'n, Press Release, *FTC Assesses Reward System for Catching Spammers* (Sept. 16, 2004), *at* http://www.ftc.gov/opa/2004/09/bounty.htm.

304. Fed. Trade Comm'n, *A CAN-SPAM Informant Reward System: A Report to Congress* at 20–21 (Sept. 2004), *available at* http://www.ftc.gov/reports/rewardsys/040916rewardsysrpt.pdf.

305. *Id.* at 21–22.

306. *Id.* at 23–24.

bounties to hunt down spam senders.[307] Overall, the Commission implied that government employees could produce the admissible evidence necessary to enforce CAN SPAM against the worst offenders more cheaply than cybersleuths could.[308] Thus, the FTC supported focusing a reward system on insiders or whistleblowers.[309] While acknowledging that establishing the correct level of incentives for insiders to provide information would be difficult, the FTC advocated rewards between $100,000 and $250,000.[310] The Commission recommended that Congress, if it decided to create a reward system, include five essential elements: limiting eligibility to imposition of a final court order, funding rewards through appropriations rather than collected penalties, limiting rewards to insiders with high-value information, allowing the FTC to set reward amounts without review or appeal, and creating rewards sufficient to induce whistleblowing.[311] Finally, the FTC suggested that Congress protect informants' identities, make it unlawful to provide false information through the reward system, and state explicitly that the FTC cannot provide immunity to whistleblowers.[312] Overall, the FTC's report contemplates, at best, a highly limited reward system unlikely to produce major benefits.[313]

f. Wireless Spam

¶ 79 The CAN SPAM Act anticipates the problem of "unwanted mobile service commercial messages," or cell phone spam.[314] The Act requires the Federal Communications Commission ("FCC"), in consultation with the FTC, to create rules

307. *See* Jonathan Krim, *Cash Bounties for Spammers Win Limited FTC Backing*, WASH. POST, Sept. 17, 2004, at E1.

308. Fed. Trade Comm'n, *supra* note 304, at 25.

309. *Id.* at 26–28.

310. *Id.* at 40 (taking into account the large downside risk faced by the informant).

311. *Id.* at 34.

312. *Id.* at 41.

313. The Commission itself noted that "in the case of the bounty scheme operated by the Securities and Exchange Commission ("SEC"), the SEC has rewarded only three informants since the inception of its bounty scheme in 1988. Insider informants are . . . trusted associates . . . with whom the insider trader has a relationship of trust, or they may be implicated in the illegal insider trading activity. These factors are possible reasons for the infrequent use of the SEC bounty scheme." *Id.* at 28 (internal citations omitted). The FTC's decision to limit rewards to similarly-situated insiders seems questionable in light of this precedent.

314. 15 U.S.C. § 7712(d). The Act defines "mobile service commercial message" as "a commercial electronic mail message that is transmitted directly to a wireless device that is utilized by a subscriber of commercial mobile service." "Commercial mobile service" is defined in reference to 47 U.S.C. § 332(d), which refers to "any mobile service . . . that is provided for profit and makes interconnected service available (A) to the public or (B) to such classes of eligible users as to be effectively available to a substantial portion of the public, as specified by regulation by the Commission." In turn, "mobile service" is defined under 47 U.S.C. § 153(27) as

> a radio communication service carried on between mobile stations or receivers and land stations, and by mobile stations communicating among themselves, and includes (A) both one-way and two-way radio communication services, (B) a mobile service which provides a regularly interacting group of base, mobile, portable, and associated control and relay stations (whether licensed on an individual, cooperative, or multiple basis) for private one-way or two-way land mobile radio communications by eligible users over designated areas of operation, and (C) any service for which a license is required in a personal communications service.

protecting consumers against such messages within 270 days.[315] The FCC must "consider the ability of a sender of a commercial electronic mail message to reasonably determine that the message is a mobile service commercial message" in crafting the rules.[316] Within this constraint, the FCC must set rules allowing mobile service subscribers to avoid receiving messages unless they give prior consent and allowing message recipients to opt out of future messages electronically.[317] The Act requires the FCC to consider the relationship between mobile service providers and their subscribers in deciding whether to allow providers to transmit these messages to subscribers; if the FCC exempts providers from these rules, it must mandate that subscribers may opt out of messages from providers when signing up for the service and when paying bills.[318] The FCC must also consider how message senders can comply with these rules given the "unique technical aspects" of mobile devices.[319]

¶ 80 The FCC published rules for spam on cell phones and wireless devices (such as personal digital assistants, or PDAs) in September 2004.[320] The FCC's rules prohibit anyone from sending a mobile service commercial message unless the sender has the recipient's "express prior authorization;" is forwarding the message to her own address; is forwarding to another address without compensation and without the message advertising for the forwarding entity; or unless the message is to a domain not classified by the FCC as a wireless domain for at least thirty days.[321] Mobile service providers are expressly not exempt from these requirements; the FCC followed Congress' mandate to evaluate the service provider-subscriber relationship and concluded that messages "sent by CMRS providers are not fundamentally different from those sent by other senders."[322] In addition, senders must follow six requirements: stop transmitting messages within ten days of an "opt-out" request by a recipient; include an electronic opt-out mechanism; allow recipients who authorize messages to opt-out using the same electronic means by which they initially acceded to messages; ensure that at least one opt-out option does not create additional charges for the subscriber; identify itself in the message so the recipient can determine that the sender is authorized; and remain capable of receiving opt-out requests for at least thirty days after transmitting the message.[323]

¶ 81 In its definition of "Mobile Service Commercial Message," the FCC warned that a "commercial message is presumed to be a mobile service commercial message if it is sent or directed to any address containing a reference, whether or not displayed, to an Internet

315. 15 U.S.C. § 7712(b).
316. *Id.* § 7712(c).
317. *Id.* § 7712(b)(1), (2).
318. *Id.* § 7712(b)(3).
319. *Id.* § 7712(b)(4).
320. Fed. Commc'ns Comm'n, *Rules and Regulations Implementing the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003; Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, 69 Fed. Reg. 55,765 (Sept. 16, 2004) (to be codified at 47 C.F.R. pt. 64).
321. *Id.* (listing modifications to 47 C.F.R. § 64.3100(a)). Note that entities can send such messages to recipients in domains not listed by the FCC for thirty days only if the sender "does not knowingly initiate a mobile service commercial message." 47 C.F.R. § 64.3100(a)(4).
322. Fed. Commc'ns Comm'n, *supra* note 320, at 55,773.
323. 47 C.F.R. § 64.3100(b).

domain listed on the FCC's wireless domain names list."[324] The Commission limited express prior authorization by a recipient to the specific sender authorized, unless the recipient expressly agreed to include affiliated entities when granting permission.[325] Authorization requests must include specified disclosures, including that the subscriber may be charged by her wireless service provider for the messages and that she may revoke authorization at any time.[326] Finally, wireless service providers must provide e-mail domains they use specifically for wireless messages to the FCC,[327] which will list them on its Web site.[328] The new rules apply only to electronic mail messages, not text messages (such as short message service, or SMS,[329] transmissions).[330] However, the FCC stated that the Telephone Consumer Protection Act's "prohibition on using automatic telephone dialing systems to make calls to wireless phone numbers applies to text messages."[331] Cellular service provider Verizon Wireless employed a similar theory to sue spammers who sent Internet messages that were converted to SMS messages and routed to Verizon subscribers' phones.[332]

¶ 82 The FCC's rules follow CAN SPAM in creating different standards for wireless spam than for regular unsolicited messages. Before sending a message to a user's cell phone, an advertiser must get the user's consent, but the advertiser can transmit the message to the recipient's computer without advance permission. The "walled garden" provision that blocks unsolicited messages only to listed, exclusively wireless e-mail domains will help legitimate advertisers avoid violating the new rules,[333] but may also create opportunities for spammers to target wireless recipients—for example, with offers to switch one's provider.

g. Results

¶ 83 CAN SPAM has been widely derided as ineffective.[334] Enforcement of CAN

324. *Id.* § 64.3100(c)(7).
325. *Id.* § 64.3100(d)(3).
326. *Id.* § 64.3100(d)(5).
327. *Id.* § 64.3100(e).
328. *Id.* § 64.3100(c)(7).
329. *See* WEBOPEDIA, *Short Message Service*, *at* http://www.webopedia.com/term/s/short_message_service.html (last modified May 6, 2004) (defining SMS).
330. Fed. Commc'ns Comm'n, *supra* note 320, at 55,767 (noting that the FCC "agree[s] with those commenters who maintain that phone-to-phone SMS is not captured by section 14 of the CAN SPAM Act because such messages do not have references to Internet domains").
331. *Id.*
332. *See* Brian S. McWilliams, *Lawsuit Over Cell Phone Spam*, PC-RADIO.COM, July 21, 2004, *available at* http://www.pc-radio.com/verizon-spam.html.
333 *See* Jonathan Krim, *FCC Blocks Spam on Wireless Devices*, WASH. POST, Aug. 5, 2004, at E1.
334 *See, e.g.*, Jeffrey D. Sullivan & Michael B. De Leeuw, *Spam after CAN-SPAM: How Inconsistent Thinking Has Made a Hash Out of Unsolicited Commercial E-mail Policy*, 20 SANTA CLARA COMPUTER & HIGH TECH. L.J. 887, 902–05 (2004) (noting that most unsolicited commercial e-mail does not comply with CAN SPAM and that governmental enforcement efforts have been weak to date); Matthew B. Prince, *Countering Spam: How to Craft an Effective Anti-Spam Law* 3, (International Telecommunication Union World Summit on the Information Society, Discussion Paper, 2004), *at* http://www.itu.int/osg/spu/spam/contributions/Background%20Paper_How%20to%20craft%20and%20effective%20anti-spam%20law.pdf (last visited Feb. 16, 2005) (noting that three months after CAN SPAM passed, only 3% of messages complied, and that by June 2004 compliance fell to 1%).

SPAM's criminal provisions has been quite limited to date. In April 2004, U.S. prosecutors charged four men in Detroit, Michigan with sending fraudulent messages advertising weight-loss products; Federal Trade Commission investigators stated they had received over 10,000 complaints about this particular spam source.[335] In the first criminal conviction under CAN SPAM, a Los Angeles resident agreed to plead guilty to a single felony charge for "wardriving"—driving around Venice, CA while using his laptop's wireless Internet capability to detect unsecured wireless networks and employing those networks to send spam advertising pornographic Web sites.[336] In May, the FBI promised Congress it would increase efforts and stated it had targeted fifty spam senders for prosecution in late 2004.[337]

¶ 84 Civil enforcement has also been limited. The Massachusetts Attorney General sued a Florida man and his company that sent spam advertising pre-approved mortgages and claimed to have a business address in the state; the suit alleged that the company failed to include a working opt-out address in messages, did not identify the messages as advertising, and used a non-functional sender address.[338] The defendants recently settled the case, agreeing to pay a $25,000 fine and to comply with CAN SPAM.[339] A number of ISPs have filed suit in federal court to pursue large-scale spammers.[340] Microsoft has sued defendants who sent sexually explicit spam without labeling the messages as required by CAN SPAM.[341] The FTC has pursued some civil actions against spammers, winning a freeze on the assets of a Florida spammer[342] and suing Australian company Global Web Promotions with the help of Australia's Competition and Consumer Commission.[343]

---

335. '*Can Spam*' *Arrests Made*, WASH. POST, Apr. 29, 2004, at E2; *see also* Press Release, U.S. Dep't of Justice, Department of Justice Announces Arrests of Detroit-Area Men on Violations of the 'CAN SPAM' Act (Apr. 29, 2004), *at* http://www.usdoj.gov/opa/pr/2004/April/04_crm_281.htm (announcing a criminal complaint against four men for sending "hundreds of thousands of messages advertising medical and other products").

336. Richard Shim, '*Wardriving*' *Conviction Is First Under Can-Spam*, CNET NEWS.COM (Sept. 30, 2004), *at* http://news.com.com/Wardriving+conviction+is+first+under+Can-Spam/2100-7351_3-5390722.html (noting that Nicholas Tombros pleaded guilty to "unauthorized access to a computer to distribute multiple commercial spam messages" and faces up to three years in federal prison).

337. *See* Declan McCullagh, *FBI Plans Spammer Smackdown*, CNET NEWS.COM, May 20, 2004, *at* http://news.com.com/2100-1028_3-5217299.html.

338. *See* Press Release, Off. Mass. Att'y Gen., AG Reilly Sues Deceptive Spammer For Violating Massachusetts Law, Federal CAN SPAM Act (July 1, 2004), *at* http://www.ago.state.ma.us/sp.cfm?pageid=986&id=1257; *see also* Jerry Kronenberg, *Mass. AG is First Using Anti-spam Law*, BOSTON HERALD, July 2, 2004, at 23.

339. Hiawatha Bray, *Spammer To Pay $25,000 Settlement: Mass. Lawsuit Was The First By A State Under US E-mail Law*, BOSTON GLOBE, Oct. 8, 2004, at D3.

340. *See* Hansell, *4 Big Internet Providers File Suits To Stop Leading Senders of Spam*, *supra* note 59, at A1.

341. *See* Press Release, Microsoft Corp., Microsoft Sues Spammers Who Violate CAN-SPAM "Brown Wrapper" Rule (Dec. 2, 2004), *at* http://www.microsoft.com/presspass/press/2004/dec04/12-02BrownPaperPR.asp.

342. Press Release, Fed. Trade Comm'n, FTC Sues Florida Man for Illegal Spam and False "Human Growth Hormone" Product Claims (July 29, 2004), *at* http://www.ftc.gov/opa/2004/07/creaghan.htm.

343. Press Release, Fed. Trade Comm'n, FTC Announces First Can-Spam Act Cases (Apr. 29, 2004), *at* http://www.ftc.gov/opa/2004/04/040429canspam.htm.

¶ 85 Importantly, spam's share of e-mail traffic has increased since CAN SPAM passed.[344] Internet research firm JupiterResearch found that more than one-third of e-mail marketing offers in its study did not comply with the law; nearly one-quarter of advertisers did not respect "opt-out" requests, and 16% contacted recipients who opted out after the mandated period of ten business days.[345] E-mail marketers generally included a working opt-out mechanism but failed to follow the law's more detailed provisions.[346] Some senders are trying to evade the law's requirements through tactics such as including opt-out information in an embedded graphic not visible to users with text-only mail clients, or claiming that their message's "primary purpose" is non-commercial.[347] One spammer exploited a vulnerability in Microsoft's Internet Explorer Web browser to download and run a program on the computers of users who clicked the removal link in its messages, allowing the spammer or others to use the infected computer as a spam relay or to capture data such as passwords.[348] Filtering software firm SurfControl found that 95% of spammers were "ignoring the law completely,"[349] and e-mail security firm MX Logic found only 6% of spam complied with the Act in November 2004.[350] Spammers have also reacted to CAN SPAM by shifting activities to foreign jurisdictions such as China that do not criminalize their activities.[351] The director of the anti-spam organization Spamhaus Project[352] stated that seventy percent of spam originates in China from American senders who have outsourced message transmission.[353] Research firm Commtouch found that 68% of Web sites advertised through spam were located in China in October 2004.[354] Anti-spam vendor MX Logic argues that the shift to sending spam from foreign servers is an important factor in the

344. *See* Hansell, *4 Big Internet Providers File Suits To Stop Leading Senders of Spam*, *supra* note 59, at A1 (noting that Brightmail found 58% of e-mail to be spam in December 2003, but 62% in February 2004).

345. Press Release, JupiterResearch, JupiterResearch Finds Legitimate E-Mail Marketers Struggling with Federal Can-Spam Compliance (Apr. 20, 2004), *at* http://www.jupitermedia.com/corporate/releases/04.04.20-newjupresearch.html.

346. *Id.*

347. Chris Ulbrich, *Spam Travels into Gray Area*, WIRED NEWS, Jan. 29, 2004, *at* http://www.wired.com/news/technology/0,1282,62087,00.html.

348. *See* John Leyden, *Click Here to Become Infected*, REGISTER, Sept. 22, 2004, *at* http://www.theregister.co.uk/2004/09/22/opt-out_exploit/ (noting that "if users click on the remove link and scroll down the page [this] triggers a DragDrop JavaScript exploit . . . [that] uses an IE bug to download and run an EXE file").

349. *See* Ulbrich, *supra* note 347.

350. John P. Mello Jr., *CAN-SPAM Compliance Hits New High of 6 Percent*, TECHNEWSWORLD, Dec. 14, 2004, *at* http://www.technewsworld.com/story/38945.html (noting that the 6% compliance rate is the highest ever reported by e-mail security company MX Logic).

351. Mei Fong, *Chinese Servers Helping E-Mailers Spam the Globe*, WALL ST. J., Mar. 19, 2004, at B1 (noting that "in Asia-Pacific, only South Korea, Japan and Australia have antispam legislation").

352. *See* The Spamhaus Project, *at* http://www.spamhaus.org/ (last visited Feb. 8, 2005).

353. Graeme Wearden, *Russia and China 'Behind Current Spam Deluge,'* ZDNET UK, June 8, 2004, *at* http://uk.news.yahoo.com/040608/152/evi5t.html. The director, Steve Linford, also noted the role of Russian organized crime in "supplying US-based spammers with details of compromised PCs that can be used to send out their unsolicited commercial messages." *Id.*

354. Colin Galloway, *Spammers Hide Behind the Great Wall*, ASIA TIMES ONLINE, Dec. 14, 2004, *at* http://www.atimes.com/atimes/China/FL14Ad02.html.

declining compliance with the legislation.[355] Thus far, spam senders have responded to CAN SPAM with evasion, defiance, and a tiny measure of compliance.

2. State Laws

¶ 86 A few states have adopted spam legislation that avoids CAN SPAM's pre-emption. For example, Maryland adopted a criminal prohibition on breaking into a computer to relay messages, knowingly deceiving ISPs or recipients about a sender's identity or a message's origin, and using false information to register fifteen or more e-mail addresses if one uses those addresses to send spam.[356] Violators can receive up to five years in prison and fines of $25,000; the attorney general can sue for civil penalties of up to $25,000 per day, or between $2 and $8 per message sent.[357] Spammers face liability if they send messages to a Maryland resident, and both the attorney general and local police can file charges.[358] The measure is touted as "one of the strongest anti-spam laws in the nation."[359] Maryland also has legislation prohibiting sending commercial e-mail from the state, or to a resident, that uses a third party's domain name or address without permission, or includes false or misleading information in the subject or transmission path.[360] Violators are subject to civil liability for statutory minimum damages or actual damages to recipients, ISPs, or third parties whose domain name or address was used.[361] However, a state judge recently ruled that the law is unconstitutional because it regulates commerce outside Maryland in violation of the Commerce Clause.[362]

¶ 87 Virginia imposes felony liability upon any person who uses a computer with the intention of "falsify[ing] or forg[ing] electronic mail transmission information or other routing information in any manner in connection with the transmission of unsolicited bulk electronic mail."[363] The state also criminalizes selling, distributing, or possessing software primarily designed or produced for such falsification, or that is marketed for that purpose. The criminalization, however, requires that the software have "only limited commercially significant purpose or use" outside of the illegal activity.[364] Anyone "whose property or person is injured by reason of a violation" may sue for actual or liquidated damages, as well as attorneys' fees.[365] The state convicted Jeremy Jaynes, a prolific spammer, in November 2004 in the nation's first felony prosecution for unlawful

355. David McGuire, *Report: More Spam Violates Law*, TECHNEWS.COM, June 9, 2004, *at* http://www.washingtonpost.com/ac2/wp-dyn/A29136-2004Jun9.

356. Tom Stuckey, *Maryland Anti-spam Law Kicks In*, WASH. TIMES, Oct. 1, 2004, *available at* http://washingtontimes.com/metro/20040930-100341-4159r.htm.

357. *Id.*

358. Scott Shane, *Bill Would Make Spammers' E-mail Tactics a Crime*, BALT. SUN, Apr. 15, 2004, at 1B.

359. Stuckey, *supra* note 356.

360. MD. CODE ANN., COM. LAW II § 14-3002(b) (2004).

361. *Id.* § 14-3003.

362. *See* David Snyder, *Judge Faults Md. Anti-Spam Statute: U.S. Commerce Clause Cited*, WASH. POST, Dec. 15, 2004, at E5.

363. VA. CODE ANN. § 18.2-152.3:1(A)(1) (2003).

364. *Id.* § 18.2-152.3:1(A)(2).

365. *Id.* § 18.2-152.12(B), (C). Liquidated damages and attorneys' fees are available if the defendant knowingly violates an electronic mail service provider's terms of use, or if those terms of use are available on the provider's Web site.

distribution of spam.[366] Jaynes was sentenced to nine years in prison.[367]

¶ 88 Florida prohibits using a computer in the state to send, or transmitting to a state resident, a spam message that: (1) uses a third party's domain name without permission, (2) falsifies routing information, (3) has a misleading subject line, or (4) includes false information in the message body intended to cause damage to the recipient's receiving device; however, one escapes liability if the message is caused by a virus, without the sender's knowledge or consent.[368] The Sunshine State also forbids distributing software that falsifies routing information.[369] Enforcement means are limited to the Florida Department of Legal Affairs, interactive computer services, telephone companies, and cable providers.[370]

¶ 89 California enacted anti-spam legislation that creates criminal penalties[371] for sending unsolicited commercial e-mail advertising from California or to a California e-mail address.[372] The new legislation forbids e-mail advertising that uses a third party's domain name without permission, has falsified header information, or has a subject line that a reasonable person would find likely to mislead the recipient about its contents or subject matter.[373] Recipients of unsolicited commercial messages, ISPs, and the California Attorney General can sue for either actual or liquidated damages; liquidated damages constitute up to $1000 per unlawful message, with a limit of $1 million per incident.[374] If the defendant established and implemented reasonable measures to prevent violations, liquidated damages can be reduced to $100 per e-mail, with maximum total damages of $100,000 per incident.[375] The act prevents harvesting e-mail addresses, using scripts to produce e-mail addresses, or using scripts to create multiple e-mail accounts to send unsolicited commercial messages from California or to a California e-mail

366. *See* Karin Brulliard, *Jury Finds 2 Guilty of Felony Spam*, WASH. POST, Nov. 4, 2004, at E1 (noting that Jaynes and his sister were each convicted on three felony counts).

367. Linda Rosencrance, *Spammer Sentenced to Nine Years in Jail*, PC WORLD, Nov. 5, 2004, *available at* http://www.pcworld.com/news/article/0,aid,118493,00.asp.

368. *See* S.B. 2574, 2004 Leg., Reg. Sess. (Fla. 2004), *available at* http://www.flsenate.gov/cgi-bin/view_page.pl?Tab=session&Submenu=1&FT=D&File=sb2574er.html&Directory=session/2004/Senate/bills/billtext/html/ (last visited Feb. 16, 2005); *see also Bush signs bills targeting spam, offensive names*, USA TODAY, May 26, 2004, *available at* http://www.usatoday.com/tech/news/techpolicy/2004-05-26-spam-bill-fl_x.htm.

369. Fla. S.B. 2574, *supra* note 368.

370. *Id.*

371. CAL. BUS. & PROF. CODE § 17500 (2005) (criminalizing violations of the relevant section of California's business and professions code, where the spam legislation will be codified, as misdemeanors).

372. *See* S.B. 186, 2003–2004 Leg., 2003–2004 Sess. (Cal. 2004), *available at* http://www.leginfo.ca.gov/pub/03-04/bill/sen/sb_0151-0200/sb_186_bill_20030924_chaptered.pdf (relevant provision to be codified at CAL. BUS. & PROF. CODE § 17529.2); *see also* Steve Lawrence, *Schwarzenegger Signs Bodysurfing, Battered Women Bills*, NORTH COUNTY TIMES, Sept. 17, 2004, *available at* http://www.nctimes.com/articles/2004/09/18/news/state/14_38_529_17_04.txt (noting that California governor Arnold Schwarzenegger signed a bill to "allow Internet service providers, the attorney general and recipients of commercial 'spam' e-mail to recover damages of up to $1,000 per unsolicited e-mail which doesn't disclose a valid e-mail address contact and the name and location of the sender").

373. Cal. S.B. 186, *supra* note 372.

374. *Id.* (to be codified at CAL. BUS. & PROF. CODE § 17529.8).

375. *Id.* (to be codified at CAL. BUS. & PROF. CODE § 17529.8(b)).

address.[376] The bill modifies existing California e-mail statutes, which survived CAN SPAM pre-emption, by limiting e-mail service providers to recovery under only one provision for the same unsolicited e-mail advertising message.[377]

¶ 90 Ohio,[378] Minnesota,[379] and New Jersey[380] are debating spam legislation. While states have been slow to react to CAN SPAM, more are likely to follow Virginia and Maryland and listen to ISPs' urgings in crafting criminal prohibitions against spam.[381]

3. Other Actions

¶ 91 Initially, ISPs and others burdened by spam faced the challenge of finding legal theories to defend against unwanted messages; spam-specific statutes had not been codified. Providers such as AOL and Hotmail brought actions based on common-law claims, trademark law, and computer fraud and abuse statutes. These approaches provided early victories but also suffer limitations that make them less useful today,[382] particularly those approaches based on an information framework.

a. Common Law Suits

¶ 92 Early lawsuits by ISPs against organizations sending unwanted e-mail advertisements to their users advanced common law claims such as trespass to chattels. For example, the ISP Compuserve sued spammer Cyber Promotions and its president for sending unsolicited messages to Compuserve subscribers despite repeated orders to desist, and for circumventing efforts to block this flow of e-mail.[383] The District Court enjoined Cyber Promotions from sending any unsolicited e-mail advertisement to Compuserve members on a theory of trespass to chattels.[384] Trespass to chattels involves

376. *Id.* (to be codified at CAL. BUS. & PROF. CODE § 17529.4).

377. *Id.* (to be codified at CAL. BUS. & PROF. CODE § 17538.45(f)(4)).

378. *See* H.B. 383, 125th Gen. Assem., Reg. Sess. (Ohio 2004), *available at* http://www.legislature.state.oh.us/bills.cfm?ID=125_HB_0383. The Ohio Senate passed the bill in November 2004. *See* James Drew, *State Senate supports crackdown on Internet spam*, TOLEDO BLADE, Nov. 18, 2004, *available at* http://toledoblade.com/apps/pbcs.dll/article?AID=/20041118/NEWS24/411180506.

379. *See* H.F. 2498, 83d Leg., Reg. Sess. (Minn. 2003), *available at* http://www.revisor.leg.state.mn.us/cgi-bin/getbill.pl?session=ls83&version=latest&number=HF2948&session_number=0&session_year=2003; *see also* S.F. 2622, 83d Leg., Reg. Sess. (Minn. 2003), *available at* http://www.revisor.leg.state.mn.us/cgi-bin/getbill.pl?session=ls83&version=latest&number=SF2622&session_number=0&session_year=2003.

380. *See* S.B. 1037, 211th Leg., 2004–2005 Sess. (N.J. 2004), *available at* http://www.njleg.state.nj.us/2004/Bills/S1500/1037_r1.htm.

381. *See* Susan Levine, *Assembly Sends Spammers a Message; E-Mail Bill, Now in Ehrlich's Hands, Calls for Prison Time, Fines Up to $25,000*, WASH. POST, Apr. 14, 2004, at B1 (noting that the sponsor of the Maryland bill "envision[s] other states following suit").

382. *See* Associated Press, *Judge Delivers $1 Billion Spam Judgment*, WALL ST. J. ONLINE, Dec. 20, 2004, *at* http://online.wsj.com/article_print/0,,SB110349923676804327,00.html (reporting on an award of over $1 billion to an ISP who sued spammers under the federal Racketeer Influenced and Corrupt Organizations Act (RICO) and Iowa criminal law, but noting the plaintiff was not likely to collect the judgment).

383. *Compuserve Inc. v. Cyber Promotions, Inc.*, 962 F. Supp. 1015, 1019 (S.D. Ohio 1997).

384. *Id.* at 1019.

unauthorized use of personal (rather than real) property that deprives the possessor of her property for a substantial time, damages the property, or causes harm to the possessor of an item in which she has a legally protected interest.[385] The trespass must cause actual damage.[386] The court found that computer communication through electronic signals was sufficiently physical to support a trespass claim,[387] and held that the burden Cyber Promotions' messages placed on the Compuserve computer system impaired the network's value, thus creating liability.[388]

¶ 93 While Compuserve's willingness to accept e-mail created "at least a tacit invitation for anyone on the Internet to utilize plaintiff's computer equipment to send e-mail to its subscribers," the court found that Compuserve revoked that consent in a discussion with Cyber Promotions' president, and that this consent was subject to express limitations.[389] The court enjoined Cyber Promotions from sending spam to Compuserve users, noting that "no government entity has undertaken to regulate the Internet in a manner that is applicable to this action," and that "if there were some applicable statutory scheme in place this Court would not be required to apply paradigms of common law to the case at hand."[390] Other courts have followed *Cyber Promotions* in applying trespass to chattels in spam litigation.[391] However, in a lawsuit based on non-commercial spam, the Supreme Court of California rejected a trespass to chattels claim, holding that the spam must harm the plaintiff's computer system in order to incur liability; harms based on message content are not sufficient.[392]

¶ 94 Common law actions against e-mail advertisers have three primary drawbacks. First, theories such as trespass to chattels developed in a property context quite different from that involved in Internet communications, and adapting them to this new setting can be problematic.[393] For instance, courts often struggle to define the chattel at issue, use an insufficient threshold for the damage requirement, or use a trespass to real property approach rather than trespass to chattels.[394] Second, common law claims are more effective, in theory and in practice, against larger and larger-volume spammers.[395] Large senders are more likely to have assets available to satisfy a judgment, and advertisers

385. *Id.* at 1020–22.
386. *Id.* at 1023.
387. *Id.* at 1021.
388. *Id.* at 1027.
389. *Id.* at 1023–24.
390. *Id.* at 1026.
391. *See, e.g.*, *Am. Online, Inc. v. IMS*, 24 F. Supp. 2d 548 (E.D. Va. 1998) (granting summary judgment to AOL on trespass to chattels claim); *Hotmail Corp. v. Van$ Money Pie Inc.*, 47 U.S.P.Q.2d (BNA) 1020 (N.D. Cal. 1998) (issuing preliminary injunction against use of Hotmail accounts to send spam and falsification of return addresses to include the hotmail.com domain).
392. *Intel Corp. v. Hamidi*, 71 P.3d 296, 300 (Cal. 2003) (stating that "under California law the tort does not encompass, and should not be extended to encompass, an electronic communication that neither damages the recipient computer system nor impairs its functioning").
393. *See* Dan Hunter, *Cyberspace as Place and the Tragedy of the Digital Anticommons*, 91 CAL. L. REV. 439, 483–88 (2003).
394. *Id.* at 486–88.
395. *See* Sorkin, *supra* note 65, at 367 (noting that 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").

who transmit large volumes of messages have a greater chance of exceeding the threshold for damage to a recipient's computer system. Finally, common law claims focus on message volume and authorization, not on information value for recipients. Theories like trespass to chattels focus on cost, not cost relative to benefit, although an enterprising court could stretch the concept of implied license to use the chattel to cover situations where the messages confer sufficient benefits to avoid liability.

b. Trademark Law

¶ 95 ISPs have used trademark laws, such as the federal Lanham Act,[396] to sue spammers who use their marks to falsify messages' origins. For example, AOL won summary judgment against spammer LCGM for sending ninety-two million unsolicited messages advertising pornographic Web sites to AOL's users over a period of six months.[397] LCGM forged its messages' headers so that the e-mail appeared to come from AOL's domain.[398] In granting summary judgment and injunctive relief to AOL, the District Court found violations of the Lanham Act for false designation of origin and for dilution.[399] ISPs often include trademark claims along with common law claims in suing senders who include their marks in unsolicited e-mail ads.[400] Microsoft was granted summary judgment against a California man who claimed to be associated with the company's Windows Update Service and who used spam to convince users to download toolbar software onto their computers.[401] Microsoft alleged trademark infringement, false advertising, and cybersquatting, and won $4 million, including $352,000 in attorneys' fees, along with forfeiture of a series of domain names that included Microsoft trademarks.

¶ 96 Trademark law protects against fraudulent use of recognizable designations of origin for e-mail—only AOL and its authorized users can send messages purporting to be from aol.com. However, trademark doctrine does not help users or ISPs distinguish whether messages that do not misuse marks have value. Thus, trademark claims are helpful against fraudulent spam, but not relevant to e-mail advertising that does not try to deceive recipients about its origins.

c. Computer Fraud and Abuse Laws

¶ 97 E-mail advertising may violate state or federal laws regulating computer fraud and abuse. For example, in AOL's case against LCGM, it won summary judgment on claims that LCGM exceeded authorized access to and impaired the ISP's computers, violating the federal Computer Fraud and Abuse Act (CFAA).[402] While the CFAA imposes a minimum damages threshold of $5000 for liability, LCGM was prevented by the court

396. 15 U.S.C. § 1051 *et seq.* (2004).
397. *Am. Online, Inc. v. LCGM, Inc.*, 46 F. Supp. 2d 444, 447–48 (E.D. Va. 1998).
398. *Id.* at 448.
399. *Id.* at 449–50, 451–53.
400. *See, e.g.*, *Hotmail*, 47 U.S.P.Q.2d (BNA) at 1020; *IMS*, 24 F. Supp. 2d at 551.
401. Matt Hines, *Microsoft Awarded $4 Million in Spam Suit*, ZDNET, July 16, 2004, *at* http://news.zdnet.com/2100-3513_22-5272776.html.
402. *LCGM*, 46 F. Supp. 2d at 450–51; *see* Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2005).

from opposing AOL's assertions of harm greater than $5000 because of discovery abuses.[403] The court also found LCGM violated Virginia's Computer Crimes Act by using AOL's computer network without authorization and converting AOL's property by obtaining free advertising.[404] Similarly, Hotmail won a preliminary injunction preventing spammers from sending e-mail to Hotmail users or using Hotmail's marks based in part on a likelihood of success of winning its CFAA claim.[405]

¶ 98 Computer fraud and abuse laws have three shortcomings. First, the federal CFAA has a damages threshold of $5000.[406] Proving damages in excess of this level may be difficult, particularly given the challenges of allocating relatively fixed costs such as Internet bandwidth and disk storage to a particular subset of e-mail messages.[407] Second, state laws impose lower thresholds (which suffer the same conceptual challenge) but force ISPs to prove sufficient damages in that state's jurisdiction.[408] This could increase the problem of meeting the damages floor if an ISP operated servers that received the spam in multiple states. Finally, like common law actions, computer fraud and abuse laws do not analyze the value of messages to users unless courts incorporate this calculation in deciding whether access is "authorized" by the recipient.

d. Financial laws

¶ 99 Certain spam may violate financial laws, such as Securities Exchange Commission regulations or the Securities Act of 1933. For example, the SEC settled a case alleging violation of the Securities Act through spam that failed to disclose the sender's interest in the stock the messages promoted in return for an injunction and $15,000 fine.[409] Financial laws are useful in addressing spam's problems because they address messages' information content. Users benefit from disclosure of certain relevant data in evaluating stock offers, such as the promoter's financial interest in the company, and this consideration applies regardless of whether recipients are solicited to invest through e-mail or postal mail. These laws apply to a subset of e-mail advertising but should be applied consistently across advertising media.

4. Challenges of Legal Regulation

¶ 100 Legal spam regulation suffers a number of shortcomings. First, jurisdictional issues in spam are difficult—senders can reach recipients worldwide via e-mail from

403. *LCGM*, 46 F. Supp. 2d at 446.
404. *Id.* at 451.
405. *Hotmail*, 47 U.S.P.Q.2d (BNA) at 1020.
406. 18 U.S.C. §§ 1030(a)(4), (a)(5)(B)(i).
407. *See, e.g.*, *Am. Online, Inc. v. Prime Data Sys.*, 1998 U.S. Dist. LEXIS 20226 at *8–10 (E.D. Va. 1998) (recommending default judgment against defendant e-mail advertisers who sent AOL over 130 million messages and acknowledging that AOL's "damages are as difficult to quantify as they are real").
408. *See, e.g.*, VA. CODE ANN. § 18.2-152.3 (2004) (stating that a person who violates the computer fraud statute is guilty of a Class 5 felony if the value of the property or services obtained is greater than $200, but guilty of a Class 1 misdemeanor if the value is less than $200).
409. SEC Fines Internet Stock Promoter Responsible for Massive Spam Campaign, SEC Litigation Release No. 15,959 (Oct. 27, 1998), *at* http://www.sec.gov/litigation/litreleases/lr15959.txt.

nearly any location.[410] As one area tightens legal controls on spam, senders relocate.[411] Second, effective spam legislation requires enforcement, and suing or prosecuting spammers may not be a top law enforcement priority in a time of budget cuts.[412] Third, spammers may shield assets from judgment by incorporating in friendly jurisdictions.[413] Fourth, a legislative "arms race" may parallel the technological arms race of spam; as legal requirements emerge, spam senders will tailor messages to evade them. Legal regulation alone is insufficient to control spam advertising.

D. Markets

¶ 101 Market-based regulatory methods attempt to re-order e-mail's cost structure, typically by increasing the sender's costs.[414] (As the New Chicago framework describes, though, these methods depend on legal or technological constraints that permit a market to operate; there is no "pure" market solution.[415]) The most common proposals look to the analogy of postal mail service, where senders purchase transport of messages at a low, but not trivial, cost, and try to duplicate this framework through technological constraints. For example, Microsoft chairman Bill Gates predicted that e-mail "postage" will play an important role in eliminating spam.[416] Software companies such as Goodmail offer e-mail stamps that trade unrestricted access to recipients through ISPs in exchange for a per-message payment.[417] Another concept, called "hash cash," requires a sender's computer to solve an arbitrary mathematical problem before transferring a

410. *See, e.g.*, Staff Writers and Wires, *U.S. taps Aussie spammer*, AUSTRALIAN IT, Apr. 30, 2004, *available at* http://www.spamcompliance.com.au/usaussiespammer (describing U.S. government civil action against Australian weight-loss and growth hormone advertisers but quoting Howard Beales, director of the consumer protection bureau at the Federal Trade Commission, that authorities must "buy the product and see who charges our credit card" since it is "virtually impossible to trace the email itself").

411. *See, e.g.*, Swidey, *supra* note 204, at 29 (noting that "as the noose has tightened around spammers, their arrangements have become even more layered and foggy, involving forged or hijacked computer addresses and Web-hosting services in China and Eastern Europe").

412. *See* Asaravala, *supra* note 299 (quoting California Attorney General Bill Lockyer as warning that "his office did not have the resources to track and prosecute spammers on its own" because it "had taken a 22 percent budget cut over the past four years").

413. *See, e.g.*, Swidey, *supra* note 204, at 29 (describing how Boca Raton, Florida, is considered "the spamming capital of the world" because "laws allow for maximum protection of assets").

414. This may be a fruitless task. Spam can be revenue-neutral with a response rate from recipients as low as .001%. Fallows, *supra* note 4, at 25. The per-message spam cost can be as low as .025 cents. Saul Hansell, *Totaling Up the Bill for Spam*, N.Y. TIMES, July 28, 2003, at C1.

415. Lessig, *The New Chicago School*, *supra* note 75, at 663; *see* Lessig, *The Law of the Horse*, *supra* note 74 at 507 (stating that "the market is able to constrain in this manner only because of other constraints of law and social norms: property and contract law govern markets; markets operate within the domain permitted by social norms").

416. *See* Saul Hansell, *Speech by Gates Lends Visibility to E-Mail Stamp In War on Spam*, N.Y. TIMES, Feb. 2, 2004, at C1.

417. *See* Goodmail Systems, *Frequently Asked Questions*, *at* http://www.goodmailsystems.com/faq.html (last visited Oct. 13, 2004) (noting that most users would have stamp costs included in their ISP charge and stating that Goodmail would enforce a "trusted unsubscribe" option on senders using its stamps).

message.[418] Hash cash imposes a cost in processing cycles that effectively limits the number of messages a sender can transfer. This limit would not affect most e-mail users, but would increase costs for bulk senders such as spammers.[419] ISPs would configure servers and clients to permit messages with hash cash "tokens" or e-stamps to bypass spam filters and blacklists.[420]

¶ 102 There are also methods employing legal constraints to increase senders' costs. For example, Microsoft has sued CheapBulletProof.com, claiming the company "actively recruit[s] spammers to use [its] services by trolling Internet forums frequented by spammers."[421] CheapBulletProof.com touts that its servers are located in China, "to ensure no problems arise from complaints generated by email you send."[422] The company's Web site includes a testimonial: "Thank you for providing such an invaluable service to spammers everywhere. Everyone who receives a spam email through your servers will be eternally grateful that you ensure they won't be shut down because of their practices. Where would we be without you. [sic]"[423] However, at least one of the company's partners is located in California[424], giving Microsoft a target for enforcing U.S.-based legal constraints on spam. The Microsoft suit, if successful, will force service providers who cater to spammers to incur extra costs to avoid suits—for example, by incorporating and operating only in locations such as China that do not penalize spammers. These service providers will pass on the costs to their customers, increasing the effective cost of spam messages.

¶ 103 There are also indirect, technological methods that increase the effective cost of e-mail messages to spam senders. For example, a recent study by networking equipment vendor Sandvine found that eighty percent of spam messages came from insecure home computers connected to broadband networks; the spammers used hacking techniques, worms, or Trojan horses to take control of the computers and to use them to relay messages.[425] ISPs and broadband providers (who frequently offer combined packages that include Internet access and e-mail accounts) could reduce this low-cost transport option by providing subscribers with security tools such as firewalls and virus software. Indeed, Boston University requires its students to have these protection measures as a

418. *See* Adam Back, *Hashcash – A Denial of Service Counter-Measure* (Aug. 1, 2002), *at* http://www.hashcash.org/papers/hashcash.pdf; *see also* Marguerite Reardon, *Finding a Way to Fry Spam*, CNET NEWS.COM, Feb. 24, 2004, *at* http://news.com.com/2008-1032-5164246.html.

419. *See* Hashcash.org, *Hashcash FAQ*, *at* http://www.hashcash.org/faq/ (last visited Oct. 13, 2004) (stating that for "a normal user . . . the CPU overhead per mail is negligible because you don't send that many mails; at worst your mail is delayed a few seconds before being sent on slow old hardware," but "hashcash is bad news for spammers because the hashcash stamp takes your CPU some work to compute").

420. *Id.*

421. Jonathan Krim, *Microsoft Takes Stands Against Spam, Sanctions*, WASH. POST, Sept. 23, 2004, at E1.

422. *Id.* Note that the company's Web site claims that "Our ISP allows us and our customers to send bulk email. They will never shut us down due to complaints." CheapBulletProof.com, *Cheap BP: Frequently Asked Questions*, *at* http://cheapbulletproof.com/?p=3 (last visited Sept. 23, 2004).

423. CheapBulletProof.com, *Cheap BP: Dedicated Servers*, *at* http://cheapbulletproof.com/?p=2 (last visited Sept. 23, 2004).

424. *Id.*

425. Hiawatha Bray, *Home PCs Big Source of Spam; Study Says 80% of Junk E-Mail Is Relayed Innocently*, BOSTON GLOBE, June 9, 2004, at D2.

prerequisite to connecting to the campus network.[426] Some commentators suggest that ISPs adopt similar mandatory measures to reduce spam.[427] Cutting down the number of computers vulnerable to abuse as spam relays would force senders to use their own computers and bandwidth to transmit messages, increasing their costs and enhancing the likelihood of detection and regulation. ISPs and Internet access providers could build the cost of security measures such as firewalls and anti-virus software into their fees; while this would increase the expense to users, this added cost would be offset by cost savings from reduced spam, reduced security breaches from viruses, and fewer technical support requests.[428]

¶ 104 Interestingly, this approach posits an information asymmetry in the market for Internet access and use: consumers do not sufficiently value the security of their information and computers, and the reduction in spam traffic from securing their machines, to purchase, install, and update firewall and anti-virus programs. Microsoft, for one, recognizes this problem in its approach to security in its latest update (Service Pack 2) to its Windows XP operating system. Service Pack 2 activates Windows XP's built-in firewall by default and installs a Security Center that monitors, and can automatically download updates to, programs such as anti-virus software.[429] Many ISPs and access providers require an initial visit from a technician to install equipment (such as a cable or DSL[430] modem) and software needed for Internet access and use; including security software or hardware in this process could solve the information asymmetry through the power of default settings, since most customers do not alter their initial configuration.

¶ 105 An additional indirect technological method would impose limits on how rapidly senders could transfer large volumes of messages over SMTP. In essence, ISPs would artificially limit the bandwidth available to most users to transfer e-mail messages. Legitimate high-volume senders, such as corporations or other organizations, could pay more for the ability to send messages more rapidly. This limit would affect few small-scale users, for whom increased delay in sending messages would not be noticeable. The transfer limit would have two benefits: it would increase direct costs to spammers, who would have to find an ISP without this limit or pay the price for greater effective bandwidth, and it would reduce spammers' ability to avoid costs indirectly by hijacking computers with broadband connections, since the value of doing so decreases.

---

426. Hiawatha Bray, *Colleges To Kids: Clean Up Those PCs*, BOSTON GLOBE, Sept. 6, 2004, at D2.

427. *Id.*

428. *But see* Johnson, Crawford, & Palfrey, Jr., *supra* note 174, at ¶ 33 (noting the risks to innovation, privacy, and communication in a world where "[a]n online dictator could also require as a condition of connection that each subsidiary network install suitable security software and follow specified practices").

429. *See* Gene Johnson, *Microsoft Rolling Out Windows Security Fix; Update Addresses Nagging Vulnerabilities*, WASH. POST, Aug. 6, 2004, at E1; *see also* Starr Andersen & Vincent Abella, *Changes to Functionality in Microsoft Windows XP Service Pack 2*, MICROSOFT TECHNET, Aug. 9, 2004, *at* http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/sp2chngs.mspx.

430. DSL is an abbreviation of "digital subscriber line," a technology that allows users to access the Internet at broadband speeds over phone lines. *See* WEBOPEDIA, *xDSL*, *at* http://www.webopedia.com/term/x/xdsl.html (last modified July 24, 2003).

¶ 106 Other approaches compensate recipients for accepting messages. For example, a professor at the Yale School of Management proposes a reward-based e-mail postage system where message senders compensate recipients in exchange for permitting transfer.[431] The system would be voluntary and would operate in conjunction with filtering software that permits recipients to determine a minimum postage level and which messages lacking postage (such as those from friends) to allow.[432] Recipients could prioritize messages based on postage amount, and advertisers would have to invest funds to increase the likelihood recipients would read their messages.[433] The method's inventors compare their approach to tradeable pollution rights, with the goal of "induc[ing] efficient allocation of our precious attention without government regulation."[434]

¶ 107 A third method, called "payment at risk," imposes a financial penalty on the sender if a message is rejected as spam or if the recipient indicates dissatisfaction.[435] For example, the "bonded sender"[436] system requires commercial e-mail senders to commit to reimbursement before transmitting messages.[437] Transmitted messages include a mechanism for the recipient to penalize the sender if the message is not valuable.[438] With other systems, there is a transfer of payment from sender to recipient if the recipient determines that the message is unwanted.[439] This approach may create adverse incentives for recipients who welcome the message. "Attention bonds" proposals cite different benefits to their approach, such as dynamic adjustment to the different opportunity costs of different recipients' time and the ability to deal with previously unknown message senders.[440] Critics note that a widely deployed payment-at-risk system requires a substantial investment in infrastructure to verify and collect payments, and point to new

---

431. Shyam Sunder, *A Free Market Solution to Spam*, CATO.ORG, Feb. 27, 2004, *at* http://www.cato.org/dailys/02-27-04.html.

432. *Id.*

433. *Id.*

434. *Id.* The author ignores the fact that tradeable pollution rights function only *because* of government regulation that penalizes emitters for exceeding those rights; without government enforcement, the pollution market collapses.

435. *See* Tim Weber, *Gates Forecasts Victory Over Spam*, BBC NEWS, Jan. 24, 2004, *at* http://news.bbc.co.uk/2/hi/business/3426367.stm (discussing Microsoft chairman Bill Gates' proposal for "payment at risk" at the World Economic Forum in Davos).

436. *See* Bonded Sender Program, *Frequently Asked Questions – General Questions*, *at* http://www.bondedsender.com/faqs/general.html (last visited Feb. 16, 2005) (stating that "[o]riginators of legitimate email post a financial bond to guarantee the integrity of their email campaign" while ISPs "identify bonded email and ensure it is delivered" and "recipients report unsolicited email . . . and the sender's bond is debited").

437. *See, e.g.*, Vanquish Labs, *FAQ*, *at* http://www.vanquish.com/faq.shtml (last visited Oct. 13, 2004).

438. *Id.*

439. *See* Hiawatha Bray, *A chance to board the e-mail gravy train*, BOSTON GLOBE, Mar. 15, 2004, at C3 (describing the Vanquish system and stating that if "a recipient thinks the message is spam, he can click on the bond icon [which] forces the sender to pay a small financial penalty . . . to the recipient to compensate him for the trouble of deleting the unwanted message"). It is not clear how the Vanquish system would prevent willing recipients from both using and collecting from bonded messages.

440. *See* Thede Loder, Marshall Van Alstyne, & Rick Wash, *Information Asymmetry and Thwarting Spam* 3, (SSRN Information Technology & Systems Working Paper Series, January 14, 2004) *available at* http://ssrn.com/abstract=488444.

opportunities for fraud, such as creating fake payment providers or inducing people to send bonded messages to collect payments.[441]

¶ 108 Market-based solutions to spam share a common weakness: their method must be more attractive to message senders than the default approach of blanket e-mails. This assumption requires one of two conditions to hold true. First, ISPs might block most or all non-compliant commercial messages, but would allow compliant ones to go through. Senders would face a very limited audience (and consequently limited revenue) for non-compliant messages. Second, users might respond more frequently or more positively to compliant messages, thereby giving compliant senders a net benefit relative to non-compliant senders. Thus, a mass movement by consumers to choose the bonded sender method could effectively shift the e-mail advertising model, while a similar move by advertisers might not have any effect, unless the response by recipients increased sufficiently to cover the system's additional cost. Senders considering whether to pay—in the form of a bond, e-mail stamp, computing cycles, or a micropayment to recipients—will do so only if the "free" alternatives are less attractive. For a market approach to work effectively, it would need well-functioning technological constraints, such as blacklists and filtering software (which might make the market solutions redundant), or heightened user responses to "legitimate" spam.

E. Norms

¶ 109 Originally, social pressures and conventions regulated (and largely prevented) unsolicited commercial use of e-mail. The first spam message did not appear until 1994, when an immigration lawyer posted an offer to over 6000 Usenet newsgroups, charging $95 to aid US immigrants in a lottery for visas (known informally as "green cards").[442] The efficacy of norms waned as the Internet community grew and its character shifted from academic to commercial. Today, vestiges of a norm-based approach linger in discussions about spam's "stigma,"[443] in concerns about legitimizing this kind of e-mail advertising,[444] and in the negative media treatment of spammers. However, norms have not proved strong enough to constrain spam's volume or content and have had little apparent effect on users who purchase items advertised in spam messages.

¶ 110 Some commentators see greater evidence of norms as anti-spam controls. David Post suggests that technological measures, such as the MAPS RBL, constitute "an informal, decentralized, norm-creation process."[445] In his view, subscribers who implement RBL and "choose to apply the sanction simply turn their backs on offenders, ceasing all (electronic) communication with them."[446] Based on both legitimacy and

441. *See, e.g.*, John R. Levine, *Attention Bonds*, Taughannock Networks Weblog, *at* http://www.taugh.com/weblog/2004/07/28#attentionbond (July 28, 2004, 02:36 EDT).

442. Swidey, *supra* note 204, at 12–14 (noting that the lawyer "incurred the wrath of techies everywhere" but also gained "almost $100,000 in revenue").

443. *See* Gaither, *supra* note 229, at C1.

444. *See* Sorkin, *supra* note 65, at 382–83.

445. David G. Post, *Of Black Holes and Decentralized Law-Making in Cyberspace*, 2 VAND. J. ENT. L. & PRAC. 70, 71–72 (2000). *See supra* ¶¶ 48–49.

446. Post, *supra* note 445, at 72.

autonomy grounds, Post sees such "informal private ordering systems" as preferable to government-mandated systems.[447] However, this approach confuses implementation with creation. MAPS RBL doesn't create norms, it enforces them. The norm defines how users perceive unsolicited e-mail advertising. While MAPS refines this definition by determining which senders should have their messages blocked, it doesn't alter the underlying norm. Implementing MAPS is like installing a car alarm. A car alarm system gives effect to a norm against automobile theft, rather than creating the norm itself. While technology interacts with and shapes the value choices inherent in its design, the relative strengths of this push-pull relationship vary. Here, RBL doesn't lead, it follows.[448]

¶ 111 One interesting effect of a norms-based approach is that it may place market-based solutions at risk. Market approaches accept e-mail as a legitimate advertising medium. In exchange for bearing the increased cost, advertisers gain access to recipients by avoiding e-mail filters and blacklists. Because users dislike e-mail advertising (even though some make purchases based on it), they might oppose a system that legitimizes some amount of spam. If users believe they should not have to accept any advertising messages they have not requested, this norm may trump the pragmatic recognition that some amount of unsolicited advertising through e-mail is inevitable and that market solutions will help by reducing its volume.

F. Summary

¶ 112 The current methods for controlling unsolicited e-mail advertising have not worked. This reflects the complexity of the spam problem, though it mostly represents a failure to approach the issue correctly. In the next section, we consider an alternative, information-based perspective on spam.

IV. AN INFORMATION-BASED MODEL FOR SPAM

A. The Framework

¶ 113 This Paper creates and employs an information-based model for spam policy. The approach is similar to information law, which looks at information in the context of its value, channels, and controls.[449] Unlike cyberlaw, information-based models focus on information, not technology.[450] The nascent information law theoretical framework

447. *Id.* at 72–73.

448. One might argue that blacklists like the RBL have shaped norms about Internet mail configuration—for example, by pushing server administrators to not allow SMTP relaying—but even this contention has two weaknesses. First, objections to relaying substantially predate RBL. Second, RBL's value choices affect only its community of subscribers, not the Internet community generally.

449. Gasser, *supra* note 2, at 9 ("Information Law is defined as the sum total of the legal norms that relate to information (mainly from the standpoint of its processing by modern information technology) and that particularly concern the classification and distribution of the economic, cultural, and constitutional asset information as well as the potential threat posed thereby.").

450. Jacqueline D. Lipton, *A Framework for Information Law and Policy*, 82 OR. L. REV. 695, 699–700 (2004).

holds promise for guiding an evaluation of spam.[451] This information analysis operates at a different level than the New Chicago scheme explicated by Larry Lessig, which examines how regulation should be achieved. Information law looks at whether regulation is desirable, what goals it should set, and how regulators should measure the success or failure of their efforts. By employing an information-based approach to spam, we re-examine the initial assumptions and questions about spam and produce important new insights for understanding and controlling this information channel. Unsolicited e-mail advertising provides valuable information to consumers by introducing them to new products and services, expanding their horizon of consumption choices, and providing information to differentiate among options within a product category. However, these values are offset by spam's costs, including the time and effort needed to sort out useless messages and the disutility of dealing with messages containing offensive content, such as offers for pornographic websites. Thus, an approach that considers spam's value and detriments as information can be helpful in guiding policy.

B. Examples of Information-Based Approaches

¶ 114 Two scholars offer information-based approaches to law and policy, in different contexts, that help create a model for our spam analysis. First, Jacqueline Lipton proposes a normative framework for evaluating regulation based on information. In evaluating laws related to information technology, Lipton focuses on the first word, and argues that cyberlaw concentrates too narrowly on the second.[452] She concentrates on control over information and suggests "utilizing concepts of rights to property, privacy, and access in relation to various classes of information as 'organizing tools'" for her schema.[453] Lipton's goal in creating this framework is a pragmatic one. She wants a model that is "relatively easy to translate into practice by those law and policymakers charged with the task of doing so."[454]

¶ 115 Lipton casts information policy decisions as a balance among property, privacy, and access rights. Property rights confer control over information, generally including the ability to prevent others from using it, in order to facilitate commercial transactions.[455] Privacy rights give an individual control over disclosure of or access to information, in order to facilitate autonomy.[456] Unlike property rights, privacy rights serve personal, not commercial, ends.[457] Access rights grant the ability to gain access to

451. *Id*. at 714–18.

452. *Id*. at 717 (arguing that a "relatively broad definition of 'information' . . . would provide a clearer focal point for a new field of law than currently contemplated in the 'cyberlaw' area . . . because cyberlaw does not in itself connote any focal point for the subject-matter of the relevant legal field, other than perhaps the idea of Internet- or computer-related technologies").

453. *Id*. at 719, 777 (stating that "information law might be organized around a rights-based normative framework that is focused on balancing control rights and access rights in information").

454. *Id*. at 725–26 (describing her goal of "a policy framework that informs the development of relevant law").

455. *Id*. at 728–36.

456. *Id*. at 737.

457. *Id*.

certain data based on social needs that countermand other control rights.[458] For example, the "fair use" copyright exception "can be reconceived as relating to a distinct access right rather than a mere limitation on a copyright (a property right)."[459] She also describes the policy questions inherent in databases containing personal information, such as balancing the incentives to compile data (property rights) with the protection of confidential facts (privacy rights) and error correction (access rights).[460] Lipton's information law perspective recognizes the social value of information and the need to construct a policy framework that balances competing demands upon it.

¶ 116 Second, Jean Nicolas Druey analyzes information problems in the context of "information overload." Druey contradicts the prevailing view that information has an inherently positive value, arguing that information can be detrimental if it is of poor quality, has an immoral purpose, or is redundant.[461] He states that too much information is harmful for three reasons: oversupply of information incurs costs with no corresponding benefit to consumers; information overload reduces a receiver's ability to process information; and overproduction increases the risk that a listener or reader will select the wrong information.[462] Competition for a receiver's scarce information-processing resources creates the risk that important data will be lost or ignored. This can have an effect on outside interests, such as when a citizen concentrates on sports news rather than cogent facts relevant to voting, or when institutions depend on relevant information to function.[463] Most importantly, where regulators employ information to control processes, too much information may be socially harmful. Druey points to concepts such as "equality," which require selective ignorance of certain individual characteristics in order to treat entities alike, citing philosopher John Rawls' "veil of ignorance" as an example.[464] Druey posits a potential "right against information," but notes that legal regulation has not yet adopted this remedy to address the concerns he raises.[465] He asserts that intermediaries, such as the media and interest groups, perform a critical filtering function that regulate and limit the problem of information overload.[466] Thus, Druey focuses on the value of information in particular contexts. He recognizes that more information is not necessarily beneficial, and puts forth a potential regulatory mechanism to mitigate the harms of information overload.

---

458. *Id*. at 743–47 (stating that an access right permits a "person to have access to specific information that is effectively controlled by another person for a particular purpose supported by public policy justifications").

459. *Id*. at 752.

460. *Id*. at 764–71.

461. Jean Nicolas Druey, *Information als Gegenstand des Rechts* 68–71 (1995). I am indebted to Urs Gasser for translating and summarizing Druey's work. The translation of Druey's work can be found in Urs Gasser, *Information overload – a legal perspective (Part I), at* http://blogs.law.harvard.edu/ugasser/2004/10/08 (Oct. 8, 2004).

462. Druey, *Information Overload*, *supra* note 461, at 68–69.

463. *Id*. Druey cites EVERETT M. ROGERS & REKHA AGARWALA-ROGERS, COMMUNICATIONS IN ORGANIZATIONS 90 (1976), regarding the institutional challenges of information overload.

464. Druey, *Information Overload*, *supra* note 461, at 69. Rawls introduces his concept of the veil of ignorance in JOHN RAWLS, A THEORY OF JUSTICE 136 (1971).

465. Druey, *Information Overload*, *supra* note 461, at 135.

466. *Id*. at 137 n.16.

¶ 117 Druey expands on his ideas of information rights and information overload in another article.[467] He notes that law has traditionally balanced opposing interests, but points out that legal regulation of information typically conceives of situations where one party seeks information that a second party does not wish to reveal—for example, trade secret laws.[468] The rise of the "information society," however, creates the need for a negative information right, where one party seeks to avoid receiving information.[469] This need arises because processing information requires investment and incurs costs; receivers may also draw the wrong conclusion from some data (for example, where information has low quality).[470] Druey outlines three possible approaches to information overload: (1) the receiver must adapt through improved selection and processing; (2) intermediaries such as the media and teachers must intervene to pre-screen data; or (3) the sender must reduce her transmission level/volume.[471] Since consumers can assess information's relevance only after consuming it, data overload risks increasing intake of irrelevant information and decreasing processing of relevant information.[472]

¶ 118 Druey cites four examples where law seeks to limit information dissemination. First, in some countries, physicians have a "therapeutic privilege" not to disclose relevant medical data to a patient if there is evidence that doing so would risk serious, imminent harm to the patient's physical or emotional health.[473] Druey views this privilege as an integral part of the trust-based relationship between doctor and patient.[474] Second, anti-trust law in the United States recognizes that providing some information may be harmful. For example, when access to information permits dominant market entities to coordinate their behavior in an anti-competitive fashion, this has a detrimental effect on the market as a whole.[475] Third, consumer protection laws that mandate information disclosure may overload people with data, causing them to fall back on simple, easily digested information such as television advertising.[476] While intermediaries such as testing organizations can mitigate this problem, relying on intermediaries merely shifts the locus of the information overload challenge, reduces the consumer's autonomy in decision-making, and can affect the product market itself.[477] Finally, Druey notes that the law may seek to limit or constrain information based on cultural and educational concerns. He argues that the concept of "free flow of information" cannot function

467. Jean Nicolas Druey, "*Daten-Schmutz*" – *Rechtliche Ansatzpunkte zum Problem der Über-Information, in* FESTSCHREIFT ZUM 65. GEBURTSTAG VON MARIO M. PEDRAZZINI 379–96 (1990). I am grateful to Urs Gasser for translating and summarizing this article. Gasser notes that the term "Daten-Schmutz" is a play on words in German—it sounds like the term for data protection law, "Datenschutz," but actually means "data smut." The translation of Druey's work can be found in Urs Gasser, *Information overload – a legal perspective (Part II), at* http://blogs.law.harvard.edu/ugasser/2004/10/18 (Oct. 18, 2004).

468. Druey, *Daten-Schmutz*, *supra* note 467, at 380.

469. *Id.*

470. *Id.* at 380–81.

471. *Id.* at 382.

472. *Id.* at 383.

473. *Id.* at 384–87.

474. *Id.*

475. *Id.* at 387–90. Druey cites *United States v. Container Corp. of Am.*, 393 U.S. 333 (1969), as an example of how adjustment by market participants to public information can cause anti-competitive effects.

476. Druey, *Daten-Schmutz*, *supra* note 467, at 390–92.

477. *Id.*

effectively as a policy principle because citizens have limited informational processing capabilities and because the market cannot be trusted to provide the best or most correct information.[478] Druey concludes that "one of the tasks of the law [is] to design a system of intermediaries, which guarantees a *relative* maximum of freedom to send, but also receive information."[479]

¶ 119 In examining information overload, Druey states that society should seek an optimal level of information, not a maximum level.[480] When citizens confront too much data, they overemphasize some information relative to other pieces. This sub-optimal outcome implies that free flow of information—the canonical marketplace of ideas—is not the best choice from a regulatory perspective. Thus, Druey believes that legal limitations on information dissemination are not contrary to free speech and the freedom of information, but instead are necessary to achieve it.[481]

C. Analyzing Spam As Information

¶ 120 This paper follows Lipton and Druey in using an information-based model for spam policy.[482] It examines the specific information at issue (unsolicited commercial advertising) in a particular medium (electronic mail transmitted over the Internet). Ultimately, this model weighs the value the information provides against the costs and harms it imposes to determine whether regulatory control is needed, and then suggests how control might best be achieved to preserve this value while mitigating drawbacks from spam.

¶ 121 Thus, the "spam equation" comprises both positive consumer value from relevant advertising information and negative consumer value (harm) from access, processing, and offensive content (among other costs). Most analyses that consider informational factors concentrate on the low average value of spam messages. This perspective fixates on the denominator; the high volume and poor targeting of mass mailings creates low average message value. However, the conclusion of this standard approach—that regulation should prevent spam or only allow opt-in messages—does not follow from its premises. By contrast, this paper evaluates both the equation's numerator and denominator. It first asks: what value do the messages create? While the standard approach sees no value in spam, this is clearly incorrect, because spam works. Spam has demonstrable value for users for two reasons, one theoretical and one quantitative. From a theoretical perspective, advertisers will use unsolicited mass e-mail only if it leads to purchases by, and hence revenue from, recipients. If unsolicited e-mail does not lead to purchases, then sending messages only creates costs (including, perhaps, reputation costs) with no

478. *Id.* at 392–95.

479. *Id.* at 394 (emphasis in original).

480. *Id.* at 395–96.

481. *Id.* Druey emphasizes that "we're in the phase of identifying the problem, but . . . we are far away from having solutions to it." *Id.* at 396.

482. Spam seems to fall into the gap between Lipton's information law and cyberlaw since it involves regulation both of information and of technical architecture. *See* Lipton, *supra* note 450, at 778 (noting that "it is possible that cyberlaw might ultimately focus on the task of providing principles for the regulation of computer networks while information law focuses on specific rights in relation to information").

corresponding benefit. Indeed, even with inexpensive e-mail, few commercial actors will incur the expense without an offsetting gain. Spam's persistence and increased volume suggest its use leads to purchases.[483] If a consumer purchases a product, we assume (absent mistake) she becomes better off as a result.

¶ 122 Quantitative results confirm the theory. Recipients respond to spam. A Pew Internet Project poll found that 7% of surveyed users purchased an item based on receipt of an unsolicited commercial message; one-third of users followed a link from a message to investigate a purchase.[484] Similarly, a survey by the Direct Marketing Association showed that one-fourth of all e-mail recipients who initiated an electronic commerce transaction based on receipt of a commercial e-mail message did so in response to one that was unsolicited, leading to 2003 sales of approximately $1.7 billion.[485] A survey by ISP Yahoo! found that 20% "of U.S. residents acknowledge buying products from spam purveyors," and one-third of respondents responded to spam messages.[486] A survey conducted by the Business Software Alliance (BSA) found that 22% of British consumers surveyed, and 27% of consumers in all surveyed countries, purchased software through spam.[487] The BSA study also reported that a significant fraction of consumers made a purchase or took advantage of an offer or service advertised through spam—from 32% of Canadian respondents to a remarkable 66% of Brazilians.[488] As one Yahoo! survey respondent noted, "One person's spam is another person's bargain."[489]

¶ 123 The value of unsolicited e-mail advertising is not measured simply by the revenue generated from, or the absolute number of, purchases made based on spam messages. Sales or other transactions are only a proxy for the value of information contained in a message. These transactions indicate, but do not quantify, that a particular piece of information was relevant and valuable to the recipient. Sales could misrepresent information value if consumers were deceived—for example, if product quality did not match the advertisement's representations, resulting in value less than the consumer surplus from the transaction—or if consumers did not initiate a purchase from the message, but instead used the information to guide off-line purchases or decision-making.

---

483. *Cf.* LIEBOWITZ, *supra* note 50, at 127–29 (suggesting that the intrusive use of pop-up window advertising by pornographic Web sites may be a viable tactic by site developers to make Web ads as difficult to evade as television commercials).

484. Fallows, *supra* note 4, at 25–26.

485. *See* Press Release, Direct Mktg Ass'n, The DMA Tells House: E-mail Marketing Is Boon To Small Businesses (Oct. 30, 2003), *at* http://www.the-dma.org/cgi/disppressrelease?article=523 (citing a DMA survey finding that "45.8 million Americans had made at least one purchase in the previous 12 months in response to a legitimate e-mail advertisement" and noting "nearly a quarter of these e-mail consumers, or about 11 million adult Americans, had made a purchase in response to a legitimate *unsolicited* commercial e-mail") (emphasis in original). The $1.7 billion figure results from multiplying the total $7.1 billion in sales from e-mail advertising by the 25% sales share for which unsolicited messages accounted.

486. *See* Jon Swartz, *Poll Shows Some Look Forward To Reading Spam*, USA TODAY, July 27, 2004, at 3B (citing a Yahoo! Mail survey conducted in May 2004).

487. *See* Press Release, Business Software Alliance, 1 in 5 British Consumers Buy Software From Spam (Dec. 9, 2004), *at* http://www.bsa.org/uk/press/newsreleases/online-shopping-tips.cfm.

488. *See* Business Software Alliance, *Consumer Attitudes Toward Spam in Six Countries* (Dec. 9, 2004), *at* http://www.bsa.org/usa/events/loader.cfm?url=/commonspot/security/getfile.cfm&pageid=20654.

489. Swartz, *supra* note 486.

Advertising can reveal new opportunities to consumers who do not react immediately with a purchase, but instead evaluate options in this new space to shape their consumption preferences. Thus, reducing the value of information in unsolicited e-mail advertising to a simple aggregate, such as revenues generated through spam, is dangerously reductionist. Purchases driven by spam e-mail signal that some consumers obtain value from this advertising information, but they do not measure that value accurately.

¶ 124 Thus, the numerator in the spam value calculation is not inconsiderable. Recipients benefit tangibly by learning about purchase opportunities, new products and services, and product information through unsolicited e-mail advertising. Policymakers should remain mindful of the numerator—spam's value—in considering appropriate choices for regulation or control over advertising in this medium.

¶ 125 A key aspect of our information-based model is that it evaluates advertising information. Advertising's value is difficult to ascertain ex ante for producers and for consumers.[490] Indeed, on the Web, it may be difficult even to understand the size of the audience that views a given page or piece of information.[491] Statistically, advertisers can predict the response to a given advertising level (particularly for established media) by extrapolating from past data.[492] With mass advertising, however, it is hard to predict individually which recipients will respond.[493] Thus, advertisers may expect that five percent of a television commercial's audience will recall an ad and its product, and that half of those who do will eventually purchase it, but they are unlikely to be able to select the individual audience members who will make this purchase. Mass advertising is an exercise in probabilities; it tolerates relatively poor targeting as a necessary price of success.[494]

¶ 126 Like advertisers, consumers have difficulty establishing a value for information

490. *See* LIEBOWITZ, *supra* note 50, at 131.

491. *See* Adam L. Penenberg, *Web Industry Still Flies Blind*, WIRED NEWS, Oct. 6, 2004, *at* http://www.wired.com/news/culture/0,1284,65240,00.html (noting that "it's difficult, if not impossible, for web publishers to know precisely how many people visit their sites" in discussing widely varying estimates of the number of people who viewed the Wired News site).

492. *See* LIEBOWITZ, *supra* note 50, at 132 (calculating that an advertiser should pay a maximum of "the extra profits that are generated by the additional sales resulting from the advertising" for a given ad). *See also* Lester G. Telser, *Advertising and Competition*, 72 J. POL. ECON. 537, 552 (1964) (noting that the "kind of media audience is also important to the advertiser since this determines his market potential. . . . [T]he choice of entertainment and media attracts an audience of a predictable kind that is most valuable to certain classes of advertisers").

493. *See* Telser, *supra* note 492, at 551 (stating that an "advertiser conveys messages via these media to potential customers while fully recognizing that some of these messages will go unheeded"). *See also* Dina Boghdady, *Advertisers Tune In to New Radio Gauge*, WASH. POST, Oct. 25, 2004, at E1 (describing a new method for tracking which radio stations people listen to in their cars, and noting how one car dealership found that the top two stations recommended by research firm Arbitron as advertising targets were not even in the top ten of stations listened to by people passing his dealership in their cars as identified by the new method).

494. *See* LIEBOWITZ, *supra* note 50, at 131 (stating that "advertisers do not have a very good idea of how effective their advertising is in creating additional sales" in analyzing user response data to television advertising). Liebowitz also notes that "[t]elevision, radio, and newspapers . . . are not well suited to targeted advertising." *Id.* at 133.

before they consume it. This occurs because users must process information to determine its worth—a requirement that inherently limits their ability to make fine-tuned decisions about which information to select and use.[495] Nobel laureate Kenneth Arrow described the "problem of the purchaser's inability to judge in advance the value of the information he buys"[496] in a 1962 article:

> [T]here is a fundamental paradox in the determination of the demand for information; its value for the purchaser is not known until he has the information, but then he has in effect acquired it without cost. . . . [T]he potential buyer will base his decision to purchase information on less than optimal criteria. He may act, for example, on the average value of information in that class as revealed by past experience. If any particular item of information has differing values for different economic agents, this procedure will lead both to a nonoptimal purchase of information at any given price and also to a nonoptimal allocation of the information purchased.[497]

¶ 127 Treating advertising information is challenging for the proposed model and for regulators since its worth becomes apparent only after it is consumed.

¶ 128 Furthermore, advertising serves two different information functions: it alerts consumers to types of products that can meet their needs (including needs they had not previously identified or understood),[498] and it helps them differentiate among those products. (Of course, the second function can be understood as a form of the first one – advertisers may distinguish among products by emphasizing how one particular brand or offering actually serves a different need than its competitors. For example, advertising for a laundry detergent could focus on its ability to leave clothes smelling fresh, while other detergents only clean your wash.) Thus, the advertising function expands consumer demand by identifying a new category of goods or services of value to people, and the differentiation function allocates that demand among alternative goods. Advertising's value differs in context—it may be valuable for a consumer to learn about a new type of product or service, or this category may offer her no benefit; she may seek information that lets her differentiate among competing brands, or the cost of processing this data may outweigh its marginal benefit.[499]

---

495. *See* Druey, *Daten-Schmutz*, *supra* note 467, at 383.

496. Kenneth J. Arrow, *Economic Welfare and the Allocation of Resources for Invention*, *in* THE RATE AND DIRECTION OF INVENTIVE ACTIVITY: ECONOMIC AND SOCIAL FACTORS 609, 616 (Richard R. Nelson, ed., 1962).

497. *Id.* at 615.

498. *See* Telser, *supra* note 492, at 551 (noting that "one of advertising's main functions is to introduce new products"). *See also* Hansell, *How to Unclog the Information Artery*, *supra* note 166 (quoting the vice chairman of a mail order company as saying that "[a]dvertising introduces someone to a new idea," so banning unsolicited ads is not useful because "[p]eople aren't going to say, 'I want something new today, so I want an e-mail from you'").

499. *See* Philip Nelson, *Information and Consumer Behavior*, 78 J. POL. ECON. 311, 313 (1970) (describing consumer search theory for evaluating competing brands and concluding that "[t]o maximize expected utility, a person will search until the marginal expected cost of search becomes greater than its marginal expected return").

¶ 129 E-mail messages containing ads offer recipients varying benefits; a response to a request for details on an advertised computer that provides pricing and technical specifications will generally be more valuable than an unsought promotion for a pornographic Web site. We explore this value disparity by categorizing commercial e-mail messages into three classes in order of likely value to the recipient—information solicited by the recipient, information not solicited by the recipient, and fraudulent information. When a consumer indicates interest in a product or service, information provided in response probably benefits her. She learns more about the item, even if the only additional knowledge is that a given vendor or information source is not helpful and hence not likely a good choice for purchases. Negative information (recognition that something is not of value) confers a benefit. Obviously any additional positive information (for example, data that helps differentiate among competing products) aids the user. Solicited information has a high probability of matching the consumer's preferences and needs; thus, these messages have relatively high average value and should be encouraged from a policy perspective.

¶ 130 Unsolicited information can create value for consumers, but its average value is likely lower than solicited information. This occurs because the likelihood of a match between the recipient's preferences and the information provided is less. Even if the advertiser knows a fair amount about the consumer—for example, the consumer has provided basic demographic information to the advertiser[500]—sending an unsolicited message lacks the advantage of having the consumer's revealed preferences that a request provides. Thus, the error rate for unsolicited messages is probably higher.[501] Unsolicited advertising can create significant value for consumers, but solicited information has better chances of being useful.[502] Whether policy should encourage (or even permit) unsolicited advertising requires considering absolute value created,[503] average value,[504]

500. *See, e.g.*, TreeLoot!, *Official Rules*, *at* http://www.treeloot.com/home.php (click on "your entry" then click "submit" button and click on "player agreement" to see official rules) (last visited Oct. 13, 2004) (requiring winners of an online game to provide personal demographic information to claim prizes); *see also* Virtumundo, *Privacy Policy of Virtumundo, Inc.*, *at* http://privacy.virtumundo.com/pripol.html (last modified Nov. 25, 2002) (listing uses that Virtumundo, which operates TreeLoot!, may make of consumer data, including "us[ing] Individual Information to provide promotional offers to individuals by means of email advertising, telephone marketing, direct mail marketing, online banner advertising, and package stuffers, among other possible uses" and reserving Virtumundo's ability to use this information for "any legally permissible purpose").

501. *Cf.* Telser, *supra* note 492 at 552 (distinguishing between expenditures on advertising and expenditures on personal selling and noting that the "audience of a salesman in a store is self-selected. . . . [T]he proportion of potential customers is high and generally higher than in the audience of an advertising medium").

502. This assumes that unsolicited e-mail advertising does not create greater value for a user when it is correctly targeted than a solicited e-mail advertising message does. If an unsolicited message conferred greater benefit when correctly aimed than a solicited one, average value for unsolicited messages might be higher.

503. *See, e.g.*, Direct Mktg Ass'n, *supra* note 485 (finding value of roughly $1.7 billion for unsolicited e-mail messages).

504. Average value equals the total value conferred divided by the number of unsolicited messages. Note this differs from net average value, which subtracts costs from the total value conferred in the previous equation.

and the distribution of benefits from this type of advertising.[505]

¶ 131 Third, fraudulent messages offer no value to consumers. Even if the information they convey is relevant, it is false, and hence is of no use. Fraudulent spam often tries to transfer value, for example, by tricking recipients into revealing bank account data to spammers. Society generally disapproves of such transfers as theft. Messages are also fraudulent if they offer consumers products that are counterfeit or do not function. For example, a recent study found that up to half of the Viagra pills sold on the Internet could be counterfeit, but noted that the fake pills were packaged identically to the real product.[506] In addition, fraudulent messages may not fit well with our model since they do not seem to have a commercial purpose—there is no real market transaction that takes place, since recipients do not gain anything in the exchange.[507] E-mail policy should unambiguously combat fraudulent messages—particularly those that seek to deceive users into revealing valuable information.[508]

¶ 132 From an information perspective, solicited e-mail advertising is likely to be helpful and should be encouraged, while fraudulent e-mail advertising or information is pernicious and should be eliminated. Unsolicited e-mail advertising occupies an uncertain middle position and will be the subject of most of our analysis. The framework factors explored above—the value of information, the special characteristics of advertising, and its average likelihood of being useful to a given recipient—give us an initial framework to think about information problems. Next, we turn to the particular context of unsolicited advertising through e-mail by examining how spam is defined.

D. What Is Spam?

¶ 133 "Spam"[509] is a colloquial term for e-mail with particular informational content and purpose, though commentators frequently disagree about its precise definition.[510] Definitions of spam vary from narrow to broad.[511] Key elements of many definitions

505. Average value and cost might poorly represent the overall unsolicited advertising picture, depending on the distribution of benefits and costs.

506. *See* Reuters, *Buying Viagra on the Net? Don't expect miracles*, ZDNET, Sept. 28, 2004, *at* http://news.zdnet.com/2100-1009_22-5387377.html.

507. Fraudulent messages might also propose an exchange that is worthless—for example, selling sugar pills as vitamins or other medication. This transaction is deceptive but fits more closely with a market model.

508. *See* Fed. Trade Comm'n, *How Not to Get Hooked by a "Phishing" Scam*, *at* http://www.ftc.gov/bcp/conline/pubs/alerts/phishingalrt.htm (June 2004) (describing "a high-tech scam [known as 'phishing'] that uses spam to deceive consumers into disclosing their credit card numbers, bank account information, Social Security numbers, passwords, and other sensitive information").

509. *See* WIKIPEDIA, *Spam (Monty Python)*, *at* http://en.wikipedia.org/wiki/Spam_(Monty_Python) (last modified Feb. 14, 2005) (noting that the term "spamming" for sending large volumes of e-mail messages containing advertising derives from a Monty Python skit); *see also* SCHWARTZ & GARFINKEL, *supra* note 12, at 11.

510. *See* Sorkin, *supra* note 65, at 327–33 (describing the disagreement over and difficulties in defining spam).

511. *See* Marketingterms.com, *Email Spam*, *at* http://www.marketingterms.com/dictionary/email_spam/ (last visited Feb. 16, 2005) ("The definition of email spam is purposely vague because everybody has his or her own definition. . . . [S]pam is in the eye of the beholder.").

include:

- Consent—some definitions classify as spam all messages that recipients have not explicitly consented to receive (an "opt-in" model)[512], while others limit spam to messages sent after the recipient indicated she did not wish to receive them[513]
- Purpose—some classifications include only messages with a commercial focus,[514] while others are content-neutral[515]
- Volume—most definitions rely on the number of copies of a message that the sender transmits[516]
- Targeting—many approaches look to whether the sender seeks to provide information tailored to the recipient[517]
- Benefit—some versions encompass only messages where the primary benefit is to the sender[518]

¶ 134 Except for the last element, benefit, the advantage of each of these is that they can be evaluated before transmitting the message—it's clear whether a message is spam when it is sent. From an information perspective, though, the most important and challenging criterion is the final one: does the message create benefit for the user? The inevitable difficulty with this measure is that it becomes apparent only once the recipient has received and reviewed the message, complicating classification for potential senders and regulators. This paper simplifies definitional questions by focusing on whether information conveyed to a recipient has value, what costs it imposes, and whether it is desirable to adopt policies that condone or encourage this transmission.

¶ 135 Most legal regulations[519] define spam as unsolicited commercial e-mail, without

512. *See, e.g.*, The Spamhaus Project, *The Definition of Spam*, *at* http://www.spamhaus.org/definition.html (last visited Feb. 16, 2005) (restricting spam to unsolicited messages, meaning that "the Recipient has not granted verifiable permission for the message to be sent").

513. *See, e.g.*, Direct Mktg Ass'n, *Anti-Spam*, *at* http://www.the-dma.org/stopspam/workingstrategy.shtml (May 27, 2003) (stating that "responsible e-mail marketing" provides "[a]n opt-out that works and is easy to find and easy to use").

514. *See, e.g.*, Coalition Against Unsolicited Commercial E-mail (CAUCE), "*How do you define 'Spam?'*" *in* Quick FAQ, *at* http://www.cauce.org/about/faq.shtml#how (last visited Feb. 16, 2005) (stating that CAUCE "believe[s] the largest and most pressing problem is *unsolicited commercial email (UCE)*" but that it also considers non-commercial bulk e-mail a problem) (emphasis in original).

515. *See* Kelkea, *Definition of Spam*, *at* http://www.kelkea.com/support/spam_def.html (last visited Feb. 21, 2005).

516. *See, e.g.*, Spamming Bureau, *Spam Definition*, *at* http://www.spammingbureau.com/spam-definition.php (last visited Feb. 16, 2005) (noting that there "is no predefined 'magic number' that serves as a threshold for spam, but the consensus is 20"); Scott Southwick & J.D. Falk, *The Net Abuse FAQ*, *at* http://www.cybernothing.org/faqs/net-abuse-faq.html#3.1 (last modified 1998) (stating that twenty postings to USENET newsgroups constitutes USENET spam); *see also* Infinite Monkeys & Co., *Spam Defined*, *at* http://www.monkeys.com/spam-defined/ (last visited Feb. 16, 2005) (stating that "Internet spam is one or more unsolicited messages").

517. *See, e.g.*, Infinite Monkeys, *supra* note 516.

518. *See, e.g.*, The Spamhaus Project, *supra* note 512 (stating that a spam message is one where "transmission and reception of the message appears to the recipient to give a disproportionate benefit to the sender").

dealing with other bulk e-mail such as political messages[520] or chain letters.[521] Restricting coverage to e-mail with commercial advertising has three benefits. First, in the United States, constitutional protections for commercial speech are narrower than those protecting other speech, enhancing the probability a reviewing court will uphold spam laws.[522] Second, most spam e-mail is commercial.[523] Third, commercial spam creates a pecuniary incentive to send such messages; other types of bulk e-mail, such as chain letters or political exhortations, generate primarily non-pecuniary benefits to senders.[524] Non-commercial spam may also face implicit penalties for abuse; for example, many politicians and political organizations avoid use of unsolicited e-mail for lobbying and advocacy due to fears of voter backlash.[525] Commercial spam presents the opportunity to generate a profit (or at least cover costs)[526], while non-commercial spam imposes only cost from a financial perspective.[527]

¶ 136 The definition one adopts for the spam "problem" drives and constrains the contours of the solution one proposes. Unfortunately, most approaches to spam neglect the informational issues explored above; hence, their solutions fail to address the relevant

519. *See, e.g.*, CAL. BUS. & PROF'L. CODE § 17529.2(a) (2004) (forbidding any person or entity from "initiat[ing] or advertis[ing] in an unsolicited commercial e-mail advertisement from California or advertis[ing] in an unsolicited commercial e-mail advertisement sent from California").

520. *See* Mark Sweet, *Political E-Mail: Protected Speech or Unwelcome Spam?*, 2003 DUKE L. & TECH. REV. 1, 8–9 (arguing in favor of permitting political spam); *But see* Declan McCullagh, *Political spam as national pastime*, CNET NEWS.COM, May 17, 2004, *at* http://news.com.com/2010-1028-5213287.html?tag=nefd.acpro (describing recent use of unsolicited bulk e-mail by political candidates and noting that since the CAN SPAM Act does not apply to political messages, "the best response to spamming politicians is the old-fashioned one: vote the bums out of office").

521. *See State v. Heckel*, 24 P.3d 404, 406 (Wash. 2001) (defining spam as "unsolicited bulk e-mail" in upholding Washington's statutes regulating commercial e-mail).

522. *See Central Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of N.Y.*, 447 U.S. 557, 563 (1980) (stating that the Constitution "accords a lesser protection to commercial speech than to other constitutionally guaranteed expression").

523. *See, e.g.*, Robyn Greenspan, *The Deadly Duo: Spam and Viruses, August 2004*, *at* http://www.clickz.com/stats/big_picture/applications/article.php/3407371 (Sept. 13, 2004) (finding 79% of all Internet mail to be spam in January 2004 and over 73% of spam falling into the categories of Drugs, Software sales, Mortgage/Refinance, Shopping, Porn, or Organ enlargement).

524. *See, e.g.*, Barbara & David P. Mikkelson, *Craig Shergold*, *at* http://www.snopes.com/inboxer/children/shergold.htm (last modified Dec. 26, 2001) (describing how the persistence of a chain letter seeking business cards to set a Guinness world record for a young cancer patient has led people to send over 200 million cards, even though the patient recovered in 1991 and Guinness has retired the category).

525. *See, e.g.*, Jeffrey H. Birnbaum, *Consultants Deliver Politics to Voters' Inboxes, at a Price*, WASH. POST, Aug. 29, 2004, at A1 (noting that many "leaders in electronic lobbying have decided against putting together a [list of e-mail recipients cross-referenced with additional data such as residential addresses] for fear of sparking voter outrage").

526. *See* Wolcott, *You call it spam, they call it a living*, CHRISTIAN SCIENCE MONITOR, Mar. 22, 2004, at 12, *available at* http://www.csmonitor.com/2004/0322/p12s02-ussc.html (describing a former accountant who started a spamming business and earned almost $200,000 in six months).

527. Non-commercial bulk e-mail, such as political spam, may also face a stronger constraint from recipient disapproval. Users who dislike commercial messages refrain from buying the advertised product and may complain to others about it. However, recipients who dislike political messages (and who reside in the relevant jurisdiction) can make displeasure known more directly by voting against the candidate endorsed in the message. *Cf.* McCullagh, *Political spam as national pastime*, *supra* note 520.

characteristics that challenge recipients of commercial e-mail advertising.

E. Information-Based Shortcomings of Standard Arguments

¶ 137 For most observers, the term "spam" has a uniformly negative connotation.[528] Commentators generally define spam as either "unsolicited bulk e-mail" or "unsolicited commercial e-mail"[529] and object to it based on each word of the definition. First, spam seems to invade a user's privacy as it involves communication neither initiated nor sought by the sender. Second, spam messages are not targeted to a recipient's preferences or needs; they are sent to a mass audience with little or no customization.[530] Third, the message has a commercial purpose and content. American legal thinking traditionally accords such information less normative value than other types of communications such as political messages.[531] Fourth, e-mail is generally considered to be a more private medium than other contexts in which unsolicited information is directed at consumers. The audience for a message is selective since a sender must affirmatively choose to whom the message is targeted.[532] Finally, e-mail reverses the normal economic arrangement for communications in that the recipient bears most of the cost. Senders benefit from economies of scale; one copy of a message can be addressed to multiple recipients[533], but each recipient must deal with an individual copy of the message. Thus, scholars and thinkers point to privacy concerns, mass communication, e-mail's unusual economics, and the distribution of access rights as the source of spam's challenges, and their proposals mirror their diagnoses.

¶ 138 However, none of these objections suffices to condemn spam e-mail. An information-based analysis uncovers weaknesses in the standard arguments. First, *unsolicited* communications may be valuable. Before receiving an advertisement, consumers may not understand either that a need exists or that a product is available. E-mail messages thus can serve the classic informational function of advertising.[534]

---

528. *See* Sorkin, *supra* note 65, at 327 (stating that since for many, "spam means little more than 'unwanted e-mail,' it is perhaps tautological to say that nearly everyone agrees that spam is undesirable"); *see also* Dan Hunter, *Cyberspace as Place and the Tragedy of the Digital Anticommons*, 91 CAL. L. REV. 439, 478 (2003) (calling spam "a pernicious evil to Internet usage").

529. *See* Fallows, *supra* note 4, at 9 (stating that "92% of emailers agree that spam is 'unsolicited commercial email from a sender they do not know or cannot identify'").

530. *See, e.g.*, Sorkin, *supra* note 65, at 330–31 (defining unsolicited bulk e-mail and noting that "a sender may make very minor changes to each copy of a message"); The Spamhaus Project, *supra* note 512 (defining spam as unsolicited bulk e-mail).

531. *See, e.g.*, *Central Hudson Gas & Elec. Corp.*, 447 U.S. at 563; *see also 44 Liquormart, Inc. v. Rhode Island*, 517 U.S. 484, 498–500 (1996) (noting the Court's "early cases recognized that the State may regulate some types of commercial advertising more freely than other forms of protected speech").

532. This selection is weaker when the sender directs a message at an e-mail group or a listserv, since these comprise lists of users each of whom the sender may not be familiar with, but the sender nonetheless possesses a high degree of information about the targets of her information.

533. *See* Postel, *supra* note 8, § 3.1 ex.1 (demonstrating command syntax for a single e-mail message from one sender to three recipients); *see also id.* § 2 ("When the same message is sent to multiple recipients the SMTP encourages the transmission of only one copy of the data for all the recipients at the same destination host").

534. *See, e.g.*, Telser, *supra* note 492, at 324 (noting that "response to an advertisement need not involve purchase of the good advertised. . . . If the consumer likes what he sees in an advertisement . . . he

¶ 139 Second, *commercial* messages may be particularly valuable. Indeed, seven percent of users surveyed in a poll by the Pew Internet & American Life Project reported purchasing a product or service advertised in an unsolicited commercial e-mail.[535] Internet commerce generates substantial revenue[536], and direct marketing through e-mail resulted in an estimated $7.1 billion in sales in 2003.[537] An example illustrates the potential benefits of unsolicited commercial information. The lawyer responsible for the first known spam message (posted to Usenet newsgroups in 1994) recently sent an unsolicited message advertising a book about the need to support educators to 50,000 schoolteachers.[538] The message included a link to his Amazon.com affiliate site.[539] When almost 700 of the teachers purchased the book through the link, he earned nearly $700 in revenue.[540] This message, though perhaps better targeted than most spam, alerted its recipients to a product they likely did not previously know of, but found valuable.

¶ 140 Third, *non-commercial* information sent through e-mail—such as appeals to join a religious group[541] or hate speech[542]—may be equally vexing to consumers. The most common objection to commercial messages seems to be a concern that the profit motive will lead senders to target recipients indiscriminately.[543] However, senders with non-pecuniary motives may also blanket users with bulk e-mail, including political

---

will make sure that he searches that brand; but nearby brands, whether they were advertised or not, will usually be searched too").

535. Fallows, *supra* note 4, at 25–26 (stating that "7% of emailers report that they have ordered a product or service that was offered in an unsolicited email" but noting that "12% of email users say they have responded to an email offer, only to find out later that it was phony or fraudulent").

536. *See, e.g.*, Bob Tedeschi, *More Canadians than Americans use the Internet, but they do far less of their shopping there*, N.Y. TIMES, Jan. 26, 2004, at C5 (estimating U.S. Internet retail commerce at $65 billion in 2003); Bob Tedeschi, *Reporting healthy increase in sales, this holiday shopping season was the best ever for Internet retailers*, N.Y. TIMES, Dec. 29, 2003, at C5 (citing U.S. e-commerce sales of $51.51 billion through Dec. 26, 2003).

537. *See* Direct Mktg Ass'n, *supra* note 485 (finding that "45.8 million Americans had made at least one purchase in the previous 12 months in response to a legitimate e-mail advertisement" and noting that "nearly a quarter of these e-mail consumers, or about 11 million adult Americans, had made a purchase in response to a legitimate *unsolicited* commercial e-mail") (emphasis in original).

538. Swidey, *supra* note 204, at 32.

539. *Id.*

540. *Id.* The lawyer experienced a response rate of roughly .014%; if each address required a separate message (an unlikely possibility), he earned 1.4 cents per message sent.

541. Unsolicited e-mail with religious content has increased in volume recently. *See* Dan Ilett, *Spam gets religion*, CNET NEWS.COM, Nov. 19, 2004, *at* http://news.com.com/Spam+gets+religion/2100-1032_3-5459848.html.

542. *See* Elizabeth Phillips Marsh, *Purveyors of Hate on the Internet: Are We Ready for Hate Spam?*, 17 GA. ST. U. L. REV. 379, 382 (2000) ("The Internet empowers not only the groups that society may wish to foster, namely, churches, synagogues, school groups, political organizations, and public interest groups, but also criminals, hate groups, and groups that seek to impede others in the exercise of their rights."); *cf.* Eugene Volokh, *Cheap Speech and What It Will Do*, 104 YALE L.J. 1805, 1837 (1995) ("Cheap electronic distribution might mean that not only the ACLU or NRA newsletters, but also the KKK and Communist Party newsletters, could be sent to millions of subscribers.").

543. *See, e.g.*, Ray Everett-Church, Chief Privacy Officer & Vice Pres. for Public Policy, AllAdvantage.com, Prepared Statement before H.R. Subcomm. on Telecommc'ns, Trade & Consumer Prot. (Nov. 3, 1999), *available at* http://www.everett.org/testimony/house/.

campaigning[544], religious evangelism[545], or superstition (as with chain letters[546]). MailFrontier, an anti-spam company, "estimates that more than 1.25 billion unsolicited political e-mails will be sent to registered voters" in the U.S. in 2004, and a single tax-cut advocacy group sent 2 million electronic messages to Pennsylvania voters in only 2 weeks.[547] In total, though, the volume of unsolicited, undesired non-commercial messages is lower than that of such commercial messages[548], making this type of e-mail a less pressing problem.[549]

¶ 141 Fourth, spam's unusual distribution of *costs* makes the medium attractive for senders, but this result alone does not mean recipients are harmed. For example, if recipients value a message more than the costs of receiving and sending it, not only are they better off, but society benefits.[550] The appropriate focus for economic evaluation of spam concentrates on *net benefit*, not simply cost. E-mail advertising generates sales revenues of roughly $1.7 billion per year, demonstrating the need to move beyond cost-based analysis in examining spam.[551] Thus, spam costs do not *per se* justify anti-spam measures.

¶ 142 Spam's cost distribution skews costs towards recipients in two ways. First, a sender can transmit one message to many recipients, but each recipient receives an individual copy of the message (expansion on delivery). Second, recipients must examine and process messages to determine which have value and which do not (contextual sorting). Of these two sources of increased cost to recipients, only the second (contextual sorting) supports precautions against spam. If spam were worthless e-mail traffic with a different content and purpose—say, forwarded jokes from acquaintances—its cost burden would occasion less outrage. Spam's information value to recipients determines whether its storage, processing, sorting, and other expenses are pure costs or should be weighed against offsetting benefits. However, it is hard to determine *ex ante*

544. *See* Sorkin, *supra* note 65, at 338 n.54 (noting that 2000 presidential candidate Steve Forbes sent out e-mails to support his campaign that included a one megabyte multimedia file); *see also* Birnbaum, *supra* note 525, at A1 (noting that a consulting company has taken "a nationwide list of registered voters [and] cross-referenced [it] with multiple lists of e-mail addresses collected from magazine subscribers, catalogue shoppers, [and] online poll participants").

545. *See, e.g.*, Brightmail, *Spam Statistics* (March 2004), *at* http://nospam-pl.net/pub/brightmail.com/spamstats_March2004.html (finding 1% of all spam to be "information pertaining to religious or spiritual evangelization and/or services").

546. *See, e.g.*, U.S. Dep't of Energy Computer Incident Advisory Capability (CIAC) Hoax Pages, *Hoaxbusters Home Page*, *at* http://hoaxbusters.ciac.org/ (last modified May 10, 2004).

547. Birnbaum, *supra* note 525.

548. *See* Brightmail, *supra* note 545.

549. *See* McCullagh, *supra* note 520 (quoting Cindy Cohn, legal director for the Electronic Frontier Foundation, as saying she hasn't seen evidence that political spam is a "sufficient-enough problem" and she is "always nervous about attempts to regulate political speech, even with the best of intentions").

550. Recipients bear only their own costs of receiving and processing commercial e-mail messages, so they benefit if the value derived from the message is greater than the messages' costs. From a societal perspective, though, costs include the sender's costs to compose and send the messages, and benefits include value the sender derives.

551. Direct Mktg Ass'n, *supra* note 485. One qualification is that consumers might have purchased these products or services through other channels were e-mail advertising not available or used; if so, the value of e-mail ads is the consumer's value from the online transaction based on the message minus the value she would have obtained from the next-best channel option.

which messages have value and which do not. Even seemingly egregious spam—such as the wave of offers of herbal impotence remedies[552]—provides enough benefit to some recipients that it is worthwhile for advertisers to continue to send the messages. Blocking spam reduces costs but also benefits, including value to recipients not aware they would gain from this information or commercial opportunity. One must recognize this tradeoff, resulting from the uncertainty of information's value before it is processed, in shaping approaches to spam.

¶ 143 Finally, proponents of "opt-in" regulation often cite *informational considerations* in advancing regulatory proposals. They argue advertisers can better target potential customers when communication is limited to recipients who indicate an interest in the product or service. However, this reverses the puzzle of advertising. Consumers may not know they need a product or service until they learn about it.[553] The opt-in argument treats consumers' interests and needs as static, while information and advertising theory acknowledge that this range can be expanded.[554] Advertising assumes information asymmetry; consumers may not know what they don't know. This is a critical policy point, because it removes one option for reform; greater information disclosure. By definition, consumers cannot evaluate *ex ante* the value of advertising experience that offers them data on new opportunities or new product characteristics. Given the option to do so, nearly all consumers would forgo or prevent e-mail advertising because its costs are easily predicted but its benefits are not. "Opt-in" does not work because consumers cannot know what they're missing.

¶ 144 From an information perspective, the standard attacks on spam messages lose most of their force but reveal important aspects of the spam puzzle. We next evaluate the problems of unsolicited e-mail advertising based on informational considerations.

F. What Challenges Does Spam Pose?

¶ 145 Why is spam often harmful?

¶ 146 Posing this question risks ridicule. E-mail users' inboxes clog with pitches for herbal impotence remedies, low-cost home loans, and online dating services. ISPs must devote ever-increasing technical and personnel resources to managing the tidal volume of spam.[555] Spam messages create financial and security breaches.[556] Many users list spam

552. *Cf.* Fed. Trade Comm'n, *The Truth About Impotence Treatment Claims* (Oct. 1998), *at* http://www.ftc.gov/bcp/conline/pubs/alerts/impoalrt.htm.

553. Advertising theory predicts that multiple exposures to new information may be necessary for consumers to consider or purchase a product. *See* Telser, *supra* note 492, at 555 (noting that there "might be a threshold of awareness such that consumers fail to notice a product unless they have received at least a certain number of messages"). Thus, a single e-mail message about a new consumption choice might not be sufficient for consumers to derive the value that choice offers in expanding their horizon of options.

554. *See, e.g.*, JOHN KENNETH GALBRAITH, THE NEW INDUSTRIAL STATE 219 (1978) (stating that in "the absence of the massive and artful persuasion that accompanies the management of demand, increasing abundance might well have reduced the interest of people in acquiring more goods" in explaining that advertising increases demand for goods as well as redistributing it among vendors).

555. *See, e.g.*, Sara Radicati & Masha Khmartseva, *Focus: The IT Cost of Spam*, MESSAGING TECH. REP., Aug. 2003, at 2; *see also* Chris Seper, *Companies hate spam, too*, CLEVELAND PLAIN DEALER, July

as the primary drawback of communication via e-mail.[557] Spam can even impede the efficient functioning of a government.[558] However, these problems are *effects*, not causes. The spam problem is not the commercial nature of the messages or their volume or unsolicited character. Commercial messages pervade the daily environment, from television (both broadcast and cable)[559] to billboards, newspaper ads, radio jingles, and corporate sponsorship of places and events.[560] Consumers accept, ignore, or occasionally heed these blandishments. In a thirty-minute network television broadcast, commercial messages consume eight to ten minutes—and this does not count "product placement." It is no accident that the characters in "24" drive Fords[561], or the judges in "American Idol" drink Coca-Cola on camera.[562] Nearly all of these messages are unsolicited. Perhaps consumers accede to advertising by using media where it is rampant, but no one asks permission before Mike Ditka lectures viewers about impotence.[563] Why, then, do people hate spam for exposing them to advertising without their express consent?

¶ 147 There are three parts to this question's answer. First, users don't actually hate advertising by e-mail since some purchase the highlighted products. The "commercial" part of spam's definition highlights a generally neglected feature of this advertising technique—it works. Advertisers use spam because recipients purchase products after receiving it. If spam did not pay, it would not continue to exist. In addition, dislike of advertising is an accepted American phenomenon. While people complain about it vocally, they respond to it economically.[564] Thus, the rhetoric about spam contradicts

---

14, 2003, at E2 (reporting that faucet company Moen has had to employ an anti-spam service to deal with a spam problem costing the company an estimated $1 million in lost productivity annually); Jonathan Krim, *Spam's Cost to Business Escalates*, WASH. POST, Mar. 13, 2003, at A1 (citing consulting group Ferris Research as estimating spam's costs to US businesses at $10 billion in 2003 and quoting an IDC research manager as calculating that a firm with 14,000 employees would spend $245,000 a year to combat spam).

556. *See* Sorkin, *supra* note 65, at 337–40; *see also* Marguerite Reardon, *Spam seen as security risk*, CNET NEWS.COM, Feb. 11, 2004, *at* http://news.com.com/2100-7355-5157275.html (describing infection of over 2 million computers by the e-mail-based MyDoom worm); Shelley Emling, "*Brand spoofing spam*" *a growing Web threat*, DESERETNEWS.COM, July 14, 2003, *at* http://deseretnews.com/dn/view/0,1249,510039241,00.html (describing spam that purports to be from financial institutions and deceives recipients into revealing confidential information).

557. *See* Fallows, *supra* note 4, at 28–29 (stating that 52% of surveyed users "say spam has made them less trusting of email in general" and 70% "say spam has made being online unpleasant or annoying").

558. *See, e.g.*, John Blau, *Spam clogs German government's e-mail system*, COMPUTERWORLD, May 21, 2004, *available at* http://www.computerworld.com/printthis/2004/0,4814,93338,00.html (describing a "crippling tide of spam" that "clogged the government's e-mail system" during a debate over a proposed anti-spam law).

559. *See* LIEBOWITZ, *supra* note 50 at 124–28.

560. *See generally* Dannielle Cisneros, *Do Not Advertise: The Current Fight Against Unsolicited Advertisements*, 2003 DUKE L. & TECH. REV. 10 (2003).

561. *See* Royal Ford, *More Automakers Seek Star Treatment For Vehicles*, BOSTON GLOBE, Mar. 31, 2004, at J1.

562. *See* Stuart Elliott, *Some Sponsors are Backing off to Fine-Tune the Art of Blending Their Products into Television Shows*, N.Y. TIMES, Jan. 22, 2003, at C5.

563. *See* Christopher Rowland, *Making the Lineup For the Big Game: This Super Bowl To Be First To Air Ads For Impotence Drugs*, BOSTON GLOBE, Jan. 27, 2004, at F1.

564. *See* Cisneros, *supra* note 560, at 4 (stating that despite people's dislike of pop-up ads, there is "a high correlation between clicking on a pop-up ad and making a purchase according to online discount travel manager Orbitz").

peoples' behavior towards it.

¶ 148 Second, most advertising in other media carries an implicit bargain; consumers look at ads in exchange for their sponsors defraying some of the costs of consumption.[565] Presumably, movie tickets are less expensive because Nissan, Pepsi-Cola, and other corporations subject patrons to ads before the previews (commercials in themselves) and the feature film.[566] Broadcast television is defined by this bargain—without it, free TV would likely not exist.[567] Radio is almost entirely advertising. Songs operate both as products and advertisement. Broadcasting drives consumption in other formats (compact disc, MP3, cassette tape, etc.) and lures listeners to pay attention to ads for other goods. Tickets to sporting events are made (to some degree) more affordable when companies pay millions of dollars to name eponymous arenas.[568] Spam, however, does not underwrite most users' Internet or e-mail access; rather, it increases costs. In fact, during the late 1990s, some "dot com" companies traded use of computers [PeoplePC] or Internet access [Juno] for consumption of advertising, but these businesses did not prove popular and have largely disappeared.[569] Thus, Americans may feel cheated by spam because it violates their unwritten understanding with advertisers.[570]

¶ 149 Third, and most relevant for this paper, spam has low average information value for most recipients. A lot of spam is fraudulent and thus by definition has zero (or negative) value for users. Other spam advertises products that are of no interest (or, indeed, offensive) to the vast majority of recipients. Few female e-mail users are directly interested in herbal Viagra pitches, and explicit solicitations to visit pornographic websites actively dissuade many consumers from using e-mail.[571] The architecture of e-mail predisposes the medium to untargeted advertising.[572] Senders face low error costs because transmitting messages to thousands of uninterested recipients requires very little additional financial investment. This low marginal cost makes it less attractive to invest

565. *See* Telser, *supra* note 492, at 540 (noting that advertisers "indirectly supply entertainment by sponsoring television and radio programs"); *cf.* Volokh, *supra* note 542, at 1841 (stating that competition will drive down the cost of advertising-free services, thus providing a counter-argument to the claim that advertising is the only way to provide the bargain of lower costs to the consumer).

566. *See* Stuart Elliott, *Under an audacious campaign, the chatter before the movie starts might just be about a Nissan*, N.Y. TIMES, Nov. 6, 2003, at C6 (describing the Nissan ad campaign in movie theaters).

567. *See* LIEBOWITZ, *supra* note 50, at 128 ("Television viewers are used to these [advertising] intrusions and understand that they are a necessary evil if they are to see the free programming").

568. *See* Charles V. Bagli, *It's First-and-$800 Million*, N.Y. TIMES, Apr. 12, 2004, at D10 (reporting that the New York Jets will try to cover part of their $800 million investment in a new stadium through selling naming rights worth at least $10 million per year and quoting the Jets' President, L. Jay Cross, as stating that in New York the Jets "should be able to exceed the highest numbers to date" for corporate suites, naming rights, and advertising, and that the Jets "don't intend to finance the stadium on the backs of taxpayers or loyal seat fans").

569. *See, e.g.*, LIEBOWITZ, *supra* note 50, at 123 n.5.

570. *Compare Id*. at 129–30 (suggesting that the 26% of surveyed Web surfers who described banner advertising as "great" must have "thought of advertisers as partners helping to make their surfing possible—i.e., providing the funds for the low prices and giveaways that were the characteristics of early Internet commerce").

571. *See* Fallows, *supra* note 4, at 29–31 (describing negative reactions by users, particularly women, to pornographic spam).

572. *See supra* Section II.

in focusing messages on likely purchasers. The low cost of e-mail advertising reduces the need to reach only a target demographic.[573] If a message will reach both interested and uninterested recipients through cheap mass transmission, investing to weed out consumers with little likelihood of a positive response is not economically sensible. This is spam's "denominator problem"—average message value is low because senders have scant incentive to limit e-mail volume for ads.

¶ 150 Despite living in an environment saturated by unsolicited advertising, consumers particularly dislike spam because it fails to support their e-mail use and offers little benefit on average. Next, we will look at the scope of the spam challenge.

G. How Much Spam Is There?

¶ 151 Spam is a sizeable challenge. The research firm Radicati Group estimates spam constitutes 45% of the global e-mail traffic of 57 billion messages per day.[574] The anti-spam software company Brightmail reported that 62% of e-mail was spam in February 2004.[575] A small group of companies based in Canada sent Yahoo! users almost 94 million messages "offering mortgages, insurance and travel services" in the first three months of 2004.[576] The ISP AOL reports that it blocks or deletes 75% of incoming messages as spam.[577] Microsoft reports that in 2003, 83% of the 3 billion daily e-mail messages received by its Hotmail service were spam.[578] Leading Internet research firm IDC stated that in North America alone, spam messages constitute 38% of the 31 billion messages sent each day.[579] While spam estimates vary and the methodologies used to calculate these numbers have been questioned, there is general consensus that spam is a serious problem.[580]

¶ 152 Dealing with spam is expensive. The Radicati Group estimated that spam cost organizations $49 per user mailbox per year in 2003 and extrapolated a world-wide cost

---

573. By contrast, television advertising is expensive, forcing advertisers such as political campaigns to select their audiences more carefully. *See* Volokh, *supra* note 542, at 1842–43 (quoting a political consultant's advice for television advertising that "if you want to talk to women, buy 'Sisters' Saturday night; men, you buy ESPN; seniors, 'Murder She Wrote;' everyone, [the local football team] or '60 Minutes'").

574. Bray, *supra* note 209, at A14.

575. Hansell, *4 Big Internet Providers File Suits To Stop Leading Senders of Spam*, *supra* note 59 at A1.

576. *Id.*

577. Janis Mara, *AOL Reports Drops in Both E-Mail and Spam Volume*, CLICKZ NEWS, Mar. 19, 2004, *at* http://www.clickz.com/news/article.php/3328841.

578. Microsoft Corp., *Caller ID for E-mail: The Next Step to Deterring Spam* (Feb. 12, 2004), *at* http://download.microsoft.com/download/2/e/2/2e2850b8-2747-4394-a5a9-d06b5b9b1a4c/callerid_email.pdf

579. *Spam volume keeps rising*, CNET NEWS.COM, Sept. 1, 2004, *at* http://news.com.com/2100-1032-5339257.html.

580. *See* Carl Bialik, *Reports on Spam Levels Paint Differing Views of the Problem*, WALL ST. J. ONLINE, Sept. 21, 2004, *at* http://online.wsj.com/article_print/0,,SB109509729214016383,00.html (citing the MessageLabs estimate of spam for August 2004 at 84% and the Brightmail estimate of 66% and noting that most spam estimates are from anti-spam vendors, who have an interest in presenting the problem as a serious one).

of $20.5 billion in additional hardware, software, and information technology support personnel to deal with spam.[581] Based on a survey of Fortune 500 companies, Nucleus Research estimated that spam would cost large companies almost $2000 per employee in 2004.[582] Ferris Research estimates U.S. costs alone at $10 billion in 2003.[583] Businesses face lower productivity from employees who must sort and delete spam.[584] According to Ferris, corporations invested $120 million in anti-spam software in 2003.[585] The ISP Earthlink spends one million dollars each year on legal fees in fighting spam.[586] Spam's high volume, large share of e-mail traffic, and costs make it an important legal and policy topic.

¶ 153 Fraudulent spam constitutes a significant share of the overall pool of messages.[587] These messages are an important component of the problem because their information creates no value. Frequently, these messages attempt to convince recipients to reveal valuable information (such as Social Security Numbers, bank account data, or credit card numbers[588]) that the sender can exploit. These messages can transmit viruses or worms that enable additional spam.[589] While fraudulent spam challenges regulation, it is clear that no one (other than its purveyors) contends these messages have value or should be permitted.

¶ 154 Information-based analysis of spam suggests that altering the current information dynamic of e-mail advertising is desirable. Importantly, it points towards key goals, and several regulatory possibilities, to preserve consumer value from these ads while reducing their costs to e-mail users. We will look at four goals for information-based spam reform and three alternative methods to achieve them.

---

581. Radicati & Khmartseva, *supra* note 555, at 2.

582. *See* David McGuire, *Report: Spam Costs Are Rising at Work*, WASHINGTONPOST.COM, June 7, 2004, *at* http://www.washingtonpost.com/wp-dyn/articles/A21657-2004Jun7.html.

583. Hansell, *Totaling Up the Bill for Spam*, *supra* note 414, at C2.

584. *See* Seper, *supra* note 555, at E2; Hansell, *Totaling Up the Bill for Spam*, *supra* note 414, at C2 (quoting the research director at Nucleus Research as stating that "[s]pam is one of those areas where we see a severe impact on productivity" and that "[t]he average worker receives 13.3 spam messages a day, which takes six and a half minutes to process . . . [which] comes to 1.4 percent of their productive time").

585. Hansell, *Totaling Up the Bill for Spam*, *supra* note 414, at C2.

586. Hansell, *How to Unclog the Information Artery*, *supra* note 166, at C1 (quoting Earthlink's CEO, Garry Betty).

587. In the Pew Internet Project poll, 12% of users responded to a spam message, only to learn that it was fraudulent. Fallows, *supra* note 4, at 26.

588. In a survey, 4% of users reported they had responded to an unsolicited commercial e-mail by providing the sender with personal information requested in the message.

589. *See, e.g.*, John Schwartz, *Malicious Computer Worm Detected*, N.Y. TIMES, Mar. 18, 2004, at C7 (noting that "[p]revious bot programs have commandeered large networks of machines and used them to anonymously send spam"); John Leyden, *Dangerous Mimail Variant Knocks Over Anti-Spam Sites*, REGISTER, Nov. 3, 2003, *at* http://www.theregister.co.uk/2003/11/03/dangerous_mimail_variant_knocks_over/ (noting that the worm "Mimail-C normally spreads through email using its own Simple Mail Transfer Protocol (SMTP) client"); Symantec Security Response, *Trojan.Bedrill*, *at* http://securityresponse.symantec.com/avcenter/venc/data/trojan.bedrill.html (last modified Nov. 18, 2003) (describing a Trojan horse program that sends spam from infected computers); Fallows, *supra* note 4, at 12 (estimating that 70% of spam originates from "hijacked" computers).

V. INFORMATION-BASED SPAM POLICY REFORMS

A. Goals

¶ 155 The goal of an information-based policy approach to unsolicited e-mail advertising is to maximize net information value for recipients. From this perspective, policymakers should focus on five goals: eliminating fraud, pushing advertising towards legitimate channels, targeting revenues, sharing information, and using language carefully.

1. Eliminate Fraud

¶ 156 Fraudulent messages create no value for consumers and can cause harm through deceptive practices such as "phishing." Deterring and preventing fraud is difficult in both the on- and off-line contexts, though, and regulators will likely have to settle for minimizing rather than eliminating it. To reduce fraud, policymakers should employ several techniques. First, law enforcement officials must vigorously pursue and prosecute advertisers and senders who employ deceptive techniques. This enforcement mechanism should involve both civil actions by the FTC and criminal prosecution by attorneys general. This method is primarily legal, though technology would be vital to determining liability and establishing proof.

¶ 157 Second, ISPs should implement technological measures such as rejecting messages from known fraud sources through blacklists and blocking SMTP traffic from computers that allow relaying.[590] Technological authentication of senders, such as Caller ID for E-mail or DomainKeys, would aid ISPs in targeting restrictions more accurately. Vendors have begun introducing products to aid ISPs. For example, WholeSecurity's product Web Caller-ID detects phishing websites disguised as legitimate sites by analyzing their content; and it can protect end users who install the tool in their Internet browser and can assist companies and ISPs to update blacklists.[591] An Australian company, Pipe Networks, offers a service that redirects users who attempt to access known phishing sites to Web pages that explain the problem and help educate users.[592] Pipe explicitly seeks to enable information sharing among "banks, ISPs and enforcement agencies" to combat phishing.[593] A tool like Pipe's has two benefits: it prevents users from unknowingly divulging sensitive information based on phishing messages, and it educates users about why they've been blocked from reaching a site and how they can protect themselves from this type of fraud. Financial services groups have launched several similar efforts to

590. ISPs can also offer technological solutions tailored to more specific fraud problems. *See, e.g.*, *EarthLink Aims to Block "Phishing" Scams*, CNET NEWS.COM, Apr. 19, 2004, *at* http://news.com.com/2100-7355_3-5194778.html (describing "EarthLink's ScamBlocker feature, a downloadable browser-based toolbar" that "warns people about accessing known or suspected phisher sites and redirects them to an EarthLink-generated Web page that provides additional information about phishers and similar online scams").

591. *See* Paul Roberts, *New Tool Identifies "Phishy" Web Sites*, INFOWORLD, Aug. 16, 2004, *at* http://www.infoworld.com/article/04/08/16/HNphishywebsites_1.html; *see also* WholeSecurity, *Phishing Protection*, *at* http://www.wholesecurity.com/products/wcid.html (last visited Feb. 16, 2005).

592. *See* Kate Mackenzie, *Pipe's Patrol Blocks Phishers*, AUSTRALIAN, Aug. 10, 2004, *at* http://www.theaustralian.news.com.au/printpage/0,5942,10394549,00.html.

593. *Id.*

coordinate technological and educational measures to combat phishing.[594]

¶ 158 Third, ISPs and government should educate consumers about the need for caution in conducting electronic commerce based on e-mail solicitations.[595] This educational method combines market pressures with the underlying norm "caveat emptor"; while it does not decrease fraudulent messages directly, it reduces their profitability by decreasing the number of consumers likely to fall victim to them.

2. Push Advertising Towards "Legitimate" Channels

¶ 159 ISPs and governments should encourage consumers to purchase only from sources that comply with the standards of relevant certifying organizations such as TRUSTe[596] or the Better Business Bureau.[597] Information theory supporting concepts such as advertising[598] and trademarks[599] posits that providing consumers with reliable source identifiers builds incentives for businesses to create and maintain quality products.[600] Market-based programs that create monetary incentives for good advertising practices (such as bonded sender arrangements) are valuable in this context. ISPs should adopt these programs—and allow messages complying with them to bypass filters—wherever possible.

3. Target Revenues

¶ 160 The key factor in shaping incentives for e-mail advertising is controlling its revenues. By reducing revenues from disfavored practices, regulators can make engaging in them less attractive. User education (as discussed above) can be useful in this regard. Technological measures could also be powerful. For example, AOL has begun blocking access by its members to websites from spammers about whom it has received complaints.[601] ISPs could block access to Web sites known to contain fraudulent

---

594. *See* Steve Marlin, *Banks Join Group to Battle Phishing*, INTERNETWEEK.COM, Oct. 4, 2004, *at* http://www.internetweek.com/showArticle.jhtml?articleID=49400626.

595. *Cf.* Fed. Trade Comm'n, *Shop Online Safely* (Mar. 2004), *at* http://www.ftc.gov/bcp/conline/pubs/online/cybrsmrt.htm; Fed. Trade Comm'n, *What's in Your In-Box?* (Apr. 2002), *at* http://www.ftc.gov/bcp/conline/pubs/alerts/inbxalrt.htm; Microsoft Corp., *Help Safeguard Your Personal Information Online* (Mar. 1, 2004), *at* http://www.microsoft.com/security/incident/spoof.asp.

596. *See* TRUSTe, *TRUSTe for Consumers*, *at* http://www.truste.org/consumers/index.php (last visited Feb. 16, 2005).

597. *See* BBBOnline, *Browse BBBOnline Reliability Participants*, *at* http://www.bbbonline.org/consumer/Relbrowse.asp (last visited Feb. 16, 2005).

598. *See* George J. Stigler, *The Economics of Information*, 69 J. POL. ECON. 213 (1961) (describing how advertising benefits buyers in markets by revealing prices and additional sellers).

599. *See, e.g.*, *Qualitex Co. v. Jacobson Prods.*, 514 U.S. 159, 164 (1995) (stating that trademark "law helps assure a producer that it (and not an imitating competitor) will reap the financial, reputation-related rewards associated with a desirable product"); William M. Landes & Richard A. Posner, *Trademark Law: An Economic Perspective*, 30 J.L. & ECON. 265 (1987).

600. *See, e.g.*, I.P.L. Png & David Reitman, *Why Are Some Products Branded and Others Not?*, 38 J.L. & ECON. 207 (1995) (describing how gasoline service stations use affiliation with national brands to signal quality to consumers for products where cheating on quality is a risk).

601. *See, e.g.*, John Leyden, *AOL attacks spamvertisers*, REGISTER, Mar. 22, 2004, *at* http://www.theregister.co.uk/2004/03/22/aol_attacks_spamvertisers/ (noting that AOL's move is "designed

information or to utilize deceptive commerce practices, preventing them from realizing revenue from the provider's subscribers.

4. Share Information

¶ 161 ISPs and government agencies should actively share data on fraud, deceptive business practices, and so forth. These entities should share information not only horizontally (among themselves), but also vertically (with users). This involves educating users on best practices for Internet purchases, spam, and information disclosure. Further legislation could insulate ISPs from anti-trust challenges to this practice if necessary, and technological measures (similar to blacklists) could automate the process.

5. Use Language Carefully

¶ 162 The term "spam" has become a convenient moniker for a wide spectrum of information delivered through e-mail, from bulk advertising messages by legitimate advertisers to phishing missives that seek to entice recipients into revealing sensitive information. However, this shorthand lumps together e-mail messages with widely divergent information value. In addition, it creates a normative view—all spam is bad and should be prevented—that is difficult to realize and that consumers consistently undercut. Blocking or preventing all spam is likely not possible,[602] and is undesirable from an information law perspective. Instead, policymakers should concentrate on more specific goals, such as reducing fraud and increasing the average value of e-mail advertising to users. As discussed below, one promising approach to spam is to adopt a "most favored nation" policy for unsolicited e-mail advertising. Policymakers, ISPs, and others risk diminishing the legitimacy of this method, though, if they portray all spam as equally bad. Thus, they should be careful about rhetorical shortcuts; talking about eliminating spam is appealing, but unhelpful. Instead, it is preferable to discuss "reducing on-line fraud" or "reducing unwanted ads." These linguistic formulations also dovetail helpfully into similar Internet information in other delivery modes, such as pop-up ads[603] and Web sites[604], which suffer similar problems.

¶ 163 We examine four possible methods of implementing these four goals: a "spam tax"; helping users respond differently to spam to disaggregate its informational functions; offering paying advertisers "most favored nation" status and blocking access to non-

---

to remove the rationale for sending spam messages by making it impossible for AOL members to access spamvertised sites").

602. Richard Thomas, the information commissioner for the United Kingdom, recently admitted that "[w]e are not going to eliminate spam altogether" at an international meeting of government officials focused on creating "a united front . . . to crack down on the problem of unsolicited bulk e-mail." Will Sturgeon, *Britain, U.S. talk up spam fight*, CNET NEWS.COM, Oct. 11, 2004, *at* http://news.com.com/2100-1028_3-5406072.html.

603. *See* Sinrod, *supra* note 5.

604. *See, e.g.*, Securities and Exchange Commission v. Jared Ray Leisek and Byron John Leisek, Litigation Release No. 17,053 (June 26, 2001), *at* http://www.sec.gov/litigation/litreleases/lr17053.htm (describing settlement of an SEC case against defendants who ran a stock-picking Web site that they used to inflate values of stocks they held through posting false information).

paying spammers; and dividing electronic messages between the current e-mail system and a new, secure "safe-mail" system.

B. The Spam Tax

¶ 164 To implement the goals described above, regulators might consider a spam tax. The goal would be to force consumers to be more cost-conscious in evaluating purchases through unsolicited e-mail advertising and to allocate more evenly the benefits and burdens of spam. Spam often creates an externality; it benefits recipients who value the information or who use it to initiate a purchase, but imposes costs on others. The parties who benefit from a transaction initiated or consummated through unsolicited e-mail advertising do not bear the full societal cost of that transaction because senders can cheaply transfer a single message to many recipients, only a few of whom may value the message's information. Neither those few recipients nor the sender must support the cost imposed on recipients for whom the message is worthless. A classic approach to externalities uses a tax to internalize costs.[605] For example, a company that manufactures a good may pollute the environment, but neither the company nor the consumer who buys the good must pay for this harm (unless there is a well-functioning, compulsory mechanism such as environmental regulation and enforcement). Regulators can force transacting parties to bear the full societal costs of the transaction, and thus to factor these costs into their decisions to produce or to purchase, through imposing a tax that reflects the harm to the environment.

¶ 165 Proposals such as e-postage or bonded sender try to achieve a similar effect indirectly by increasing senders' costs. A more direct (but technologically complicated) way to internalize costs would tax recipients who purchase items from spam. Schematically, the process would work in the following manner:

1. An e-mail user receives an unsolicited message advertising a product or service; the message includes a URL link to a site where the item can be purchased.
2. Finding the offer to be of value, the user clicks the URL in the message, launching a Web browser that loads the advertiser's site.
3. The user purchases the advertised product or service.
4. Either the site or the user's ISP charges a "spam tax" to the user.[606]

---

605. *See* Guido Calabresi & A. Douglas Melamed, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, 85 HARV. L. REV. 1089, 1111 (1972) (describing use of a tax to internalize the costs of pollution); *see also* Louis Kaplow & Steven Shavell, *Property Rules Versus Liability Rules: An Economic Analysis*, 109 HARV. L. REV. 713, 751 (1996) (discussing use of taxes to internalize harm from pollution and stating that "if the government employs pollution taxes in the way economists generally recommend—setting the tax equal to expected harm—the total quantity of pollution will be approximately efficient" and "that pollution taxes offer certain advantages over conventional liability"); R.H. Coase, *The Problem of Social Cost*, 3 J.L. & ECON. 1, 41–42 (1960).

606. In theory, users could be required to calculate and submit such a tax on their own. While a number of states have adopted this model through Internet use taxes to recover sales tax lost to online sales, compliance would be a major problem. *Cf.* Marc Santora, *Forthrightness Put to the Test By a New Item on Tax Forms*, N.Y. TIMES, Feb. 5, 2004, at B3 (describing New York's new use tax that seeks to recover part of the estimated $1 billion it lost in sales tax to Internet sales in 2003 through a new line item in the state

¶ 166 The benefits of a "spam tax" are clear. Users would face increased costs for purchases made through spam messages, decreasing their willingness to do so. However, users still learn about new products and opportunities through e-mail—even if they are unwilling to complete the purchase after learning of the increased cost from the tax, they still receive a benefit from the advertising. The increased total price (including the tax) decreases demand, leading to fewer sales by spam advertisers.[607] This makes spam a less attractive advertising method for producers and a less attractive commerce method for consumers. While reducing the volume of spam does reduce some value for consumers, it likely creates an incentive for better targeting in advertising, which should both reduce costs (from diminished message volume) and increase average benefit (from consumers receiving more valuable messages and fewer worthless ones). In addition, the tax shifts some of the cost of e-mail advertising's overbreadth to the consumers who benefit from it.[608] Thus, taxation helps alleviate the distributional problem of value derived from spam advertising.

¶ 167 The challenges of a spam tax are in its implementation. Self-reporting of spam purchases by users is possible, but unlikely.[609] Thus, imposing a tax effectively would require compliance by spam advertisers (an unlikely prospect) or technological detection of purchases and collection of the levy. For example, ISPs might be able to detect when a subscribing user clicks a URL in an e-mail message that launches a website. If the user later concluded a transaction at that site, the ISP could note the purchase and charge the consumer, either at the time of purchase or through a fee included with the monthly bill. One possible method would detect the use of a Web bug in a URL request (particularly when the bug includes the user's e-mail address as part of the HTTP GET request string) as the trigger for imposing the tax.[610] This approach has two benefits. First, it detects a technique used by spam advertisers to track which recipients respond to their messages.[611] Second, it may discourage use of Web bugs, reducing the ability of spammers to discern responsive from non-responsive recipients. However, this potential method is technologically challenging to enact. ISPs would have to deduce what products a user purchased and their total cost, while avoiding imposing a tax when a user browsed the site but did not complete a transaction. Many e-commerce websites use Secure Sockets Layer (SSL) encryption to prevent third parties (such as the taxing ISP)

---

income tax form). If users can evade taxation with some frequency, the tax must be increased to have the desired deterrent effect, increasing the temptation to fail to report the purchase.

607. We assume price elasticity here.

608. This tax approach treats spam like a nuisance. Imagine a homeowner who enjoys listening to music in his backyard at loud volume. His neighbors hate both the volume and genre of his music. Without a tax, he listens to the music at any time (and at any volume) that brings him added net marginal utility (benefit greater than the cost of electricity, the opportunity cost of other uses of his time, etc.). However, imposing a tax on the homeowner equal to the neighbor's disutility leads the homeowner, instrumentally, to incorporate their harm in his decision-making. *Cf.* Coase, *supra* note 605, at 2–8.

609. Santora, *supra* note 606. The disclosure problem may be exacerbated if consumers purchase items through e-mail advertising that are seen as embarrassing or controversial—for example, impotence remedies, pornography, or credit cards for consumers with poor credit.

610. *See* Richard M. Smith, *The Web Bug FAQ* (Nov. 11, 1999), *at* http://www.eff.org/Privacy/Marketing/web_bug.html (describing how Web bugs work and their use in spam messages).

611. *See, e.g.*, Anil Chopra, *Beyond Anti-Spam Tools*, PCQUEST, June 5, 2003, *at* http://www.pcquest.com/content/topstories/spam/103060506.asp.

from eavesdropping on the transaction between the user and the site.[612] Circumventing or working around this encryption would be difficult.[613]

¶ 168 Another difficulty would be ascertaining the correct level of taxation. The generally negative view of spam might push lawmakers to set a tax so high that it effectively dissuades purchases from spam advertisers. This would cut down on spam, but would also forfeit the value consumers derive from this mode of advertising. Alternatively, industry groups supporting e-mail advertising might seek to minimize tax rates to such an extent that they would have no significant effect on advertiser or consumer behavior. Setting the rate of taxation correctly requires quantifying spam's harm to non-transacting parties and determining whether to tax based on the volume of messages from a given advertiser or sender or based on the overall level of messages in a country or through an ISP. Making these determinations involves overcoming the challenges of obtaining accurate data and choosing a methodology for setting rates.

¶ 169 A tax on spam could achieve the information-based goals described above. Though it faces technical and political challenges, using a tax implicitly recognizes that spam messages can have value; this approach pushes users to consider the costs of advertising through e-mail as they decide whether (and how) to purchase products. Of our four options, the spam tax is conceptually the most simple, but practically the most difficult, making it the least attractive regulatory choice of this set.

C. Disaggregation

¶ 170 Disaggregation splits advertising's two primary functions (providing information about new opportunities for products or services and differentiating among competing brands) to preserve informational value for consumers. The goal of disaggregation is to help consumers learn about new types of products while preventing them from being inundated with information about product categories that are not of interest. Thus, this option tries to preserve access for unsolicited messages that alert consumers to new opportunities for consumption but seeks to block those that are repetitive or contain information about products that meet a need that the user does not have. Consumers exposed to advertising for a particular category of products, and who understand the need this type of product meets, may decide the category is not relevant or useful to their tastes—for example, a single consumer without children may not find information about different diapers valuable since it does not correspond with a presently-felt need.[614]

612. *See, e.g.*, Johnny Papa, *Secure Sockets Layer: Protect Your E-Commerce Web Site with SSL and Digital Certificates*, MSDN MAG., Apr. 2001, *available at* http://msdn.microsoft.com/msdnmag/issues/01/04/SSL/.

613. *See, e.g.*, ERIC RESCORLA, SSL AND TLS: DESIGNING AND BUILDING SECURE SYSTEMS 45 (2001) (noting that when "SSLv2 was first designed in 1994, the Web security problem that people were most worried about was how to pass information from the client to the server without disclosing it to attacking third parties [taxing entities]. . . . [T]he first major design goal was to provide *confidentiality* for traffic between client and server" (emphasis in original)).

614. The information might have expected future value—for example, if the consumer expected to become a parent, she might remember the data on diaper brands. However, presumably she can adjust her preferences for receiving advertising when her tastes change. This raises the potential problem of default settings—users may be effectively "locked in" to their indicated preferences since there is a stronger

Thus, it would be optimal if consumers could indicate a lack of interest in a given category of products after learning about the category's characteristics and the need it serves. For example, users might configure a set of preferences with their ISP that reveals categories of information for which they do not wish to receive advertising. Opting out of advertising categories preserves the possibility of learning about new areas, products, or services while reducing the burden of processing information that holds no value for a particular person.

¶ 171 To implement disaggregation, users or ISPs would have to find technical ways to reveal their preferences to advertisers. For example, an ISP could establish a policy that unsolicited e-mail messages which accurately describe their content in the subject line—thus following CAN SPAM's legal mandates[615]—are allowed to bypass the provider's filters for users who indicate an interest in or need for that type of product or service. This system would face three obstacles. First, the ISP would need to set up a way for users to indicate their preferences. Most providers, though, already allow users to configure and specify which messages can reach their accounts through methods such as individualized spam filters.[616] Second, the ISP would need to prevent advertisers from incorrectly describing the contents of a message to bypass filters. This problem could worsen under the disaggregation approach since spammers would know that some messages would be likely to reach users by including certain terms in the subject lines. Authentication and reputation-based systems such as SPF or Sender ID would mitigate these problems, and ISPs could encourage the government to focus regulatory efforts on fraudulent or misleading messages to further deter this type of evasion. Finally, ISPs would need to educate users that some messages can be helpful to them to prevent users from simply opting out of messages in all categories. ISPs might illustrate the potential harm by noting that a total opt-out approach might prevent messages from reputable e-mail advertisers from reaching users. These obstacles are important, but not fatal to the disaggregation option.

¶ 172 An information-based complication with the disaggregation concept is that consumers might have imperfect or incomplete information about a category after receiving initial advertising as other products or brands might have features that would make the category appealing. For example, a homeowner might have no interest in information about mortgages because she fears being locked into a single interest rate in an environment of variable inflation. Advertising about fixed-rate mortgages offers her no value and so she views the category of "mortgage information" as useless. However, if she received advertising that alerted her to a different mortgage product—an adjustable-rate loan—she would find that very useful. Thus, as the second information

---

pressure to opt out of ads (from annoyance at unwanted messages) than to opt in for additional information. *See* Eric Johnson, *Methods may have changed, but have the customers?*, FINANCIAL TIMES, Aug. 22, 2002, at 14 (describing importance of default settings for e-mail marketing); *cf.* Paul M. Schwartz, *Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy-Control, and Fair Information Practices*, 2000 WIS L. REV. 743, 755 (2000) (describing problems with user interfaces and the concomitant "blinking twelve" problem of default settings on VCRs).

615. *See* 15 U.S.C. § 7704(a)(1)–(2).

616. *See, e.g.*, Yahoo! Mail, *What are filters, and how can I set them up?*, *at* http://help.yahoo.com/help/mail/manage/manage-06.html (last visited Oct. 12, 2004).

function of advertising bleeds into the first by refining or subdividing product categories, this "opt out" opportunity becomes less useful from an information perspective. Preserving information value through disaggregation requires taxonomic balancing: creating sufficiently refined categories so that users do not generally miss valuable new opportunities while keeping the list of categories limited so that users are not overwhelmed simply by having to choose from an extensive set (which might lead them simply to select all categories).

¶ 173 Disaggregation depends on technological or legal ability to foreclose receiving certain types of advertising. In theory, advertisers should use disclosure by consumers to refine how they target messages, but spammers are unlikely to do this for two reasons. First, the error cost of including additional recipients for a message is very low. Second, spammers understand advertising's information asymmetry—their recipients claim to hate spam, but some of them respond to it. Thus, end users or ISPs need to block out messages, or government needs to enforce legal penalties sufficient to force advertisers to channel their advertising. As discussed above, the technological approach would employ filtering to screen messages. The legal approach would comprise, effectively, an "opt-in" system for advertising. Unfortunately, this approach is incompatible with CAN SPAM, which implements an "opt-out" system, and thus would require Congress to revise the statute. Both approaches face challenges; legal constraints require revisions to the federal anti-spam statute and effective enforcement, and technical constraints require ways to channel advertising while preventing circumvention by spammers.

¶ 174 Furthermore, an effective disaggregation technique could, ironically, limit the opportunities it seeks to preserve. By definition, consumers do not know about some categories of products and services described by advertising and have no way to know whether they will find them of value. Thus, if an ISP or end user software filter allowed users to select from a checklist of options to block e-mail advertisements, consumers might avail themselves of every "opt-out," forfeiting future opportunities that could prove valuable to them. Truly effective filtering software would likely tempt ISPs to block all messages that resemble spam. Their consumers might complain about overinclusive filters that blocked desired messages, but would probably not object to controls on advertising since, again, they cannot value ex ante information that introduces new opportunities or product categories to them.

¶ 175 Disaggregation works well in theory but, in practice, depends on consumers recognizing that unsolicited advertising has some value (enough to want to receive certain types of this information) and on legal or technological constraints that limit spam to providing this information.

D. "Most Favored Nation" Status For Advertisers

¶ 176 ISPs can preserve advertising's value for consumers while reducing the costs of useless messages by shifting tactics in their role as gatekeepers. They can do this by creating incentives for advertisers to invest financially in reaching consumers, either through programs such as bonded sender or by paying ISPs for access. ISPs in turn would permit these compliant advertisers to bypass spam filters and to send unsolicited

messages to subscribers. Providers would use cost savings from reduced expenditures on fighting spam and payments from advertisers to compensate users for receiving messages from compliant senders. Critically, ISPs would eliminate incentives for advertisers to "defect" from legitimate programs by blocking the websites of non-compliant senders, undercutting their ability to gain revenue from spam. Finally, ISPs should share best practices to increase the efficacy of these steps. Specifically, providers should: give preference to advertisers who pay, block advertisers who free-ride, and share information to improve effectiveness.

1. Give Preference to Advertisers Who Pay

¶ 177 ISPs should permit paying advertisers to bypass their spam filters. These advertisers fall into two categories. First, senders who use models such as bonded sender, e-postage, or payment at risk are more likely to be legitimate and responsible advertisers since they will pay to access potential consumers—an indication of quality.[617] Bonding vendors such as IronPort provide some quality control and auditing,[618] and advertisers willing to invest in such measures have a greater stake in reputation effects. The added cost of these methods pushes advertisers to target messages more carefully. An important qualification here is that these models depend on their underlying technology—ISPs must be able to verify that a message complies with the relevant requirements cheaply and easily, and falsification or duplication of an authorized sender's credentials must be difficult and rare. For example, if faking bonded sender status is easy, spammers will duplicate this information to bypass filters, and if verifying this status is hard, ISPs are less likely to devote computing resources to this method.

¶ 178 Second, ISPs should allow advertisers to pay them in exchange for bypassing spam filters. Providers could charge a flat rate, a per-message rate, or a per-recipient rate. ISPs could protect subscribers' privacy by assuming responsibility for message delivery—the advertiser provides the message, and the ISP ensures it reaches each user's (or a subset of users') mailbox. This split keeps advertisers from learning users' addresses. The benefit of this "pay to play" approach is that it shifts the e-mail cost model towards that of other communications media such as radio and television where advertising revenue underwrites part of the service's cost. It may be difficult to conceive of users acceding to spam in exchange for a lower monthly access charge, but there are three reasons to believe they would do so. First, consumers are accustomed to this bargain in other

617. *See* Telser, *supra* note 492, at 539 (arguing that "advertising may signal a certain level of quality. . . . [C]onsumers may justifiably regard the risk of using the advertised product to be less than the risk of using the non-advertised product").

618. *See, e.g.*, Bonded Sender Program, *Email Standards*, *at* http://members.bondedsender.com/bsp/register/index.do (last visited Feb. 16, 2005) (listing standards that a sender must meet to participate in the program). Microsoft has adopted Ironport's bonded sender program for its MSN and Hotmail services. Stefanie Olsen, *Microsoft taps IronPort in spam fight*, CNET NEWS.COM, May 5, 2004, *at* http://news.com.com/2100-1024_3-5206012.html.

communications media.[619] Second, the discount could be a significant fraction of the monthly charge, particularly for dial-up users. ISPs who reduce spam loads through this approach gain both a cost advantage (from diminished hardware, software, and personnel expenditures on fighting spam) and a revenue advantage (from advertisers' payments). Hence, users might see a price reduction not only from the two dollars per month they pay to cover spam costs,[620] but also from the advertising revenue ISPs gain. 51 million users accessed the Internet over dial-up connections in 2003, at prices typically ranging from $10 to $21.95 per month.[621] At this level, even the savings of two dollars from reduced spam loads would cut a dial-up user's costs by ten to twenty percent. Third, consumers routinely trade inconvenience or information disclosure—such as enduring ads during television shows or before movies, or providing personal data in exchange for free e-mail accounts, discounts,[622] or a chance to win prizes[623]—for products and services.

¶ 179 An important feature of this approach is that users should not be able to opt out of receiving all spam. Instead, users should be able to reject particular categories or advertisers, but should not be able to ban e-mail advertising completely.[624] Providing advertisers with an alternative to undirected mass dispatches of unsolicited e-mail is at the root of the "Most Favored Nation" (MFN) approach. If advertisers cannot effectively reach consumers through models like bonded sender or ISP payments, they will revert to the current model of spam. As e-mail without advertising is an unlikely and undesirable possibility, the goal of the MFN approach is to channel advertising to maximize social and individual value.

2. Block Advertisers Who Free-ride

¶ 180 In contrast to the MFN provision giving compliant advertisers access, ISPs should block e-mail from non-compliant advertisers with blacklists and should block subscribers from accessing websites of non-paying advertisers that send unsolicited messages.[625] ISPs should identify these sites by analyzing spam messages sent to their users (or blocked before delivery) and obtaining complaints from subscribers. If successful, this

619. *See* Cisneros, *supra* note 560, at 10 (noting that even the plaintiff suing a movie theater for running commercials after the listed start time of films "does not take issue with the advertisements and previews that run prior to the announced start time of the feature film").

620. *See* USA TODAY, *supra* note 61.

621. Matt Richtel, *In a Fast-Moving World, Some Prefer the Dial-Up Lane*, N.Y. TIMES, Apr. 19, 2004, at A5 (quoting a study by research firm The Yankee Group).

622. *See* Saul Hansell, *Internet Is Losing Ground in Battle Against Spam*, N.Y. TIMES, Apr. 22, 2003, at A3 (noting that clothing store Gap offered consumers a 10% discount in exchange for providing their e-mail addresses).

623. *See, e.g.*, TreeLoot!, *supra* note 500.

624. ISPs would need to control "defections" by users who agree to accept legitimate e-mail advertising but then set up filtering software to intercept these messages. Presumably, few users would do so if the advertising burden were not onerous. ISPs could also contractually prohibit users from filtering advertising messages and could test customer compliance by using either dummy messages or "read receipts" on e-mail with ads.

625. ISPs should only block sites of non-paying advertisers that use spam. Otherwise, ISPs might use Web site blocking as an anti-competitive strategy to channel users only to sites of advertisers who are marketing partners of the ISP.

tactic prevents spammers from realizing revenue through their e-mail advertising. E-mail advertisers who complain should be directed to the payment-based programs described above.

¶ 181 ISPs show increasing interest in adopting site-blocking. AOL cuts off access to sites that advertise via spam on a limited basis.[626] ISPs in the United Kingdom adopted a similar measure by creating a new "best practices" guideline, permitting them to shut down websites promoting themselves through spam or selling spam tools such as software or e-mail address lists.[627] These ISPs coordinated their approach through the London Internet Exchange (LINX), an Internet exchange point that handles ninety percent of UK Internet traffic through peering arrangements.[628] This coordination improves the effectiveness of blocking by increasing its scope and threatening non-compliant ISPs with the loss of peering arrangements.[629]

¶ 182 Site blocking has a number of advantages. First, it cuts off revenue to advertisers who fail to comply with "best practices" that encourage responsible marketing. In effect, site blocking makes spam financially unrewarding. This financial disincentive motivates spammers to stop sending messages, to pay for access to ISP users, or to try to evade detection by shifting websites or by refining their e-mail content. This final concern, threatening an "arms race" between spammers and ISPs, is lessened by users' ability to complain about a site marketed through spam. Even if such an advertiser successfully reaches a consumer, that consumer can take action to make future e-mail efforts unrewarding. In addition, site blocking concentrates on the components of e-mail advertising with the greatest cost: order acceptance and payment processing. ISPs can force advertisers to pay to set up new Web locations by blocking their URLs.

¶ 183 Second, site blocking can maintain much of the information value of unsolicited advertising. Currently, ISPs that block spammers' websites, such as AOL, simply return an error page to users who try to access the site.[630] Instead, ISPs could return a website (perhaps with a disclaimer or notification of the redirection) from a compliant advertiser in the same product category. For example, if a user tries to launch a URL from a spam message about home mortgage loans, the ISP could redirect the user's browser to the Web page for a compliant mortgage lender. Thus, a user who wants to learn more about a type of product or service can do so, but from a "Most Favored Nation" advertiser instead. Consumers gain most of the information benefit from unsolicited ads (though they lose access to the specific product described) without supporting advertisers who use disfavored techniques. This redirection prevents the spammer from generating sales while enhancing benefits to advertisers who comply with the ISP's "best practices,"

626. *See* Leyden, *supra* note 601.

627. *See* John Leyden, *ISPs Gang Up on Spammer-Run Websites*, REGISTER, Aug. 18, 2004, *at* http://www.theregister.co.uk/2004/08/18/isp_war_on_spam/; *see also* Press Release, LINX, New War on Spam (Aug. 18, 2004), *at* https://www.linx.net/www_public/press_events/press_releases/pr103.

628. LINX, *supra* note 627.

629. *Id*.

630. *See* Jonathan Krim, *AOL Blocks Spammers' Web Sites*, WASH. POST, Mar. 20, 2004, at A1 ("AOL members attempting to visit a blocked Web page receive an error message that says a connection to the page could not be made, but are not told that it is a spammer's site that has been placed off limits").

reinforcing the value of "Most Favored Nation" status. In addition, redirection increases the value of MFN status to compliant advertisers, leading to a concomitant greater incentive for advertiser participation.

¶ 184 Redirection does raise concerns. First, ISPs would have to determine what type of product to which a spam message URL corresponds before loading an alternative site. This requirement creates computer processing overhead in looking up the blocked URL, finding its category, and loading an alternative site. However, if this overhead proves too costly, ISPs could simply return an error page. Second, this is private regulation of content by ISPs, which may raise concerns about control over information by these intermediaries.[631] Third, if ISPs offer users alternative sites, there could be antitrust concerns. For example, if Hotmail or AOL partners with certain vendors and redirects users to its sites, this redirection might lead to claims based on tying or monopolization under the Sherman Act.

¶ 185 A third benefit of site blocking is its evasion of the "freemail" problem by targeting the site advertised in a spam message, not the source that sent it. ISPs need not worry about blocking messages originating from Hotmail or Yahoo! Mail since the MFN strategy cuts off spam indirectly by preventing it from earning revenue. This approach eliminates problematic blacklists that target spam sources, such as domains, IP addresses, and free e-mail services. Users can still receive messages from free e-mail providers, but they cannot access URLs in spam messages from these providers.

¶ 186 If users complain about inability to access a site, the ISP has three options. The ISP may permit users to reach the site, continue to block the site, or contact the site and offer to allow access in exchange for payment. ISPs should establish procedures to allow users to complain about blocking and to seek access to sites. Also, providers should not block sites that do not pay but abstain from using spam to advertise. Competition for users among ISPs should prevent anti-competitive site blocking in most cases. In areas where only a single broadband provider is available, regulators might need to consider using antitrust laws to combat monopolistic behavior by the ISP.

3. Share Information to Improve Effectiveness

¶ 187 ISPs could improve the comprehensiveness of their spam site blocking by sharing information about blocked sites through a common database or daily list swaps. This approach has two benefits. First, it reduces each ISP's research costs by leveraging other providers' efforts. Second, it provides a check on blacklist entries. For example, if multiple ISPs block a site, the likelihood that this site does not comply with ISPs'

631. *See Id.* (quoting Cindy Cohn, legal director of the Electronic Frontier Foundation, as concerned that this approach is "paternalistic" and worried that companies could block a competitor's site by spamming an ISP's members with messages that include its URL); *cf.* Cisco Systems, *Beyond Tunneling: Cisco Managed Broadband Access Architecture for Cable Operators*, *at* http://www.cisco.com/en/US/products/hw/cable/ps2209/products_white_paper09186a008017913e.shtml (last visited Feb. 16, 2005) (describing how cable broadband operators can use different Quality of Service levels for different content providers, how certain "ISPs promote their ability to prevent customers from obtaining content that is not family appropriate," and how the Cisco solution "ensure[s] that all traffic from the user travels directly to that ISP and cannot travel directly to the Internet").

standards would be high. However, sharing information requires ISPs to coordinate standards and potentially exposes the ISPs to antitrust claims. To exchange information effectively, providers must use similar criteria to block sites. If Hotmail permits senders under a "payment at risk" program, but AOL blacklists all advertisers except those who pay a fee, then sharing lists would not be useful because AOL blocks sites that Hotmail would permit. In this case, information exchange could lead Hotmail to overly inclusive blocking under its own standards. ISPs could mitigate this problem by coordinating standards through industry bodies such as the U.S. Internet Service Provider Association (USISPA).[632] Blocked sites might also bring Sherman Act monopolization claims against ISPs, arguing that blocking violates the law by restraining trade. If this becomes a realistic threat, ISPs should lobby for, and Congress should pass, a narrow antitrust exception permitting this behavior, as blocked sites can regain access through third-party mechanisms such as bonded sender programs.

¶ 188 The "Most Favored Nation" approach concentrates on the role of the ISP as intermediary between advertisers and e-mail users. ISPs are excellent enforcers of regulations, both technical and legal, against spam. They are primarily large organizations with technological expertise and the financial resources to employ legal experts. Providers have a financial and reputational stake in controlling the flow of e-mail advertising to their users. They have a coordinating body, the USISPA, to advocate their interests before state and federal regulators and to coordinate enforcement efforts with other jurisdictions.[633] While both the CAN-SPAM Act and Internet experts endorse an expanded role for individual users through programs such as "bounty hunter" rewards for reporting spammers, these provisions seem unnecessary.[634] ISPs have the incentive, resources, and expertise to enforce spam regulations effectively.

E. Safe-mail

¶ 189 The open, trust-based system of e-mail creates opportunities for low-cost advertising, fraud, and cost-shifting through spam. However, it also allows reliable, cheap, and anonymous communication through simple universal standards. Safe-mail preserves the benefits of electronic mail while offering more secure messaging by creating a parallel system designed for secure and trustworthy communication. Conceptually, safe-mail operates alongside e-mail, similar to the way e-mail among users on a local network, such as within an office building's local area network (LAN) once operated separately over different protocols from Internet e-mail. Safe-mail offers security features that e-mail does not, but also diminishes some of the benefits of e-mail. It eliminates insecure features of e-mail without requiring difficult and expensive changes to the SMTP protocol.

---

632. *See* U.S. Internet Serv. Provider Ass'n (USISPA), *Mission*, *at* http://www.usispa.org/mission.html (last visited Feb. 16, 2005) (stating that the "U.S. Internet Provider Association will serve both as the ISP community's representative during policy debates and as a forum in which members can share information and develop best practices for handling specific legal matters").

633. *Id.*

634. *See* 15 U.S.C. § 7710(1) (requiring the FTC to report within nine months of the Act's enactment on adopting a system to reward people who report violators); Asaravala, *supra* note 302 (quoting Stanford Law School professor Lawrence Lessig in his critique of the CAN-SPAM Act).

¶ 190 Creating a second electronic messaging system instead of altering or replacing e-mail may seem redundant. However, this approach has four key benefits. First, maintaining parallel systems lets users choose the right medium for communication. If users need anonymous, widespread messaging to users with whom they have not previously interacted, e-mail is the correct choice. If users need a system that offers secure communication with other users known to the sender, safe-mail is the better option. Second, creating a second system guides users to associate different norms and expectations with each medium. As consumers increasingly rely upon and establish trust with safe-mail, they will shift to that system for communication requiring security and integrity. Accordingly, their expectations regarding e-mail will drop, since they will prefer the protections of safe-mail. Thus, consumers will regard e-mail with a greater skepticism that more closely aligns their expectations to the system's architecture. Third, consumers already routinely use multiple e-mail systems and clients.[635] Many users who interact with e-mail at work also maintain a separate e-mail account with an ISP for personal communication, particularly if the user's employer monitors or accesses messages sent over its network.[636] A common tactic to reduce spam volume is to employ a separate account, such as a free e-mail account from Hotmail or Yahoo! Mail, for purposes such as e-commerce transactions and newsgroup postings.[637] Thus, users are accustomed to maintaining multiple e-mail accounts, using different software, such as Lotus Notes at work and AOL at home, and expecting different levels of privacy and security for each account.[638] Adding a safe-mail option would not constitute a significant additional burden. Fourth, creating safe-mail as a separate messaging protocol eliminates the challenges of backwards compatibility arising from any change to SMTP, thereby permitting users to move gradually to safe-mail at a time of their choosing.

¶ 191 Safe-mail would operate under a different protocol than e-mail's SMTP. The system would conform to new IETF standards for cryptographic authentication of senders and servers.[639] The safe-mail system would supply content-level security by providing encryption to prevent unauthorized access and offering methods to detect tampering or alteration of a message. The safe-mail system would also grant revocable trust for senders, servers, domains, and executable code within messages. As the name implies, safe-mail seeks to be secure, even though attaining this security requires compromises in scalability and usability. By default, safe-mail is an "opt-in" system. Users must actively

635. *See* Benjamin M. Gross, *Multiple Email Addresses: A Socio-technical Investigation* 2–7 (July 2004), *at* http://www.ceas.cc/papers-2004/183.pdf.

636. *Id.* at 4; *see Courts Say It's OK: Peep Away*, CIO MAG., June 1, 2002, *at* http://www.cio.com/archive/060102/expert.html (noting that a "court is highly unlikely to conclude that an employee has a reasonable expectation of privacy in his e-mail communications when the employer has a policy clearly stating that such communications are subject to monitoring").

637. *See* Fed. Trade Comm'n, *You've Got Spam: How to "Can" Unwanted Email* 2 (April 2002), *at* http://www.ftc.gov/bcp/conline/pubs/online/inbox.htm (advising users to think about using "two email addresses - one for personal messages and one for newsgroups and chat rooms" and to "consider using a disposable email address service that creates a separate email address that forwards to your permanent account").

638. Gross, *supra* note 635, at 3–5.

639. *See* Stefanie Olsen, *Net Visionary Urges E-mail ID Standard*, CNET NEWS.COM, June 17, 2004, *at* http://news.com.com/2100-1024_3-5238202.html (describing Vint Cerf, the co-inventor of TCP/IP, advocating "digital signatures as a means to encrypt and verify senders").

choose senders or domains from which to accept mail. The safe-mail protocols would permit, but might discourage, extended trust, as the user would decide whether to accept messages from everyone whom another trusted user deemed trustworthy.

¶ 192 Conceptually, safe-mail works like an unlisted phone number. A safe-mail user only accepts messages from senders whom she has selected as trustworthy. Thus, she forfeits the possibility that any unsolicited communications, such as messages from telemarketers, could provide her any value. However, she would still receive these types of communications from e-mail. Reputable advertisers would be willing to invest in a safe-mail account to contact her. The safe-mail system operates in the following manner:

1. A consumer obtains a safe-mail account, perhaps from a service provider, a bank, or her local government. The account provides access to that entity's safe-mail network, client software to access the network to send and retrieve mail, a set of cryptographic keys to encrypt, sign, and decrypt messages, and instructions or training in the secure operation of safe-mail. The user sets up the software and the safe-mail account.
2. When the user wants to send a safe-mail message, she starts the software, composes the message, signs and encrypts it with a cryptographic key managed by the software, and sends the message.
3. The safe-mail server for her network receives the destination address for her message and her cryptographic signature, *but not the contents of the message*.
4. The server contacts the destination safe-mail server. The two computers verify each other's identity through the safe-mail authentication protocol.
5. The sending server transfers the recipient's address and the sender's signature to the receiving server.
6. The receiving server looks up the recipient and ascertains whether that potential receiving user accepts messages from that sender.
7. The receiving server returns one of three codes to the sending server, instructing the sending server that it could not find the recipient, that the recipient accepts messages from the sender, or that the recipient does not accept messages from the sender.
8. If the recipient accepts messages from the sender, the sender's safe-mail server allows the sender to transfer the message contents. In turn, the sending server transfers the contents of the message to the recipient's server for delivery. If the recipient does not accept messages from that sender, then the sender's server returns a message to the sender stating that the recipient will not accept her messages.[640]

¶ 193 This safe-mail architecture faces several challenges. First, the safe-mail system deviates from the "store and forward" system of e-mail, where the sender transfers the

640. Safe-mail providers could further deter spammers by imposing penalties, such as temporary or permanent suspensions of service, for senders who incur too many failed message transfers. This would impede users who rely on dictionary attacks or other automated means that guess at a recipient's address.

entire message in one transaction to an ISP or destination server. Instead, the safe-mail system uses a "verify then send" system, where messages are not transferred until the safe-mail server determines that the recipient accepts mail from that sender.[641] Second, safe-mail requires that the client software store or synchronize a user's preferences, the list of permitted senders, to the safe-mail server. This storage or synchronization requires additional bandwidth and storage space on the server. This consideration is offset by reduced message volume from the "verify then send" architecture, since the server rarely stores messages that it cannot deliver or transfer.[642] Third, safe-mail must provide a means for senders to ask potential recipients to accept their messages. Safe-mail would accomplish this through an "invitation" message that indicates the sender's cryptographic identity, and then permits the recipient to add that user to her list of accepted senders. Fourth, the system has an inherent lag time while the safe-mail servers determine whether the recipient accepts messages from the sender. This delay disadvantages the sender, forcing her either to remain online to await message transfer or to delay transfer until the next time she connects to the network. However, this queuing effect increases the inherent "cost" of sending a message, making it more difficult to accomplish mass transfers of messages and thereby reducing the possibility of spamming on the safe-mail system. Fifth, safe-mail is less portable than e-mail. Users need access to their cryptographic keys and to the software interface to send or receive messages. However, the ubiquity of portable digital devices, including PDAs and Internet-enabled cell phones, should reduce this concern. Finally, the safe-mail architecture rests on technological means of establishing trust between users.

¶ 194 Safe-mail contemplates two possible models for security and trust: a hierarchical, "top-down" model and a peer-governed, "web of trust" model. In the hierarchical model, entities, such as businesses or governments, set up certifying authorities to provide the cryptographic "locks and keys" for safe-mail security. When a user wants to join safe-mail, she applies to that authority for an account and its associated keys. Presumably, the authority would investigate the user, perhaps through a credit check or a required deposit of funds as a bond against system misuse, before issuing these credentials. Violation of either the terms of use for the system or associated legal regulations for safe-mail would cause the certifying authority to revoke the user's credentials and shut off her access to the system. The advantage of a hierarchical system is that it makes verifying a user's credentials and her safe-mail "identity" easier, as the certifying authority vouches for them. If the certifying authority were sufficiently well established, as a major bank or a state government would be, users would trust the authority's reputation in determining that a user who claims to be John Smith is, in fact, John Smith, because the

641. A recent article proposes a similar change in how e-mail messages are transferred to the recipient's server. *See* Todd Marshall, *Spam: Leave It to the Sender*, ZDNET, Oct. 8, 2004, *at* http://news.zdnet.com/2100-1009_22-5402746.html (predicting that this change would reduce Internet traffic and increase costs to spammers).

642. In theory, the server should never store messages, since it only accepts and transfers messages with known recipients who agree to receive these messages. However, technical failures (such as malfunctions of the recipient's safe-mail server or the network) might prevent immediate transfer, forcing the sending server to store messages.

Commonwealth of Massachusetts verifies this fact.[643] In addition, relationships among certifying authorities could reduce misuse and fraud. If each authority verified a person's credentials before allowing her to establish an account, then the authorities could establish "black lists" of people whose safe-mail accounts were revoked. Such lists would also provide the reason for safe-mail account revocation, distinguishing non-payment of monthly fees from attempts to defraud other users.

¶ 195 In the "web of trust" model, individual safe-mail users vouch for each other's identities. For example, I trust that a sender is John Smith because my friend Jane Doe states that this is, in fact, his identity.[644] This method requires that the safe-mail protocols support a way to establish initial trust between users. For example, people could exchange cryptographic keys either through a centralized directory or by "out of band" means, such as trading floppy disks with public keys. The benefit of the "web of trust" architecture is its limitation on the power of outside entities, such as states or ISPs, to dictate terms of trust or to intervene in relationships between users.[645] Individual consumers decide who to trust and why. The challenge of the "web of trust" is that it can be more unwieldy than the hierarchical model, particularly as the number of users and the relationships among them grow and become more complex. Also, the "web of trust" can be vulnerable to breaches by distant users in the Web. For example, if I trust everyone that John Smith trusts, and John trusts everyone whom Jane trusts, a breach or violation by a friend of Jane, whom I may not even know, has immediate consequences for me.

¶ 196 Safe-mail faces at least three potential problems from an information perspective. First, it risks lowering unsolicited e-mail traffic from unknown senders to second-class status. Users may pay little attention to e-mail communication, particularly e-mail messages from unknown senders, when they have the security and verification of safe-mail available to them. This argument presents greater concerns in areas such as political e-mail, as it may be harder for marginalized speakers or speakers with fewer resources to enter the safe-mail system and persuade people to accept their messages. Three responses to this objection are possible. First, the prospect of invitation messages in safe-mail, offering the receiver the chance to engage in communication, gives speakers at least one opportunity to gain listeners. Second, spam messages already effectively constitute second-class speech. These messages are often filtered, labeled, and ignored by users and

643. Like all cryptographic systems, the hierarchical model faces the challenge of establishing the identity of certifiers as an initial matter. For example, the system must ensure that only Bank of America establishes a key with that identity. There are two possibilities for surmounting this obstacle. First, ISPs could delegate the creation of "root-level" keys to certain institutions, such as national governments. Under this approach, counterfeiting a key would be duplicative of the government's authority, and would lead to penalties similar to punishments for currency counterfeiting. Second, users could rely on their safe-mail provider to establish trust between root-level certifiers. This is a variant of the "web of trust" model. For instance, I might accept Bank of America's statement that a user is John Smith because my provider vouches for Bank of America.

644. *See* Johnson, Crawford, & Palfrey, *supra* note 174, at 30–32.

645. *Cf.* A. Michael Froomkin, *The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709, 798–810 (1995) (describing sources of resistance to a proposal by the United States government to adopt an encryption standard that would permit users to communicate securely, but would incorporate a "back door" for U.S. agencies of law enforcement and intelligence to decrypt and monitor these communications).

by software. In this regard, safe-mail is likely no worse than the current situation. The new protocol would worsen matters only if users' expectations and interaction with e-mail dropped further. Third, users may well distinguish among types of unsolicited messages. Objections to spam that derive from the content of messages, rather than their volume, fade when moving from commercial messages to political ones.[646] Political missives seem less likely to include pornographic images or content. Their messages may be intellectually offensive, but are not as susceptible to being personally offensive. Concerns about second-class status for some forms of commercial advertising seem less sharp in a media environment with plentiful opportunities to reach consumers, although, some of these methods may have greater expense and less broad audiences than mass e-mail postings. Thus, while safe-mail does create two tracks of communication and related expectations, it is unclear whether this system worsens the situation of speakers remaining in the e-mail track.

¶ 197 Second, safe-mail relies on the existence of both an open, cheap, and anonymous source of communication (e-mail) and a secure, authenticated, and white-listed source of information (safe-mail). If users move entirely to safe-mail and give up or neglect e-mail messages, they will lose the value of unsolicited information that may benefit them. While this risk is real, the constraints and technological complexity inherent in safe-mail's architecture make it more likely that consumers will use safe-mail for high-value, confidential communications. However, consumers will likely maintain e-mail access for fast, informal, and less sensitive messages. Evidence for the stability of this dual system exists in the way consumers often use multiple e-mail clients for different purposes, such as communication with co-workers, personal messages, newsgroup postings, and e-commerce purchases. Users accede to multiple electronic messaging environments, with different expectations and communication patterns in each environment. Safe-mail is unlikely to disturb that system.

¶ 198 Third, safe-mail allows users to choose with whom they communicate in that medium. This user discretion may risk creating an information monoculture, where a user hears only from known speakers and consumes information only supporting those positions with which she already agrees. Cass Sunstein highlights this risk in his book *Republic.com*, where he refers to MIT MediaLab founder Nicholas Negroponte's idea of the "Daily Me," a completely personalized information diet that excludes new or contrary data.[647] Safe-mail is, indeed, a medium where speakers must obtain the recipient's consent to engage in communications. As noted above, though, this risk is cabined by two factors. First, we predict that e-mail will continue to thrive alongside safe-mail. There will still be channels for unexpected, new, or surprising information to reach safe-mail users. Second, safe-mail does allow new speakers the opportunity to engage in a dialogue with users by first requesting that they accept an initial message. As with other information environments, a speaker must quickly establish relevance and interest to maintain a recipient's attention and interest. While safe-mail does allow recipients to

646. *See* Fallows, *supra* note 4, at 6 (noting that 80% of users are "bothered by deceptive or dishonest content," and 76% are "bothered by offensive or obscene content").

647. CASS SUNSTEIN, REPUBLIC.COM 3–7 (2001). The first chapter of Sunstein's REPUBLIC.COM, "The Daily Me," is available at http://pup.princeton.edu/chapters/s7014.pdf.

choose with whom they communicate, the existence of an unbounded alternative venue (e-mail) and the opportunity, however limited, for senders to communicate at least once with users limit the risk that safe-mail will lead consumers to create bounded, comfortable, and homogeneous consumption patterns for information.

¶ 199 Safe-mail combines technology and norms to address spam's information problem. It divides messages into two zones. In one zone, users can place a high degree of trust in the sender's identity and in the content as reflecting the sender's creation. However, communication in this space is limited to users whom the recipient knows and trusts enough to include in an exchange of messages.[648] This zone, for example, would offer an excellent environment for electronic commerce, including consumer purchases and other transactions such as account updates and electronic payments. In the other zone, users have a low level of trust in either identity or content. However, unsolicited exchanges and anonymous communications are possible in this zone. Both zones have their virtues and their demerits. The benefit of this hybrid system is that consumers understand the rules that apply in each medium. Safe-mail is less convenient to use and more limited in its reach and communication. However, decreased convenience is a byproduct of increased security. Users accept this tradeoff in other venues, such as the security checks necessary to travel by airplane in most countries, as long as there are more convenient, less secure alternatives available. Furthermore, safe-mail respects users' autonomy by allowing them to choose with whom to communicate, and respects senders' autonomy by permitting unsolicited communication in the e-mail space. Safe-mail preserves the opportunity to discover relevant unsolicited information by operating alongside e-mail. In addition, this hybrid system increases the probability that users will discover legitimate, valuable information by providing advertisers with a way to communicate securely, reliably, and consensually with consumers. Limits on communication can thus increase the average informational value of advertising over safe-mail.[649]

F. Summary

¶ 200 An information-based approach to spam policy suggests that regulators must focus on controlling the e-mail advertising that users receive by attacking fraud, encouraging methods that create incentives for quality, going after spammers' revenues, and sharing information on successes and setbacks. To achieve these goals, regulators should consider taxing purchases made through unsolicited e-mail ads, working to help consumers disaggregate spam's informational functions, granting legitimate advertisers "Most Favored Nation" status while blocking access to the websites of their less legitimate competitors, and creating a new, parallel system of secure messaging. The third and fourth of these alternatives seem most promising. "Most Favored Nation" statutes exhibit great potential because they focus on the Internet service provider community, comprised of actors with expertise, resources, and incentives. Safe-mail

---

648. Efforts to protect children who communicate through Internet chat have employed similar approaches. AOL and Verisign announced they would deploy chat rooms for children that require cryptographic "tokens" to validate a child's age before allowing access. *See* Paul Roberts, *AOL Shows Safe Chat Rooms*, PC WORLD, Oct. 26, 2004, *at* http://www.pcworld.com/news/article/0,aid,118342,00.asp.

649. Gasser, *supra* note 461.

shows promise because it alters norms regarding electronic messages, while also providing a secure system in which users can authenticate senders and trust content.

VI. CONCLUSION

¶ 201 Spam exists because the technical architecture of Internet e-mail makes unsolicited advertising through this medium cheap and nigh uncontrollable. Spam continues to exist because a surprising number of recipients of these ads respond by purchasing the featured product. Current attempts to regulate spam focus on the former point, but ignore the latter, thereby undermining the effectiveness of spam regulation. An information-based approach to spam recognizes that unsolicited e-mail advertising creates value for some consumers by helping to shape their consumption preferences and providing a means to satisfy them. Preserving and increasing this value is important, not only because regulatory policy should encourage the production of information useful to consumers, but also because revenues from spam purchases drive the commerce engine fueling many users' e-mail accounts. A better approach to spam channels this potent economic force, helping consumers learn about new opportunities while reducing profits and incentives for fraudulent and other low-value ads.

¶ 202 Moreover, commercial advertising is only one type of valuable unsolicited information that consumers receive through e-mail. Policymakers should hesitate before creating and imposing systems that block an entire category of content from reaching users. Even if the purposes of such systems prove benign, such capabilities can be deployed to more sinister ends, such as monitoring or preventing disfavored political speech. Terry Fisher suggests that spam may be a necessary byproduct of an open, anonymous, and easily used communications medium such as electronic mail.[650] Fisher notes that freedoms of speech and assembly create not only political pamphleteering and civil rights demonstrations, but also panhandlers in Harvard Square.[651] In short, we may have difficulty arriving at a solution for spam that does not impose more informational costs than it saves. Only by explicitly considering and evaluating policy with an information-based perspective can we choose a course that maximizes the benefits offered by e-mail.

¶ 203 For information-based spam policy to succeed, regulators must accept two uncomfortable facts. Eliminating unsolicited e-mail advertising is unlikely to occur, and such elimination would be undesirable. Instead, policymakers should focus on using consumers' responsiveness to spam to alter the information dynamic in which spam occurs. By recognizing the importance of both the value and the costs of this type of advertising, we can begin to change how we interact with it.

650. Spam was one of the cross-border issues discussed in Terry Fisher's comments during the course discussion of *Cross-Border Issues in Cyberlaw*, led by John G. Palfrey, Jr. (executive director of the Berkman Center for Internet & Society) at the Internet Law Colloquium, Harvard Law School (Sept. 29, 2004).

651. *Id.*