UIC John Marshall Journal of Information Technology & Privacy Law

Volume 22
Issue 1 *Journal of Computer & Information Law - Fall 2003*

Article 2

Fall 2003

Where's the Beef? Dissecting Spam's Purported Harms, 22 J. Marshall J. Computer & Info. L. 13 (2003)

Eric Goldman

WHERE'S THE BEEF? DISSECTING SPAM'S PURPORTED HARMS

ERIC GOLDMAN†

I. INTRODUCTION

After many failed attempts over the past six years, Congress finally enacted a law regulating unsolicited commercial e-mails, the *Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003* (the "*CAN-SPAM Act*" or "*CAN-SPAM*").[1] *CAN-SPAM* follows significant state-based efforts to regulate spam; from 1997 to 2003, nearly three quarters of the states adopted some spam regulation,[2] most of which are now preempted by *CAN-SPAM*.[3]

CAN-SPAM, like the state laws preceding it, takes a multi-faceted approach to regulating spam. Among other provisions, *CAN-SPAM* contains provisions that regulate the e-mail content,[4] restrict specific notorious spammer practices,[5] give spam recipients the ability to opt-out, and attack the spammer's funding by creating advertiser liability.

The diversity of regulatory approaches inherent in *CAN-SPAM* (and, before that, the superseded state statutes) prompts a fundamental question: exactly what harms are caused by spam that these regulations attempt to redress? There is no consensus answer to this question. Just about everyone seems to agree that spam is a problem that needs to be

---

† Assistant Professor, Marquette University Law School. E-mail: eric.goldmanmarquette.edu. Personal home page: <http://eric_goldman.tripod.com>. The author thanks the participants in the Summer 2003 Spam Seminar at The John Marshall Law School for their enlightening perspectives.

1. Sen. 877, 108th Cong. (2003) [hereinafter *CAN-SPAM Act*].

2. *See* David E. Sorkin, *Spamlaws.com, Spam Laws: United States: State Laws* <http://www.spamlaws.com/state/index.html> (accessed Oct. 30, 2003).

3. *CAN-SPAM* preempts all laws expressly regulating the use of e-mail to send commercial messages (except laws that "relate to acts of fraud or computer crime"). *CAN-SPAM Act*, *supra* n. 1, at § 8(b)(2)(B).

4. *See e.g.* restrictions on misleading subject lines; requirements that the spam contain contact information and be labeled as an ad or as sexually oriented material.

5. *See e.g.* restrictions on e-mail harvesting, dictionary attacks, using open mail relays, and signing up for free e-mail accounts.

addressed,[6] but no one seems to agree on why. Without clearly understanding the targeted harms, policy-makers cannot craft regulations designed to fix them.

This Essay examines the purported harms caused by spam in an effort to isolate bona fide areas needing legislative intervention. However, few such needs exist. Instead, most purported harms are illusory, already adequately addressed by existing laws or best left to market solutions. This analysis thus undercuts many of the purported justifications for regulating spam.

II. DEFINING THE HARMS OF SPAM

A. DEFINING SPAM

Any attempt to intelligently discuss spam is immediately hampered by the word's imprecision. Simply put, the term "spam" lacks a single well-accepted definition.[7] Usually "spam" refers to some form of unwanted e-mail, although some users generalize the term to describe all forms of unwanted advertising, both in e-mail and other media.[8] *CAN-SPAM* 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."[9] Building on this definition, this Essay refers to "spam" as unsolicited "commercial electronic mail messages." However, this definition is both under- and over-inclusive because the definition includes e-mails recipients want and does not include all e-mails not wanted by recipients, and thus it may not track recipient expectations.[10]

---

6. *See* Humphrey Taylor, *HarrisInteractive, Majority in Favor of Making Mass-Spamming Illegal Rises to 79% of Those Online*, <http://www.harrisinteractive.com/harris_poll/index.asp?PID=387> (accessed July 16, 2003) (seventy-nine percent favor making mass-spamming illegal).

7. *See* Michelle Delio, *Wired News, Spam: Much Hated, Little Defined* <http://www.wired.com/news/print/0,1294,58682,00.html> (May 1, 2003) (discussing the diversity of definitions for spam articulated at the Federal Trade Commission's Spam Forum in Spring 2003); Mailshell, Inc., *Results of the SpamCatcher Attitude Survey* <http://www.mailshell.com/mail/client/oem2.html/step/pr/article/17> (Apr. 30, 2003) [hereinafter *Mailshell Survey*] (press release of Mailshell, Inc.) (providing some statistical analysis of consumer definitions of spam and concluding "[t]here is no clear definition of spam").

8. *See* Evan Hansen & Stefanie Olsen, *CNET News.com, Spam: It's More Than Bulk E-mail* <http://news.com.com/ 2102-1023_3-961134.html?tag=st_util_print> (Oct. 8, 2002).

9. *CAN-SPAM Act*, *supra* n. 1, at § 3(2). The law further requires the Federal Trade Commission to promulgate regulations defining "primary purpose." *Id.* § 3(2)(C).

10. *See* Deborah Fellows, *Pew Internet & American Life Project, Spam: How it is Hurting E-mail and Degrading Life on the Internet* ii <http://www.pewinternet.org/pdfs/PIP_Spam_Report.pdf> (Oct. 22, 2003) [hereinafter *The Pew Report*] ("e-mail users are not entirely clear on just what is spam, an issue that is an absolute stopper for writing effective, enforceable legislation against spam").

B. SPAM IS ANNOYING

1. *Distinguishing Wanted and Unwanted Content*

Many e-mail recipients castigate spam as annoying,[11] but the reasons why are less clear. Some annoyance is attributable to the objectionable content in spam,[12] a point addressed *infra* in subsection II(D). Otherwise, the annoyance is based (among other factors) on the unsolicited, high-volume, time-consuming or unpreventable nature of spam.[13]

I believe these concerns all derive from the same source: spam is *unwanted*. A simple example may illustrate this. Assume Jane is ready to purchase a Canon PowerShot S400 digital camera. An unsolicited e-mail arrives in Jane's in-box from a trustworthy retailer that she has never transacted with. The retailer offers to sell her the camera for $100 less than any other retailer. Is this spam?

Some recipients would say "yes" because the e-mail is unsolicited or otherwise invades their privacy. However, most e-mail recipients would consider this e-mail valuable instead of annoying, in which case they would want this e-mail because it will save them time and money.

Perhaps this example gives us an important insight on the nature of spam. E-mail recipients want e-mail that saves money, saves time, educates on matters of interest, or is otherwise relevant and helpful.[14] Thus, many e-mail recipients gladly would receive unsolicited e-mails that meet those specifications. In contrast, e-mail recipients are annoyed to receive a high volume of irrelevant and unhelpful e-mails.[15]

Unfortunately, frequently spam is irrelevant and unhelpful to recipients because it is relatively untargeted. Like any other marketers, spam advertisers will pay for targeted e-mail lists that are more likely to yield higher results. However, the negligible marginal cost of sending spam lowers the optimal level of targeting for spammers. Thus, spammers can profitably use low-yield and untargeted practices such as e-mail harvest-

---

11. *Id.* at 27; Taylor, *supra* n. 6 (ninety-three percent of those surveyed said spam was somewhat or very annoying).

12. *See The Pew Report*, *supra* n. 10, at 27.

13. *See Id.*

14. *See* DoubleClick, *2003 Consumer E-mail Study, Oct. 2003* 3 <http://www.doubleclick.com/us/knowledge_central/documents/research/dc_consumere-mailstudy_0310.pdf> (Oct. 2003). The survey considered permission-based e-mail marketing. Respondents were asked what motivated them to act on an e-mail; thirty-eight percent said it was the "product I needed at the time" and thirty-five percent said a "special offer or discount." *Id.*

15. The Federal Trade Commission has specifically focused on the high percentage of false claims in spam, Federal Trade Commission, *False Claims in Spam* <http://www.ftc.gov/reports/spam/030429spamreport.pdf> (Apr. 30, 2003). These concerns are effectively subsumed under the category of irrelevant and unhelpful e-mails. Other harms created by false claims are covered under other existing laws like false advertising.

ing and dictionary attacks.[16]

Even though spammers can profitably send very-low relevance e-mails to lots of recipients, not all spam is bad. Inevitably, some recipients will find a particular spam e-mail helpful and relevant. More specifically, recipients' perceptions about each spam's relevance usually sort into a bell curve: some will find the e-mail completely irrelevant, some will find the e-mail very relevant, and others will find the e-mail somewhat relevant.[17]

Some empirical data supports this analysis. Several recent surveys show that seven to eight percent of those surveyed have purchased a product or service in response to spam[18] and approximately thirty percent of those surveyed have responded to spam to get more information about the advertised product or service.[19] While not high percentages, the statistics seemingly contradict spam's abysmal reputation. For recipients who responded to spam (plus those who were educated but did not respond), the spam was relevant. For those who purchased in response to a particular spam, that e-mail helped the consumer find a desired product or service at an acceptable price.

We should not trivialize these consequences. Spam plays an important role in the marketplace of ideas, perhaps filling gaps left by other media, and can contribute to efficiently functioning economic markets. In some cases, spam creates transaction opportunities that otherwise would not occur due to prohibitive search costs or lack of consumer awareness about products available to solve their needs.

Of course, these conclusions do not change the fact that most spam is unwanted by most recipients. However, it is unclear why individuals seem less tolerant of irrelevant spam than irrelevant ads in other media. Consumers routinely tolerate irrelevant ads in other media with less annoyance than they feel towards spam.

Let us consider ad relevancy in a few media, starting with billboards. Billboard ads target viewers only by geography (if that), so they

16. *See* Jack Hitt, *Confessions of a Spam King*, N.Y. Times Mag., (Sept. 28, 2003) at 48 (describing different methods of acquiring e-mail addresses cheaply); *see generally* Ian Ayres & Matthew Funk, *Marketing Privacy: A Solution for the Blight of Telemarketing (and Spam and Junk Mail)*, 20 Yale J. on Reg. 77 (2003) (discussing the analogous phenomenon in the telemarketing context).

17. Recipient assessments of relevancy also vary based on when the e-mail is received. An e-mail to Jane offering a cheap price on the digital camera may be very relevant prior to her purchase and irrelevant afterwards.

18. *See The Pew Report*, *supra* n. 10, at ii-iii (seven percent); *Mailshell Survey*, *supra* n. 7 (eight percent); Thomas Leavitt, posting to Politech <http://www.politechbot.com/p-04710.html> (May 2, 2003) (citing a survey on npdor.com that seven percent "sometimes" buy from spam, plus another twenty-three percent "very rarely" buy).

19. *See The Pew Report*, *supra* n. 10, at ii-iii (thirty-three percent); *Mailshell Survey*, *supra* n. 7 (twenty-eight percent).

are fairly low-relevancy advertising tools, meaning that most billboard ads will be irrelevant to most viewers.

The broadcast and newspaper media use differentiated content to segment consumers.[20] Thus, a TV show will appeal to a certain demographic, and newspapers divide their content into topical sections (e.g. sports, business, metro) that are read by only some readers. This segmentation means that ads can be targeted to consumers attracted by the surrounding content. Nevertheless, even the most targeted content will appeal to multiple demographics, so the associated ads will be less relevant to non-majority audience segments.

In these other media like billboards, broadcasting and newspapers, consumers do not vociferously demand regulation to minimize the irrelevancy of ads delivered through them. Why do consumers feel differently about spam?

2. *Sorting Spam Wastes Time*

Perhaps recipients penalize spam because it takes time to sort irrelevant spam from wanted e-mails. Sorting also creates the risk of Type I and Type II errors (i.e., legitimate e-mail gets tossed or blocked as spam, and objectionable spam gets through the sorting).[21]

But once again, spam is not different from other media. Every medium that contains ads requires consumers to sort ads from content and wanted ads from unwanted ads. For example, sorting postal mail requires the recipient to evaluate the envelope's exterior and, in some cases, open and review the contents. Broadcast ads are even more difficult to sort, because ads are interspersed with content and the viewer cannot reorder or skip the ads.

So while spam does require sorting time, recipients can manually sort e-mail relatively efficiently by reviewing subject lines,[22] and many

---

20. Not all ads are delivered on a segmented basis. For example, infomercials are often broadcast at a time when other programming would fail to generate a sufficient audience, so frequently infomercials make no effort to segment the audience.

21. *See CAN-SPAM Act*, *supra* n. 1, at § 2(a)(4) (legislative finding of Congress).

22. *The Pew Report*, *supra* n. 10, at 11 ("[a]lmost 90% of users say they identify spam by looking at the subject line and/or the sender"). *CAN-SPAM* provides further legal protection against misleading subject lines. *CAN-SPAM Act*, *supra* n. 1, at § 5(a)(2). Seventeen states also had laws regulating misleading subject lines. *See* Arizona [Ariz. Rev. Stat. § 44-1372.01(A)(2) (2003)], Illinois [815 Ill. Comp. Stat. 511/10(a) (2003)], Indiana [Ind. Code § 24-5-22-7(3) (2003)], Kansas [Kan. Stat. Ann. § 50-6,107(c)(1)(B) (2002)], Maryland [Md. Com. Law § 14-3002(b)(2)(iii) (2002)], Minnesota [Minn. Stat. § 325F.694(2)(2) (2002)], Missouri [Mo. Rev. Stat. § 407.1144(1) (2003)], Nevada [Nev. Rev. Stat. 205.492(1)(a) (2003)], North Dakota [N.D. Cent. Code § 51-27-02(1)(b) (2003)], Oklahoma [Okla. Stat. tit. 15, § 776.6(A)(2) (2003)], Oregon [Or. Rev. Stat. § 646.607(3)(1)(b) (2003)], Pennsylvania [Pa. Cons. Stat. tit. 73 § 2250.3(a)(3) (West 2002)], South Dakota [S.D. Codified Laws § 37-24-37(2) (Michie 2002)], Texas [Tex. Bus. & Com. Code Ann. § 46.002(2)

recipients develop good skills doing so.[23] Spam can also be automatically blocked without any manual sorting using e-mail filters. As a result, the amount of time "wasted" on the e-mail sorting process may very well be less than the time wasted in other media.

All media containing ads demand sorting time and create some risk of erroneous sorting, and no regulatory scheme—other than banning a medium altogether—can eliminate that. Instead, time lost to sorting is unavoidable in a media-based society, and spam is just one of many manifestations of that phenomenon.[24] Thus, the explanation for recipients' antipathy towards spam must lie elsewhere.

3. *Spam Causes Recipients to Lose Control of Their In-Boxes*

Evidence suggests that many recipients are bothered by their inability to stop spam[25] and feel that spam is a loss of privacy. This suggests that recipient frustration with spam may be the result of a feeling that recipients have lost control over their in-boxes.

However, once again this problem arises with other media. Recipients cannot stop spam except by eliminating their e-mail account altogether, but consumers of other media are similarly powerless to change what ads are delivered in that medium except by discontinuing use of that medium. For example, a newspaper or magazine reader cannot control what ads are published; the reader's only choices are to ignore unwanted ads or stop reading the publication altogether. This argument holds true for broadcast media, billboards, and junk mail as well.

Perhaps e-mail can be distinguished from other media because it delivers more important personal content to recipients than other media. Recipients seem to develop a special and personal relationship with their in-box, and this explanation might offer an insight about why telemarketing is so reviled.[26] But this explanation is not totally satisfac-

---

(Vernon 2003)], Washington [Wash. Rev. Code § 19.190.020(1)(b) (1999)], West Virginia [W. Va. Code Ann. § 46A-6G-2(2) (Michie 1999)], Wyoming [Wyo. Stat. Ann. § 40-12-402(a)(ii) (Michie 2003)]. Presumably these state laws are not preempted by *CAN-SPAM*. *See CAN-SPAM Act*, *supra* n. 1, at § 8(b).

23. *The Pew Report*, *supra* n. 10, at 11 ("nearly two-thirds (63%) of all e-mailers say about spam that they 'know it right away when they see it'"); *see* George Johnson, Sp@*m ShEn@nig@nS!!; That Gibberish in Your In-Box May Be Good News*, N.Y. Times (New York, NY) (Jan. 25, 2004), at § 4, p. 16 (discussing how spam filters cause spam to "degenerate[e] into nonsense" and become "word salad").

24. *See* Eric Goldman, *S.J. Mercury News, Spam is Just a Byproduct of Our Media-Saturated World* 6B <http://www.bayarea.com/mld/mercurynews/news/opinion/6209142.htm?template=contentModules/printstory.jsp> (July 1, 2003).

25. *The Pew Report*, *supra* n. 10, at 27 (seventy-five percent of users are bothered by this).

26. *See* Ayres & Funk, *supra* n. 16 (discussing a heightened sense of privacy at home).

tory because it does not explain the seeming dichotomy between the outrage over spam and comparative tolerance of junk mail.

A more satisfying explanation can be found by considering the relative adoption curves of spam and other media. We have had many years to develop ways to cope with ads in other media, but we are still developing ways to cope with e-mail ads. It seems likely that users will improve their ability to manage e-mail with more experience, at which point user frustration should decrease.[27] Meanwhile, new generations who grow up using e-mail should be more tolerant of spam[28] because they will develop coping strategies for spam (and media inputs generally) from an early age.

Thus, current annoyance with spam could merely reflect that user experience with e-mail is evolving. Robust e-mail management tools also should reduce annoyance, and the current annoyance may also reflect that those tools are not yet adequately deployed.[29]

4. *Conclusion on Annoyance*

Unwanted e-mails are annoying, but minor annoyances are a fact of life, and no law can eliminate them—from e-mail or otherwise. E-mail recipients' annoyance at spam appears to be an overreaction when compared to their reactions to other forms of annoying ads. Meanwhile, regulation of spam creates significant risk that some relevant e-mails will be blocked from recipients who want them. It is troubling to regulate content to protect the majority from minor annoyances if the conse-

---

27. Taylor, *supra* n. 6 (noting that the percentage of people very annoyed with spam dropped from eighty percent in 2002 to sixty-four percent in May 2003, suggesting that recipients are developing more efficient coping mechanisms); DoubleClick *2003 Consumer E-mail Study* 7 <http://www.doubleclick.com/us/knowledge_central/documents/research/dc_consumere-mailstudy_0310.pdf> (Oct. 2003) (describing increased user sophistication in deleting suspected spam without reading it); *but see The Pew Report*, *supra* n. 10, at 36 (indicating that veteran Internet users are more sophisticated at managing spam but are also more bothered than average by it).

28. *The Pew Report*, *supra* n. 10, at 33.

29. *See generally* Stefanie Olsen, *CNET News.com, Yahoo, Sendmail to Test Antispam System* <http://news.com.com/2102-1032_3-5164279.html?tag=st.util.print> (Feb. 24, 2004) (discussing new e-mail sender authentication efforts such as DomainKeys, Sender Permitted From, and caller ID for e-mail); Evan I. Schwartz, *Spam Wars*, Tech. Rev., at 32, 34-35 (July/Aug. 2003) (discussing technological solutions such as signature-based filtering, collaborative filtering, gateway intercepts, heuristic filtering, Bayesian filtering, circles of trust and vaccinations); Hanah Metchis & Solveig Singleton, *Spam, That Ill O' the ISP: A Reality Check for Legislators, Competitive Enterprise Institute* 9-12 <http://www.cei.org/pdf/3482.pdf> (May 21, 2003) (discussing technological solutions such as content filters, whitelists, challenge-response systems, collaborative filtering, blacklists (also called "block lists"), bonded sender programs and protocol redesigns); *Ferris Research, Spam Control: Problems and Opportunities* 29-34, 39-42 <http://www.ferris.com/rep/200301/report.pdf> (Jan. 2003) (surveying the various anti-spam technology providers).

quence is preventing minority interests from exchanging relevant content.

C. Spammers Impose Costs on Third Parties

As it moves from sender to recipient, spam generates bandwidth and server processing costs for the spammer's IAP, the recipient and the recipient's IAP. Depending on a spammer's practices, they can also impose some costs on unsuspecting third parties, such as server operators with open mail relays and or whose domains are forged. We consider each cost in turn.

1. *The Spammer's IAP*

The spammer and its IAP have contractual privity, and the IAP can technologically constrain the spammer's activities (i.e. capping the quantity of e-mails sent). As a result, a spammer's IAP has the capacity to charge spammers for any spam-related costs,[30] and there are no obvious market failures that require regulatory protection for the spammer's IAP.

2. *Recipients and Their IAPs*

It is frequently claimed that recipients pay to receive spam,[31] and sometimes spam is likened to junk mail sent with postage due.[32] With respect to individuals with a consumer IAP account, this claim is no longer accurate. It was true prior to the mid-1990s, when many IAPs charged customers a time-based fee for Internet connectivity. Because each e-mail took some time to download, recipients paid a small fee for each e-mail they received. Today, consumer IAPs almost universally charge flat-rate pricing for unlimited usage,[33] so consumer recipients do not pay for each e-mail received.

---

30. Privity and technological control also apply to IAPs or e-mail service providers who provide spammer "dropboxes," where the spammer directs replies to a validly-established e-mail account that the spammer knows will be overrun and shut down.

31. *See e.g. CAN-SPAM Act*, *supra* n. 1, at §2(a)(3) (legislative finding of Congress); Cal. Bus. & Prof. Code § 17529(e) (2003) (legislative finding of California); *State v. Heckel*, 24 P.3d 404, 410 (Wash. Sup. Ct. 2001); Proceedings, Federal Trade Commission Spam Forum (Day One) 6 <http://www.ftc.gov/bcp/workshops/spam/transcript_day1.pdf> (Apr. 30, 2003) (statement of Chairman Muris).

32. *See* Cal. Bus. & Prof. Code § 17529(h) (2003) (legislative finding of California).

33. *See* John Borland, *CNET News.com, Putting a Lid on Broadband Use* <http://news.com.com/2102-1034_3-5079624.html?tag=st_util_print> (Sept. 22, 2003) (but noting that some cable broadband providers are trying to impose some high-end usage limits to avoid line congestion). In contrast, many non-US telephone callers pay per-minute connect charges to make local calls, in which case callers accessing the Internet via dial-up connections pay time-based connection fees for reading or downloading their e-mail. Many service providers do limit the size of a customer's e-mail account, so in theory a user might procure

However, recipient IAPs bear some bandwidth and server processing costs for each e-mail they process, plus preventative costs (like filtering) and remediation costs (like blocking or database repair) associated with pernicious e-mail. Unlike the spammer's IAP, the recipient's IAP has no contractual privity or technological relationship with the spammer. And where corporations provide Internet connectivity to their employees, they incur these costs as a recipient directly. As a result, recipient IAPs and corporations may benefit from legal systems that allow them to pass those costs back to spammers or avoid the costs altogether.

Until recently, common law trespass to chattels was an important legal mechanism to accomplish that objective.[34] However, in *Intel Corp. v. Hamidi*,[35] the California Supreme Court recently scaled the doctrine back, rejecting trespass to chattels when a low-volume spammer's e-mails did not threaten to impair (or actually impair) the functioning of Intel's systems.[36] It remains unclear how subsequent courts will interpret *Intel*, but in all likelihood some future spammers will avoid liability for trespass to chattels.

Irrespective of trespass to chattels, corporations and recipient IAPs can use, and have successfully used, the *Computer Fraud and Abuse Act* ("CFAA") to combat spam.[37] *CAN-SPAM* supplements the CFAA (and whatever is left of common law trespass to chattels) by providing recipient IAPs a direct cause of action when the IAP is "adversely affected" by a spammer who fails to comply with selected other provisions of *CAN-SPAM*.[38] Depending on how broadly courts interpret the words "adversely affected," this provision may moot *Hamidi's* common law analysis by providing a statutory cause of action. At minimum, *CAN-SPAM* expedites recipient IAP causes of action by providing statutory damages and attorneys' fees[39] and by providing another basis (in addition to the CFAA) for federal court jurisdiction. As a result, *CAN-SPAM* should

---

a larger e-mail account to ensure enough capacity for both wanted e-mails and spam. However, users who regularly purge their e-mails should rarely encounter a problem.

34. *See e.g. Am. Online, Inc. v. IMS*, 24 F. Supp. 2d 548 (E.D. Va. 1998); *Am. Online, Inc. v. Natl. Health Care Discount, Inc.*, 174 F. Supp. 2d 890 (N.D. Iowa 2001); *Am. Online, Inc. v. Over the Air Equip., Inc.*, Civil Action 97-1547-A (E.D. Va. Nov. 19, 1997); *Am. Online, Inc. v. Prime Data Sys., Inc.*, 1998 WL 34016692 (E.D. Va. 1998); *CompuServe Inc. v. Cyber Promotions, Inc.*, 962 F. Supp. 1015 (S.D. Ohio 1997); *Hotmail Corp. v. Van$ Money Pie Inc.*, 1998 WL 388389 (N.D. Cal. 1998).

35. 1 Cal. Rptr. 3d 32 (Cal. Sup. Ct. 2003).

36. *Id.* at 43.

37. *See e.g. Am. Online, Inc. v. IMS*, 24 F. Supp. 2d 548 (E.D. Va. 1998); *Am. Online, Inc. v. Natl. Health Care Discount, Inc.*, 174 F. Supp. 2d 890 (N.D. Iowa 2001); *Hotmail Corp. v. Van$ Money Pie Inc.*, 1998 WL 388389 (N.D. Cal. 1998).

38. *CAN-SPAM Act*, *supra* n. 1, at § 7(g).

39. *Id.* § 7(g)(3)-(4).

help recipient IAPs control some of the e-mail processing costs that are externalized to them.

In addition to bandwidth, server, preventative and maintenance costs, some companies have sought legal recognition for the time employees waste on spam.[40] Indeed, analysts claim that this lost time creates enormous costs.[41] However, as discussed in Section II *supra*, time spent sorting or reading spam is not necessarily wasted, nor is it unique compared to the many other ways that employees waste time (e.g. personal e-mail, junk mail and personal telephone calls). Therefore, lost productivity due to spam is a poor policy basis for regulating spam.

3. *Open Mail Relays*

Spammers can offload costs to third party computers who have open mail relays, which can cause those server operators to incur some costs like any other recipient IAP. Of course, operators wishing to avoid those costs can simply close their mail relays, and interestingly these operators are often considered part of the problem, not victims.[42] Thus, forcing them to internalize the spam-created costs (rather than pushing those costs to a spammer) may motivate them to close the relays.[43]

---

40. *See Intel Corp. v. Hamidi*, 1 Cal. Rptr. 3d 32.

41. *See* Nucleus Research, *Spam: The Silent ROI Killer, Research Note D59* <http://www.nucleusresearch.com/research/d59.pdf> (accessed July 1, 2003) (claiming that employees have an average lost productivity of 1.4 percent per year, meaning that spam costs $874 per employee per year); Ferris Research, *Spam Control: Problems and Opportunities* 7, 16-17 <http://www.ferris.com/rep/200301/report.pdf> (accessed Jan. 2003) ("[i]n 2002, the total cost of spam to corporate organizations in the United States was $8.9 billion," of which forty-four percent was attributable to lost productivity); Basex, *Spam E-mail and Its Impact on IT Spending and Productivity* 5 <http://www.basex.com/poty2003.nsf/e67dc0f5617d6e9c85256a99005ea0e7/f8761f74ba37069385256e040019f314/$FILE/BasexReport.Spam.pdf> (Dec. 2003) ("[t]he cost of spam to companies worldwide is ca. $20 billion and growing at almost 100% per year"). *See generally* Saul Hansell, *Diverging Estimates of the Cost of Spam*, N.Y. Times, at C1 (July 28, 2003) (discussing and critiquing these studies).

42. *See* Wyo. Stat. Ann. § 40-12-402(b)(iii) (2003) (treating operators of open mail relays as responsible for participating in the dissemination of spam); Declan McCullagh, *CNET News.com, FTC Eyes Network Operators in Spam Battle* <http://news.com.com/2102-7355_35150455.html?tag=st_util_print> (Jan. 29, 2004) (the FTC e-mailed thousands of network operators with open mail relays asking them to stop); Chip Rosenthal, *MAPS TSI: Anti-Relay: What is Third-Party Mail Relay?* <http://mail-abuse.org/tsi/ar-what.html> (Apr. 23, 2001) (indicating that networked computers that permit open mail relays may be "blacklisted" by anti-spam vigilante groups).

43. Although *CAN-SPAM* did not expressly set up a cost-shifting mechanism for operators of open mail relays, it did criminalize their use by spammers. *See CAN-SPAM Act*, *supra* n. 1, at §§ 4(a)(1), 5(b)(3).

4. *Targets of Forged Headers*

Spammers also can offload costs to third parties using forged headers. A forged header occurs when a spammer manipulates an e-mail to make it look like the spam originated from X.com when it is really being sent from Y.com.[44] The X.com domain name operator (or its IAP) incurs costs when undeliverable messages and recipient complaints are directed to the operator.

The operator of a forged domain name lacks any contractual or technological way to prevent this activity,[45] so regulatory protection is appropriate. Indeed, thirty states prohibited forged headers,[46] and these state

44. *See id.* at § 3(8) (defining "header information").

45. Forged headers can be prevented only if e-mail senders are better authenticated. Project Lumos is being developed to tackle that problem. *See* Hans Peter Brondmo et al., E-mail Service Provider Coalition, *Project Lumos: A Solutions Blueprint for Solving the Spam Problem by Establishing Volume E-mail Sender Accountability* <http://www.networkadvertising.org/espc/Project_Lumos_White_Paper.pdf> (Sept. 24, 2003); *see also* Olsen, *supra* n. 25.

46. *See* Arizona [Ariz. Rev. Stat. § 44-1372.01(A)(1) (2003)], Arkansas [Ark. Code Ann. § 4-88-603(c)(2) (Michie 2003)], Colorado [Colo. Rev. Stat. § 6-2.5-103(2) (2000)], Connecticut [Conn. Gen. Stat.§ 53-451(b)(7) (1999)], Delaware [Del. Code Ann. tit. 11, § 937(b) (1999)], Idaho [Idaho Code § 48-603E(3)(b) (Michie 2000)], Illinois [815 Ill. Comp. Stat. 511/10(a) (2003)], Indiana [Ind. Code § 24-5-22-7(2) (2003)], Iowa [Iowa Code § 714E.1(2)(b) (1999)], Kansas [Kan. Stat. Ann. § 50-6,107(c)(1)(A) (2002)], Louisiana [La. Rev. Stat. Ann. § 73.6(B) (1999)], Maine [Me. Rev. Stat. Ann. tit. 10, § 1497(5)(B) (2003)], Maryland [Md. Com. Law § 14-3002(b)(2)(ii) (2002)], Michigan [Mich. Stat. Ann. § 445.2501(4)(b) (2003)], Minnesota [Minn. Stat. § 325F.694(2)(1) (2002)], Nevada [Nev. Rev. Stat. 205.492(1)(a) (2003)], North Carolina [N.C. Gen. Stat. § 14-458(6) (1999)], North Dakota [N.D. Cent. Code § 51-27-02(1)(a) (2003)], Ohio [Ohio Rev. Code Ann. § 2307.64(H) (West 2002)], Oklahoma [Okla. Stat. tit. 15, § 776.6(A)(1) (2003)], Oregon [Or. Rev. Stat. § 646.607(3)(1)(c) (2003)], Pennsylvania [18 Pa. Cons. Stat. § 7661(a)(1) (2002) and Pa. Cons. Stat. tit. 73 § 2250.4(2) (West 2002)], Rhode Island [R.I. Gen. Laws § 11-52-4(7) (1999)], South Dakota [S.D. Codified Laws § 37-24-37(1) (Michie 2002)], Texas [Tex. Bus. & Com. Code Ann. § 46.002(1) (Vernon 2003)], Utah [Utah Code Ann. §§ 13-36-103(2) (2002)], Virginia [Va. Code Ann. § 18.2-152.3:1(A)(1) (Michie 2003)], Washington [Wash. Rev. Code § 19.190.020(1)(a) (1999)], West Virginia [W. Va. Code Ann. § 46A-6G-2(1) (Michie 1999)], Wyoming [Wyo. Stat. Ann. § 40-12-402(a)(i) (Michie 2003)].

In addition, fourteen states prohibited the dissemination of software used to forge header information. *See* Arkansas [Ark. Code Ann. § 5-41-205(a)(3) (Michie 2003)], Connecticut [Conn. Gen. Stat.§ 53-451(c) (1999)], Delaware [Del. Code Ann. tit. 11, § 937(c) (1999)], Illinois [720 Ill. Comp. Stat. 5/16D-3(a-15) (2000)], Kansas [Kan. Stat. Ann. § 50-6,107(c)(5) (2002)], Louisiana [La. Rev. Stat. Ann. § 73.6(B) (1999)], Michigan [Mich. Stat. Ann. § 445.2501(5) (2003)], Nevada [Nev. Rev. Stat. 205.492(3) (2003)], Oklahoma [Okla. Stat. tit. 15, § 776.1(E) (2003)], Pennsylvania [18 Pa. Cons. Stat. § 7661(a)(2) (2002) and Pa. Cons. Stat. tit. 73 § 2250.4(5) (West 2002)], Rhode Island [R.I. Gen. Laws § 11-52-4(8) (1999)], Tennessee [Tenn. Code Ann. § 47-18-2501(g) (2003)], Virginia [Va. Code Ann. § 18.2-152.3:1(A)(2) (Michie 2003)], West Virginia [W. Va. Code Ann. § 46A-6G-4 (Michie 1999)].

laws may not be preempted by *CAN-SPAM*.[47] Meanwhile, *CAN-SPAM* criminalizes forged headers[48] and potentially sets up a private cause of action for some victims ("providers of Internet access services" who are "adversely affected").[49] The robustness of this private cause of action remains to be seen, but this *CAN-SPAM* provision, plus any coverage under non-preempted state laws and other existing doctrines like trademark law and the CFAA,[50] should provide substantial protection to the victims of forged headers.

5. *Conclusion on Costs*

Far too much rhetoric is directed to the costs borne by individual spam recipients. These individuals no longer bear a financial cost to receive spam, and any "costs" associated with the consumption of their attention makes unsupportable assumptions about the e-mail's relevancy to the recipient. Similarly, although sending IAPs may find it desirable to obtain regulatory protection against spam, they can control their financial exposure to spammers' behavior through pricing and technology.

Focusing on the costs borne by individual recipients and sending IAPs detracts from the parties who incur uncontrollable costs from spam, such as recipient IAPs, operators of open mail relays and victims of forged headers. *CAN-SPAM* provides some useful legal tools to protect these parties, although those tools may be incomplete. A crisper understanding of the real costs borne by these parties would have likely produced a more thoughtful legal solution.

D. Spam Contains or Promotes Objectionable Content

Many spam recipients complain about objectionable content of spam, especially pornographic spam.[51] Due to deep feelings towards pornographic spam, Congress specifically targeted it in *CAN-SPAM* by requir-

47. *See CAN-SPAM Act*, *supra* n. 1, at § 8(b)(1) (state laws that "prohibit falsity or deception in any portion of a commercial electronic mail message or information attached thereto" are not preempted).

48. *See id.* §§ 4(a)(1), 5(a)(1).

49. *See id.* § 7(g)(1).

50. *See Am. Online, Inc. v. LCGM, Inc.*, 46 F. Supp. 2d 444 (E.D. Va. 1998); *Parker v. C.N. Enters.*, No. 97-06273 (Tex. Dist. Ct. Sept. 17, 1997).

51. *See The Pew Report*, *supra* n. 10, at 44 ("[i]n nearly every measure we tested, pornography soared to the top as the most offensive, objectionable, destructive type of spam"); Taylor, *supra* n. 6 (eighty-six percent of those surveyed said pornographic spam annoyed them a lot); unspam, *Comprehensive Spam Survey (Oct. 2003)* <http://www.unspam.com/fight_spam/information/survey_oct2003.html> (Oct. 15, 2003) (ninety-six percent of parents are looking to block pornographic spam from reaching their children); *see also CAN-SPAM Act*, *supra* n. 1, at § 2(a)(5) (legislative findings of Congress).

ing warning labels.[52] But to understand the harms pornographic spam causes, it is useful to consider adults and minors separately.

For adults, pornographic spam is no different from any other form of unwanted content discussed in Section II(B) *supra*.[53] Nevertheless, Congress has tried to help adults avoid unwanted pornographic spam by requiring special labeling of pornographic spam in the subject line.[54] When implemented, this requirement can help recipients who automatically filter e-mail using the appropriate words because the spam will automatically be routed outside the recipient's ordinary view. Until spammers regularly comply with this law, however, filtering will not be helpful.

The mandatory labeling law may be even less helpful to recipients who manually sort e-mail. These recipients may still see objectionable content if the subject line contains objectionable terms or the recipient's e-mail software "previews" a message and the previewed content is objectionable.

So how can regulatory intervention help recipients avoid objectionable e-mails? With widely varying perceptions of what constitutes objectionable content, regulating objectionable ads is no more feasible than regulating irrelevant ads. Thus, the only "solution" may be for recipients to manage their exposures themselves, either through technological measures or by looking elsewhere when something offends.[55]

Putting the burden on recipients to avoid pornographic spam is less satisfactory when recipients are minors. In that case, society may be harmed when minors view this inappropriate material.[56]

However, minors' exposure to pornographic spam is a microcosm of a much greater problem: minors with e-mail accounts.[57] This is a major

52. *See CAN-SPAM Act*, *supra* n. 1, at § 5(b). Several states had also targeted pornographic spam, including Alaska, Arkansas, Kansas, Louisiana, Pennsylvania, Utah, West Virginia and Wisconsin. *See* David E. Sorkin, *Spamlaws.com, Spam Laws: United States: State Laws: Summary* <http://www.spamlaws.com/state/summary.html> (accessed Oct. 30, 2003).

53. However, some adults find viewing pornographic spam qualitatively more objectionable than other spam.

54. *See CAN-SPAM Act*, *supra* n. 1, at § 5(b).

55. *Cf. Cohen v. Cal.*, 403 U.S. 15 (1971) (putting the burden on citizens to redirect their attention if they objected to a profanity-emblazoned jacket).

56. It is well-accepted that states have a compelling state interest in protecting minors from being exposed to materials that are indecent or harmful to them. *Reno v. Am. Civ. Liberties Union*, 521 U.S. 844 (1997) ("[w]e agreed that 'there is a compelling interest in protecting the physical and psychological well being of minors' which extended to shielding them from indecent messages that are not obscene by adult standards") (quoting *Sable Commun. v. FCC*, 492 U.S. 115 (1989)).

57. This is a rapidly growing phenomenon. *See* Symantec Corporation, *Symantec Survey Reveals More than 80 Percent of Children Using E-mail Receive Inappropriate Spam Daily* <http://www.symantec.com/press/cgi/printfriendlypress.cgi?release=2003/n030609a.

social development because historically minors had few communication media that readily bypassed parental oversight. Today, minors can use e-mail, instant messenger, and cell phones to communicate with third parties without any parental oversight and knowledge. With this additional autonomy, minors can get into inappropriate and potentially very dangerous situations, such as interactions with sexual predators.[58]

Because of these risks, some parents restrict minors' access to the Internet altogether, and other parents permit only supervised Internet use. The former prevents any risk of exposure to pornographic spam, and the latter approach gives parents the ability to pre-screen pornographic spam or counsel the minor when seeing such spam.

Otherwise, parents who let minors have unsupervised e-mail use make a huge decision, and it is not made lightly. Because these parents accept the risk that their children will engage in dangerous online behavior, the problem of pornographic spam seems almost trivial by comparison. If the parents trust their children enough to give them that autonomy, perhaps we should infer that the parents deem their children responsible enough to cope with pornographic spam.

Regulation cannot easily solve these problems. Efforts to specifically ban pornographic spam are likely unconstitutional[59] and do not affect e-mails from foreign jurisdictions. Lesser efforts, like mandatory labeling, have low efficacy. Ultimately, there can be no substitute for parental involvement in their children's use of e-mail.

---

html> (June 9, 2003) (news release of the Symantec Corporation) (seventy-six percent of minors between ages seven and eighteen have at least one e-mail account).

58. *See* Abigail Van Buren, *Internet Predators Pose a Challenge to All Parents*, Milwaukee J. Sentinel <http://www.jsonline.com/lifestyle/advice/oct03/180747.asp?format=print> (Oct. 29, 2003). Inevitably, children will also get inappropriate e-mail. Symantec Corporation, *Symantec Survey Reveals More than 80 Percent of Children Using E-mail Receive Inappropriate Spam Daily* <http://www.symantec.com/press/cgi/printfriendlypress.cgi?release=2003/n030609a.html> (June 9, 2003) (news release of the Symantec Corporation) (eighty percent of surveyed minors received inappropriate spam on a daily basis).

59. *See Reno v. Am. Civ. Liberties Union*, 521 U.S. 844 (1997) (declaring the *Communications Decency Act* unconstitutional); *Am. Civ. Liberties Union v. Napolitano*, No. CV-00-0505-TUC-AM (D. Ariz. 2002) (striking down Arizona's statute); *Am. Booksellers Found. v. Dean*, 342 F.3d 96 (2d Cir. 2003) (striking down Vermont's statute); *Am. Library Assn. v. Pataki*, 969 F. Supp. 160 (S.D.N.Y. 1997) (striking down New York's statute); *Cyberspace Commun., Inc. v. Engler*, 238 F.3d 420 (6th Cir. 2000) (striking down Michigan's statute); *Am. Civ. Liberties Union v. Johnson*, 194 F.3d 1149 (10th Cir. 1999) (striking down New Mexico's statute); *PSINet v. Chapman*, 167 F. Supp. 2d 878 (W.D. Va. 2001) (striking down Virginia's statute); *Bookfriends, Inc. v. Taft*, 233 F. Supp. 2d 932 (S.D. Ohio 2002) (striking down Ohio's statute).

III. CONCLUSION

Society is still evolving ways to cope with media saturation. Spam contributes to this problem, but so do other media. Yet, many recipients hate spam more than other ads. As explored by this Essay, this dichotomous attitude is hard to explain. Nevertheless, the anger has caused anti-spam rhetoric to reach hyperbolic levels. But, while many spam opponents decry spam as a system breakdown, the breakdown has been more political than technological. Most state-based attempts to regulate spam, a product of political grandstanding or legislator rage instead of rational policy-making, were ineffectual,[60] reflecting their weak policy underpinnings. Early feedback on *CAN-SPAM* suggests the federal law will not be any more effective.[61]

Even if *CAN-SPAM* beneficially affects the flow of unwanted e-mails, any legislative solution seems inherently empty. Without legislative intervention, society will find ways to cope with spam, just as we have with other media. Meanwhile, entrepreneurs will continue to develop better tools to sort wanted and unwanted communications. Thus, more patience with the spam "problem" might have facilitated the development of superior results organically.

---

60. *See e.g. E-mail in December Dominated by Spam*, L.A. Times (Jan. 3, 2004) (available in LEXIS, News & Business >News> By Individual Publication >L> Los Angeles Times) (citing a study by MessageLabs showing that spam had increased from thirty-four percent of all e-mail in December 2002 to fifty-six percent of all e-mail in December 2003); Brightmail Inc., *50% of Internet E-Mail is Now Spam According to Anti-Spam Leader Brightmail®* <http://www.brightmail.com/pressreleases/082003_50-percent-spam.html> (Aug. 20, 2003) (press release of Brightmail Inc.) (quoting Enrique Salem, Brightmail President and CEO, as saying that "In less than 2 years, spam messages have increased from 8% of all e-mail traffic to more than half").

61. *See* Stefanie Olsen, *CNET News.com, Study: Spammers Turning Blind Eye to the Law* <http://news.com.com/2102-1032_3-5156629.html?tag=st.util.print> (Feb. 10, 2004) (citing studies showing that only three percent of bulk commercial e-mail complied with the law, that spam had increased as a percentage of all e-mail following the law's passage, and that more spam was originating overseas since the law passed).

Then again, many experts never expected the law to be effective, which perhaps reinforces that the predominant problem with spam is political. *See* Declan McCullagh, *CNET News.com, Spam Keeps Cookin'—Despite New Laws* <http://news.com.com/2102-1024_3516 0503.html?tag=st.util.print> (Feb. 17, 2004) ("[a] U.S. Justice Department prosecutor warned Tuesday that a new spam law's criminal sanctions likely will not stem the flow of bulk solicitations that are flooding into e-mail in-boxes").