Opting Out of Spam:  
A Domain Level Do-Not-Spam Registry

Rebecca Bolin†

INTRODUCTION

Spam, or unsolicited commercial email, drastically lowers the costs of advertising directly to prospective consumers by exploiting open electronic mail protocols. And it has become an obnoxious big business. Markets, norms, and technological measures have all failed to change sufficiently the economics of the spam business model. Spam is clogging businesses' servers and users’ inboxes, and costing too much money and time in return for too little benefit. This Note argues that despite widespread criticism, current federal spam law has in fact effectively targeted the most egregious senders. But it has also created an entitlement to send spam—one free message—before a recipient’s wish to avoid spam must be honored. This reverses the entitlement set in other media and ignores consumer demand for privacy and a Do-Not-Call Registry for email.

Part I of this Note describes spam, its scale, and its costs and benefits. Part II analyzes attempts to use the market and state legislation to fix the problem. It explains why these efforts failed, and why federal legislation was required. Part III outlines the successes of CAN-SPAM, the groundbreaking federal spam law, as well as the interlocking set of state laws used to combat spammers. Part IV compares spam law to policies addressing unsolicited commercial speech in other media and proposes a policy suggested in CAN-SPAM, but ultimately overlooked: a Do-Not-Call Registry for email. This Note concludes that a Do-Not-Spam Registry balances the easy detection of a strict liability rule with the

† Yale Law School, J.D. expected May 2006, registered patent agent. The author would like to thank Alvin Klevorick, Ian Ayres, Jack Balkin, James Grimmelmann, Adam Stubblefield, and Ira Rubenstein with Microsoft Legal Counsel for their help on this piece. This Note was made possible by Microsoft Corporation’s generous support of the Yale Information Society Project.

1. Spam is defined in this Note as any unsolicited commercial email. There are many definitions of spam, from annoying forwards by friends to an email volume reaching numeric thresholds. This Note views spam as any unsolicited advertisement email. This Note also analyzes spam as commercial speech, making non-commercial spam, though annoying, beyond the scope of this Note. For a discussion of political spam, see Seth Grossman, Note, Keeping Unwanted Donkeys and Elephants Out of Your Inbox: The Case for Regulating Political Spam, 19 BERKELEY TECH. L.J. 1533 (2004). Spam-style communications in other media, including SMS spam, VoIP spam (spit), and instant messaging spam (spim), are increasingly problematic, but this Note will confine itself to email spam.

speech freedoms safeguarded by an opt-out system.

I. WHY EVERYONE HATES SPAM

Spam was the invention of a group of crafty immigration lawyers, who bombarded some 2600 unrelated Usenet newsgroups with electronic advertising in 1994. The term “spam” was inspired by a Monty Python skit about a restaurant in which a group of Vikings drowns out all conversation by repeating “Spam!,” and while Hormel Foods sometimes insists on protecting its SPAM trademark, spam is now widely used to refer to junk email.

While spam has been a nuisance since the earliest days of electronic mail, in recent years it has become a mission-critical problem that can take down entire companies’ mail servers, spread viruses, compromise systems, and overwhelm frustrated users. This Part assesses those costs, bearing in mind that some spam does have value to recipients, and that that value must be considered in any spam policy proposal.

A. Externalized Costs

The fundamental problem with spam is that it externalizes costs to millions of uninterested users. Anyone who uses email has encountered unsolicited advertisements in his inbox. Spammers (or, more politely, direct email marketers), sell all kinds of products using unsolicited emails containing hyperlinks that, when clicked, bring customers to a website storefront selling goods and services of varying quality and authenticity. E-commerce (now just commerce) often depends on the same tools. For example, Amazon.com also has a website storefront, promotional email, and transactional email, but spammers use a different kind of marketing plan to reach millions of unwitting consumers. While data-mining technology would allow super-customized spam, most spam has taken the opposite strategy, indiscriminately lobbing literally millions of cheap emails at unwitting recipients. Even the most targeted spam is intentionally overbroad, to avoid missing a potential buyer.

Spam is made possible by the architecture of email, which, while intended

---

4. CONNOLLY, supra note 3, at 367. The skit has now been incorporated into a Broadway musical, which ironically suffered security problems in the form of leaked email addresses of parties who signed up for information. David F. Gallagher, What To Expect of 'Spamalot'? A Lot of Spam, N.Y. TIMES, Mar. 12, 2005, at B9.
to make email free and accessible, has also created a structure of costs such that
there is little difference between sending a thousand emails or one hundred
million. Spam is thus the price we pay for the Internet’s principles of freedom
and universal access. The standard mail protocol, SMTP, is based on the
TCP/IP Internet structure. Like these protocols, SMTP was developed as a
collective, free standard to allow for the free flow of information. SMTP is a
“trusting” architecture, meaning it accepts senders’ data by default, making it
an easy target for fraud. Changing SMTP to require, say, authentication, or a
payment scheme, would be highly disruptive (if not impossible), because open
protocols have no real authority over vendors. As such, change on that scale is
unlikely. SMTP itself requires neither authentication nor payment in order to
shuffle an email through several computers until it reaches its destination.

Spam is further enabled by its low marginal costs. Spammers face some
startup costs: hardware, specialized software, bandwidth, address lists, message
composition, revenue infrastructure, and legal or reputation risk. However,
once an operation is equipped to send millions of emails, the marginal cost of
sending a few thousand more emails is quite low—just a bit of bandwidth and
some legal risk. The same infrastructure can be used at minimal additional
cost to send millions of emails on behalf of multiple clients.

Email’s open architecture and low marginal costs thus combine to create a
forgiving cost structure. A spammer can make money with as low as a 0.005%
response rate, or even a 0.000005% response rate, compared with the almost
2% response rate required of direct mailings and the 8.55% response rate
required in telemarketing. As self-proclaimed spam king Alan Ralsky has
bragged: “When you’re sending out 250 million e-mails, even a blind squirrel
will find a nut.” This strategy of sheer bulk is of course impossible in physical
space, where ads are often carefully chosen and designed for intended

---

7. Reduction in Distribution of Spam Act of 2003: Hearing on H.R. 2214 Before the H. Comm. on
8. Id. at 4 (statement of Rep. Scott).
9. Derek E. Bambauer, Solving the Inbox Paradox: An Information-Based Policy Approach to
Unsolicited E-mail Advertising, 10 VA. J.L. & TECH. 5, 15-17 (2005).
10. Id. at 17-19. It is sometimes possible, however, for parties to adopt new protocols without
consensus. See infra note 66.
11. It is possible to add some authentication features without modifying SMTP itself. For example,
SPF authentication, discussed infra note 66, modifies the SMTP server and not the SMTP protocol.
incremental cost” for the volume of spam).
http://www.businessweek.com/smallbiz/content/sep2002/sb20020926_5958.htm.
15. See Tim Madigan, There Are 10 Million Reasons Why You Hate This Man, FT. WORTH STAR
TELEGRAM, Apr. 27, 2003, at 1G.
17. Mike Wendland, Spam King Lives Large Off Others’ E-Mail Trouble, DETROIT FREE PRESS,
Nov. 22, 2002, at 1A.
consumers. (Even seemingly haphazard postal bulk mailings are targeted; a mailing campaign would never, for example, send millions of pieces of mail to addresses that do not even exist, a common occurrence in the world of spam.\textsuperscript{18})

On the other hand, costs to both users and Internet Service Providers (ISPs)\textsuperscript{19} are more substantial: bandwidth, hardware, software (filtering), message processing at the ISP and user level, risk to reputation and users from fraudulent spam, and the non-trivial psychological harm of email degradation and offensive email.\textsuperscript{20} Spam senders, of course, do not compensate users and ISPs for these expenses.\textsuperscript{21} Spam, which is estimated to make up eighty percent of email traffic,\textsuperscript{22} costs American businesses somewhere between $17 and $21.6 billion each year.\textsuperscript{23} Mail providers now spend $1 billion a year on filtering alone,\textsuperscript{24} and users spend an average of three minutes a day deleting spam.\textsuperscript{25}

Email is now becoming frustrating for many users.\textsuperscript{26} In other media, we are exposed to invasive, unwanted advertisements every day—on television, radio, or even on standard websites. A key difference between spam and these more traditional unwanted advertisements is that the latter pay for some good, such as the content of a broadcast.\textsuperscript{27} One can also avoid them by simply not tuning in. Spam, however, is unwanted speech that a receiver must either receive or pay not to receive by paying for filters. Just as few postal customers would accept a COD advertisement, few, if any, users of spam find its value worth the

\textsuperscript{18} S. REP. NO. 108-102, at 3 (2003); JEREMY POTEET, CANNING SPAM: YOU’VE GOT MAIL (THAT YOU DON’T WANT) 21-24 (2004). Targeted physical mailing campaigns are also based on sophisticated location demographic data. See MARK MONMONIER, SPYING WITH MAPS: SURVEILLANCE TECHNOLOGIES AND THE FUTURE OF PRIVACY 6-11 (2002).

\textsuperscript{19} Not all mail providers are ISPs, so this terminology is not exact. A user’s ISP does not have to correlate to her email provider; for example, a major ISP in New Haven is Comcast, but a user’s email address could be through Hotmail, Yahoo, or even Yale. In this Note, the term ISP will be used to refer to any service provider that provides mail to users.

\textsuperscript{20} Bambauer, supra note 9, at 22-25.

\textsuperscript{21} A compensation system has been proposed both for email, see infra Part III, as well as for telemarketing. See Ian Ayres & Matthew Funk, Marketing Privacy, 20 YALE J. ON REG. 77 (2003).


\textsuperscript{24} Jon Swarz, Anti-Spam Industry Consolidating Fewer Vendors To Offer Broader Service Range, USA TODAY, July 20, 2004, at 2B.

\textsuperscript{25} 2004 NATIONAL TECHNOLOGY READINESS SURVEY, supra note 23. Twelve percent of users spend half an hour or more dealing with spam. FALLOWS, supra note 23, at 16.

\textsuperscript{26} Twenty-five percent of users have decreased their use of email because of spam. FALLOWS, supra note 23, at 1; see also James McNair, From the Stockroom to the Boardroom, It’s Paralyzing All Facets of Business, CINCINNATI ENQUIRER, Nov. 16, 2003, at 1D.

\textsuperscript{27} YOCHAL BENKL, THE WEALTH OF NETWORKS: HOW SOCIAL PRODUCTION CHANGES MARKETS AND FREEDOM (forthcoming 2006) (manuscript at 179-80, on file with author) (discussing advertising-based funding of media in democracies).
Opting Out of Spam

price. In fact, some users are willing to pay two dollars per mailbox per month to filter it.\textsuperscript{28} AOL, for example, now deletes some eighty percent of incoming mail to its subscribers.\textsuperscript{29} And spam is especially invasive to recipients because it is both a "push" communication like telemarketing,\textsuperscript{30} and also (unlike browsing web pages on the Internet\textsuperscript{31}) has the capacity to be a one-to-many communication, like television.\textsuperscript{32}

The time costs in dealing with spam as unwanted speech are burdensome to users. Stumbling across, say, a Barbie billboard or an anti-Barbie protest website during an Internet search for Barbies is very different than spending three minutes a day scraping ads for Barbies off your mailbox. Assuming that the average user spends three minutes a day, or ninety minutes a month, deleting spam, and using a conservative estimate of $11.00 per hour for a consumer's time,\textsuperscript{33} she spends $16.50 a month, or $200.75 a year, dealing with spam. Not only does this cost represent a severe degradation of the medium of email, spam is also all-too-often offensive,\textsuperscript{34} fraudulent,\textsuperscript{35} or infected with viruses.\textsuperscript{36}

B. \textit{Valuing Spam As Speech}

Though spam has extraordinary external costs, some spam does confer benefits. Users sometimes find spam informative and buy products advertised by it. A 2004 poll showed that about four percent of email users say they have made purchases because of spam and fully fourteen percent do read it.\textsuperscript{37} One to six percent of spam emails results in a clickthrough—that is, a link clicked on

\begin{itemize}
\item [28.] S. REP. NO. 108-102, at 6 (2003).
\item [29.] Id. at 2.
\item [30.] A listener initiates a pull communication (newspaper) but not a push communication (telemarketing). A one-to-one communication is an interaction between one speaker and one listener (telephone); a one-to-many communication is the broadcast model (television). Spam is a push communication. Khaldoun Shobaki, \textit{Speech Restraints for Converged Media}, 52 UCLA L. REV. 333, 360-361 (2004). However, spam is usually not a one-to-one communication like telemarketing, making Shobaki's discussion of spam as similar to telemarketing somewhat misleading.
\item [34.] Seventy-six percent of users are bothered by offensive or obscene spam. FALLOWS, supra note 23, at 27. \textit{See also} Fed. Trade Comm'n, \textit{False Claims in Spam} 12-13 (2003), available at \url{http://www.ftc.gov/reports/spam/030429spamreport.pdf} [hereinafter FTC FRAUD REPORT].
\item [35.] FTC FRAUD REPORT, supra note 34, at 3-10.
\item [36.] POSTINI, INC., 2005 \textit{EMAIL SECURITY ANNUAL REVIEW AND THREAT REPORT} 16 (2005), available at \url{http://www.postini.com/whitepapers/}.
\item [37.] 2004 \textit{NATIONAL TECHNOLOGY READINESS SURVEY}, supra note 23.
\end{itemize}
Finally, there is a more abstract informational value in unwanted speech, even commercial speech, as part of the marketplace of ideas.\textsuperscript{39} Because spam is a broad category, containing both the best and worst innovations in unwanted speech, it is challenging to quantify its value. Some spam has no value whatsoever in the marketplace of speech. Fraudulent speech, for one, is unprotected and makes no progress toward the truth,\textsuperscript{40} and an estimated forty percent of spam contains fraud in the message body, while forty-four percent contains fraud in either the “From” or “Subject” lines.\textsuperscript{41} The most permissive view of unwanted speech would perhaps allow this kind of speech but never support its value to a duped, paying recipient. Other kinds of spam are intentionally malicious. “Phishing” tricks users into disclosing personal data by pretending to come from a reputable company, while virus-laden spam attempts to damage users’ property.\textsuperscript{42} This kind of email is malicious fraud with no value to any recipients. The remaining spam is unrequested advertising, and of course even this last category of spam is a far cry from the truth-seeking unwanted speech Justice Holmes contemplated in the marketplace of unwanted speech.\textsuperscript{43}

The value of spam also depends upon the recipient. Some unwanted speech may be valuable to a few, but may be so offensive to others that the costs far outweigh the benefits. Graphic advertising for pornographic and medicinal products is often deeply offensive to some users, who view themselves as victims of what others might see as merely titillating speech.\textsuperscript{44} Even when the content—such as cures for erectile dysfunction—is freely discussed in traditional media, spam seems to render it more offensive.\textsuperscript{45} In one particularly

\textsuperscript{38} Alan Ralsky, a reclusive spammer, disclosed a less than one percent clickthrough rate in his only media interview. Wendland, \textit{supra} note 17. Industry results can be up to six percent. Kris Oser, \textit{Date.com Moves Away From E-mail}, DIRECT, July 1, 2003, at 9.

\textsuperscript{39} Bambauer, \textit{supra} note 9 (arguing for the informational value of spam); Note, \textit{The Impermeable Life: Unsolicited Communications in the Marketplace of Ideas}, 118 HARV. L. REV. 1314 (2005). But see Fisher, \textit{supra} note 33 (arguing commercial speech in spam should be entitled to little First Amendment protection).

\textsuperscript{40} See, e.g., Illinois ex rel. Madigan v. Telemarketing Assocs., 538 U.S. 600 (2003) (ruling fraudulent practices in fundraising are not protected speech).

\textsuperscript{41} FTC FRAUD REPORT, \textit{supra} note 34, at 7-8.

\textsuperscript{42} Research suggests that 1.15\% of email contains viruses. POSTINI, INC., \textit{supra} note 36, at 16.

\textsuperscript{43} Abrams v. United States, 250 U.S. 616, 630 (1919) (Holmes, J., dissenting) (“[W]hen men have realized that time has upset many fighting faiths, they may come to believe even more than they believe the very foundations of their own conduct that the ultimate good desired is better reached by free trade in ideas—that the best test of truth is the power of the thought to get itself accepted in the competition of the market, and that truth is the only ground upon which their wishes safely can be carried out.”); see also Note, HARV. L. REV., \textit{supra} note 39, at 1333-34 (“The fact that most people associate these communications with ads for penis enlargement or mortgage refinancing undercuts any sense of vitality these communications may have as part of the marketplace of ideas.”). See generally C. Edwin Baker, \textit{Paternalism, Politics, and Citizen Freedom: The Commercial Speech Quandry in Nike}, 54 CASE W. RES. L. REV. 1161 (2004) (discussing other speech advocates’ skepticism of commercial speech claims).


\textsuperscript{45} Chris Becker, \textit{Spam is the Best Thing in My Life Right Now}, ADVANCE-TITAN (Univ. of Wis.-
graphic example, a testicular cancer survivor was so offended by an ad for penis enlargement pills that he threatened to kill the president of the marketing company after the company continued sending him messages after repeated opt-out requests; he committed suicide after he was criminally charged.\textsuperscript{46} When the content is not available in traditional media, the effects are more negative. About seventeen percent of spam contains automatically displayed adult images, and forty-one percent of these messages have misleading sender or subject information.\textsuperscript{47} Yet other spam contains offensive products or content, from gambling to textual pornography. The indiscriminate scope of spam means this kind of material can offend adults, subject workplaces to legal liability\textsuperscript{48} or, worse, fall into the inboxes of children and young adults.\textsuperscript{49} Since spam is a "push," one-to-many communication, even when offensive speech may have great value to some, the remainder's disgust at the communication may make it inefficient.

Some spam does have higher value, such as highly specialized advertising catering to specific interests. For example, in the aftermath of Terry Schiavo's front page right-to-die controversy, her parents sold a valuable ($500 a month) 4000-address list of "compassionate pro-lifers" who had donated to their legal effort.\textsuperscript{50} Targeted spam is probably more valuable to recipients because it is carefully chosen, but it is also particularly threatening to the privacy of those who, for example, innocently gave their email addresses to Terry Schiavo's parents.\textsuperscript{51}

The solution this Note proposes to these concerns about offensive, destructive, or invasive mail is to allow readers to self-select a domain, and opt out of communications they find offensive or annoying before that first message arrives.

\section*{II. FAILED SOLUTIONS}

The market has made Herculean efforts, both technical and legal, to block

\begin{thebibliography}{99}
\bibitem{Oshkosh} Oshkosh, Feb. 16, 2005, \textit{available at} http://www.advancetitan.com/story.asp?issue=11117&story =3630 ("[T]elevised spam uses images that hint at what their product is for because there are obviously standards of decency, and commercials for penis pills can't show graphic before-and-after pictures.").
\bibitem{FTCFRAUD} FTC FRAUD REPORT, \textit{supra} note 34, at 14.
\bibitem{Ganley} See generally Ganley, \textit{supra} note 31, at 250-62 (discussing privacy interests in many kinds of internet communications).
\end{thebibliography}
spam. This Part chronicles those efforts and argues that, while effective, these measures were insufficient. Indeed, the difficulty of circumventing technical safeguards has encouraged senders to send mail ever more cleverly. Early legal actions proved not to be strong enough: ISPs lacked the appropriate legal tools to collect the judgments they did win. Moreover, early spam laws were poorly tailored and just not strong enough to respond to the tricks of spammers. This Part discusses these efforts by the market and the lessons learned.

A. Non-Legal Solutions

Though the market alone has failed to stop spam, it has made an amazing and costly array of attempts to do so. Because ISPs and users bear the costs of spam advertising, they have always had financial and reputational incentives to change the economics of spam. These market-implemented solutions, briefly and incompletely outlined here, have evolved to delete the majority of unwanted mail, created the largest blacklists in history, executed large vigilante campaigns, and caused both competition and cooperation as ISPs work to ease their burden.

It is ISPs who face the complaints of consumers who hold them responsible for routing spam they had no part in producing. MSN, for one, claims spam is a top complaint of its subscribers, and a substantial number of customers indicate they are willing to switch ISPs if a competitor offers better spam filtering. Because spam has an impact on ISPs' reputations, their equipment, their customers, and ultimately their bottom line, ISPs have made a great effort to eliminate spam.

In the 1990s, spam was only a small percentage of email traffic, but ISPs were already working to delete unwanted mail. They were aided by the 1995 decision in Cyber Promotions v. AOL, which denied the so-called right to spam. A federal district court ruled that AOL's mail system was not like a company town providing public mail services, but rather more like private property; thus AOL could not be forced to route any piece of mail. This gave ISPs the legal authority to implement filtering and blocking policies. ISPs also started high-tech, vigilante "bombings," shutting down junk mailers by

54. Ian Austen, Most Wanted: Drilling Down Spam Protection: A Reason To Switch?, N.Y. TIMES, June 28, 2004, at C9 (Fourteen percent of dialup and eight percent of broadband users "definitely" would switch; thirty-three percent of dial-up and thirty-one percent of broadband users "probably" would switch to an ISP with better spam filtering).
56. Id.; see also Access Now, Inc. v. Sw. Airlines Co., 227 F. Supp. 2d 1312 (S.D. Fla. 2002) (ruling that a website was not a place of public accommodation under the ADA).
Opting Out of Spam
clogging their servers with return notices or other mail. More modern vigilant attacks would strike at the website bandwidth or revenue infrastructure of junk emailers. AOL now blocks subscribers' access to suspected spammers' websites. Lycos U.K. released a popular screensaver that would use idle computer time to access spammers' websites and waste bandwidth. This kind of widespread malicious access is called a distributed denial of service attack and is almost certainly illegal; Lycos U.K. stopped distributing its software within a week.

Today, ISPs act as private networks with ironclad user agreements allowing them to delete any mail without notice. The current federal spam law's safe harbor for ISP mail filtering protects "a policy of declining to transmit, route, relay, handle, or store certain types of electronic mail messages," or existing mail filtering policies. To identify and delete spam, these networks now depend on sophisticated, expensive filters, from Hotmail's patented Microsoft SmartScreen filters to the open source SpamAssassin. These filters are the first line of defense for ISPs; they block, or delete without even storing, a large percentage of spam. In September 2001, spam was only eight percent of all email traffic. By May 2003, the largest ISP, AOL, was blocking eighty percent of daily inbound mail, up from one-third just two months before and one-sixth in December 2002. In 2003, EarthLink reported a 500% increase in spam traffic in the previous eighteen months. Hotmail estimates that it deletes ninety-five percent of incoming mail. Without these ISP-level filters, many businesses would lack the capacity to handle all of their mail, not to mention the viruses and phishing contained in malicious spam.

These filters depend on a range of extralegal innovations. They are proprietary and intentionally opaque to prevent "work-arounds" by spammers. Filter specifications are closely guarded secrets and probably vary significantly between mail systems and over time. Hotmail, for example, uses as a filtering

57. See JAN SAMORISKI, ISSUES IN CYBERSPACE: COMMUNICATION, TECHNOLOGY, LAW, AND SOCIETY ON THE INTERNET FRONTIER 118-19 (2002). Today, this technique has fallen out of vogue because much server information is falsified, and even if it is not, a large amount of spam comes from "zombie" computers, personal computers infected with viruses used by spammers to route mail. Indeed, over half of spam may come from such hijacked "zombie" computers. Ross Wehner, Hook, Line, and Sinker Phishers Threaten E-Commerce: Crime Fighters Try To Stop Them, DENVER POST, Dec. 27, 2004, at E1.


60. See, e.g., Yahoo! Terms of Service § 6, http://docs.yahoo.com/info/terms/ (last visited Mar. 19, 2006) ("You acknowledge that Yahoo! may or may not pre-screen Content, but that Yahoo! and its designees shall have the right (but not the obligation) in their sole discretion to pre-screen, refuse, or move any Content that is available via the Service.").


factor a tracing technique based on sending servers called Sender ID, which is now forged in the majority of spam. SPF records on mail servers list authorized outgoing IP addresses, but these too have been widely forged. Yahoo!'s identification system, DomainKeys, which uses digital signatures to authenticate origin, may be more difficult to forge, but requires more computing power to process.

Despite Cyber Promotions, those who are excluded by terms of service continue to argue that ISPs should be considered common carriers, and that their policies are opaque or unfair. When ISPs spend millions of dollars building mission-critical, fragile filters to delete as much mail as quickly as possible, demands to disclose filtering policies seem at least counterproductive, if not entirely Pollyannaish. Though intellectually appealing, especially against the backdrop of cyber-freedom, forcing ISPs to justify every filtering decision would reduce or even destroy their filtering ability and thus result in more spam. And users would contract away their right quickly, as they do today, and silent filtering would continue.

Filtering does become problematic when it causes silent non-delivery of wanted messages (false positives), and there is evidence that the arms race of spam blocking is increasingly blocking legitimate messages. Because filtering's intent is not clear, such blocking is labeled censorship by those deleted. Filtering is, in a sense, censorship, but it censors what ISPs believe

66. See Matthew D. Sarrel, Authentic E-Mail: Smtp Authentication Holds Promise, But It's Not Yet a Real Spam-Stopping Solution, PC MAG., Dec. 2005, at 120. However, forged authentication data can still be valuable to filters blocking spammers. See Deborah Radcliff, Fighting Back Against Phishing, NETWORK WORLD, Apr. 11, 2005, at 48.
69. See David R. Johnson et al., The Accountable Internet: Peer Production of Internet Governance, 9 VA. J.L. & TECH. 9, 28-29 (2004). Calls for transparency are more convincing within the context of a right to receive information, such as the one guaranteed under South African law. See S. AFR. CONST. 1996, Bill of Rights § 16(1)(b) ("Everyone has the right to freedom of expression, which includes . . . freedom to receive or impart information or ideas."); Electronic Communications and Transactions Act 25 of 2002 s. 86 (S. Afr.) ("(1) . . . [A] person who intentionally accesses or intercepts any data without authority or permission to do so, is guilty of an offence. (2) A person who intentionally and without authority to do so, interferes with data in a way which causes such data to be modified, destroyed or otherwise rendered ineffective, is guilty of an offence."). This right as applied to email filtering has not been enforced however, nor has South Africa's spam law in general.
71. Written Testimony of Ronald Scelson, supra note 68.
Opting Out of Spam

(hopefully in good faith) their customers want deleted, and it relies upon customer consent to keep operations running smoothly (indeed, running at all). More importantly, ISPs have an economic incentive to deliver wanted mail and to delete as much unwanted mail as possible. Assuming a robust and rational ISP market, ideologically based censorship against users’ will should be limited and accidental.  

ISP filtering is aided by freely available public “blacklists,” lists of mail servers that the compilers consider abusive and believe ISPs should block. For example, Yale University voluntarily uses one such list compiled by Spamhaus, and under its terms of service deletes or returns mail from blacklisted domains. Other mail servers incorporate these blacklists as one of many factors in filtering mail. These lists are now compiled in only a few places, including Russia and the U.K., because of the legal problems encountered in the United States and elsewhere. The lists are generally accurate, but can be unfair, overbroad, or even bullies. After being put on a blacklist, a blocked party has virtually no legal remedy, and they must comply with the demands of the list-maker or continue to be blocked. At times, it seems these lists have the ability to knock entire regions, or even countries, off the email landscape on account of the bad behavior of a few.

ISPs and users also use “whitelists,” lists of approved senders, which ensure that wanted mail does not get caught in the spam filters. Most whitelisting is for known senders from whom users have opted to receive mail, but whitelisting is also used for unsolicited mail. A successful commercial venture of this type of whitelisting is Bonded Sender, a certifying authority that has partnered with

---

72. Some ISPs might have other reasons to filter. For example, a religious ISP might filter by content or even all mail from a selected region. In this case, assuming a robust market in ISPs, the ISPs’ interests will align with those of their customers.


409
ISPs including Hotmail. Bonded Sender operates using a client’s current technology, changing nothing except the recipient’s spam filter settings. ISPs promise to deliver mail sent by clients of Bonded Sender, but if complaints go over a few per million messages delivered, then bonds posted by the senders are cashed by a third party charity. Bonded Sender has not disclosed the number of bonds cashed, except to say it has been very small. Presumably this reflects the quality of the senders involved, allowing senders, in a sense, to put their money where their mouths are.

As of this writing, the next wave of spam management appears to be pay-to-play solutions. Isolated users have long used challenge-response systems, under which when a client receives mail from an unknown sender, it asks that sender to expend some cost, perhaps computing cycles completing a puzzle or perhaps some human energy typing in a code that is not machine-readable or some other task (e.g., counting the number of puppies in the picture). This kind of system is limited in its application and is generally used by individuals with a tight control on their mail. This is because the system works well to prove the intentions of, say, a lost college buddy, but it effectively cripples one-to-many communications, such as newsletters, if users are not vigilant with whitelists. When ISPs demand computational proof from various organizations that depend on mass emails, the latter’s messages become collateral damage in the battle against spam.

Another implementation of the pay-to-play idea is so-called email postage. Yahoo and AOL recently announced a postage scheme that allows senders to bypass filtering for less than a penny per message, with a special verification of the message’s accuracy. Variations on this theme range from taxes for the government, optional bonds cashed by recipients for abusive

84. These taxes could be on Internet traffic in general, a bit tax, or a tax per email. It might also be possible to tax purchases made via email, though this would require tracking email to web behavior and subsequent purchasing behavior or would depend on unreliable self-reporting. See S. Con. Res. 52, 106th Cong. (1999) (rejecting the 1999 United Nations Human Development Report’s proposed global bit tax); Bambauer, supra note 9, at 167 (describing a possible “spam tax” on purchases from spam emails). See also William F. Fox & Matthew N. Murray, The Sales Tax and Electronic Commerce: So What’s New?, 50 NAT’L TAX J. 573 (1997) for a remarkably thorough discussion of internet sales taxes.
mail, or payments to recipients for their trouble and cost. A payment system might require postage from unknown senders, but none from whitelisted members. This kind of penalty postage would act like payments to pollute, without requiring government intervention. It would offset the cost of spam and focus spam efforts on the most valuable kinds of spam, but it would disadvantage non-profit newsletters as well as senders in poor countries.

In fact, and to date, none of these systems has been wholly successful. A filter will work for a while, until some clever spammer pokecs a hole in it. Blacklists are alternately underinclusive or overinclusive, and never quite fast enough. Vigilante attacks are just not big enough. There is no question that the market’s success in blocking spam has raised costs for spammers, but not sufficiently. Technical hurdles have created an escalating, expensive arms race.

B. Early Legal Solutions

In the 1990s, ISPs grew frustrated at technology’s inability to stop spammers. Though filters were improving, ISPs resented continually being the target of the same set of rogue spammers. With no laws specifically addressing spam, ISPs turned to those laws that did exist, and in the late 1990s, civil and criminal lawsuits brought on a variety of legal theories against spammers peaked. With AOL leading the way, ISPs claimed fraud related to computers, unauthorized access and destruction of stored communications, trademark infringement, and falsification of origin and description. ISPs often won judgments and injunctions. These lawsuits against spammers were complicated, incorporating multiple theories of common law, state law, and federal law.

The landmark case of Compuserve v. Cyber Promotions addressed just such a barrage of legal claims against a spammer, including a novel claim just short

85. This system is essentially the Bonded Sender approach described supra notes 78-79 and accompanying text, but the bonds are cashed by recipients instead of a third party.
88. Bambauer, supra note 9, at 164.
89. Cohn & Newitz, supra note 81, at 8-9.
90. SAMORISKI, supra note 57, at 122.
91. Id.
92. Id.
93. Id. at 124.
of conversion: trespass to chattels. After repeated requests to stop, the defendant spammer had continued to send large volumes of mail and had been fairly successful at circumventing CompuServe's technical blocking measures. The court ruled that email transmission caused sufficient damage to the servers to make the activity illegal trespass to property, and it granted an injunction against further mailing. This decision was a leap far out of the realm of existing statutory or case law. Though a number of victories subsequently relied on CompuServe, and this doctrine seemed promising for ISPs, it did not last.

Intel Corp. v. Hamidi solidly crushed the theory of trespass to chattels for spam. Kourosh Hamidi, an ex-Intel employee, used a list of Intel employee email addresses to send up to 35,000 employees a targeted set of six messages denouncing Intel; he offered and honored opt-outs, and his impact on the Intel servers was negligible. The court ruled that the damage to the servers and Intel's interests in its network were insufficient to support a trespass to chattels claim. This meant that only the most aggressive spammers causing actual damage to networks were committing trespass to chattels.

Other spam cases were based on the law of fraud. Before the passage of federal law criminalizing some types of email, the FTC had pursued several egregious cases of fraud using email. By 2002, the FTC had settled four criminal cases using existing fraud doctrine. By 2004, the FTC had brought some fifty-three cases directed at emailers, all of which depended on existing fraud law. EarthLink also had great legal success against spammers who used accounts with stolen credit cards and phishing. It won a $25 million

---

97. Fisher, supra note 33, at 386-87 (suggesting these suits would become "more prevalent" after IMS and LCGM). This kind of trespass is still accepted for unauthorized access to websites. See Ebay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058 (N.D. Cal. 2000) (ruling unauthorized website access by a competitor's program was trespass); Daniel Kearney, Network Effects and the Emerging Doctrine of Cybertrespass, 23 YALE L. & POL'Y REV. 313 (2005).
98. 71 P.3d 296 (Cal. 2003).
99. Id. at 300-01.
Opting Out of Spam

Kentucky judgment and an over $16 million New York judgment. However, executing those judgments turned out to be even harder than investigating the claims; two years later, EarthLink had not collected on either judgment. The results of Microsoft’s legal efforts were similar. It won six default judgments, one summary judgment, and settled four claims, while one case was dismissed. The summary judgment was for $4 million against Daniel Khoshnood who sent millions of emails claiming to be Microsoft. Microsoft did collect some $500,000 in settlements, but while it won around $54 million in damages, it collected very little of that figure. To this day, Daniel Khoshnood remains on the list of the top 200 spammers.

Using exiting copyright law, Habeas, Inc. devised a clever legal innovation depending on existing email metadata, the “Habeas haiku.” Since the haiku was protected by copyright and other intellectual property law, Habeas controlled who was licensed to use it in header data and planned to sue forgers. Habeas had hoped that this system would act like a whitelist, in effect buying delivery of legitimate mail. Habeas did enforce its mark in several lawsuits, proudly winning a $100,000 judgment, but even its dedicated lawyering was not enough. By the end of 2003, the presence of the Habeas haiku was statistically more likely to indicate spam than a wanted message.

By 2003 then, the law was doing little to stop spam. With only a handful of judgments actually executed and only a handful of prosecutions seemingly reserved for the worst offenders, the legal risk for spammers was still virtually nil. Spam expert John Levine noted that after a $1 billion judgment won under Iowa state law, a $10,000 settlement would have been a better deterrent, in that spammers “would realize somebody might actually come and get that kind of money.” That case provides an apt summary of the state of the law before 2003.

---

108. Sprague, supra note 53.
federal legislation; plaintiffs lawyers hoped to be able to at least collect enough to cover their costs.

III. CURRENT LEGAL SOLUTIONS

Federal spam law has radically changed the landscape of spam prevention. While the law disappointed many who believed it was too weak and too narrow, the law has effectively targeted the worst kinds of spammers. It is also the best enforced spam law in the world, with the most success at compensating ISPs for spamming costs and shutting down abusive spamming operations.

A. CAN-SPAM: Focusing on the Negative

Federal spam legislation was first introduced in 1999,¹¹⁴ and Congress considered some fourteen spam bills over several years.¹¹⁵ The bill that finally passed had twenty-two co-sponsors in the Senate¹¹⁶ and passed with a unanimous Senate vote of ninety-seven to zero.¹¹⁷ With this decisive action, Congress attempted with national legislation to settle inconsistent state law and reduce the volume of spam. Shortly before, California had passed laws raising the possible fine for spamming to $1 million.¹¹⁸ Stakes and confusion were high for anyone sending email since email addresses have uncertain and even mobile jurisdiction; a federal law was sorely needed and perhaps the only chance for compliance.¹¹⁹ The Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM) went into effect on January 1, 2004.

CAN-SPAM’s most important provision is its prohibition of “materially false or misleading” header information and subject lines.¹²⁰ Before CAN-SPAM, information falsification was not illegal, and fifty-six percent of spam fell outside federal definitions of fraudulent mail.¹²¹ The practices that were (and still are) the modi operandi of spammers were not illegal until CAN-

¹¹⁸. McNair, supra note 26.
¹¹⁹. Tom Spring, Spam Wars Rage, PC WORLD, Apr. 2004, at 24-25.
Opting Out of Spam

SPAM. Unsolicited commercial email now must contain a return address and a functioning website or email address to process opt-outs for thirty days after receipt. Following an opt-out, a sender must not send mail after ten days, and may not transfer the address to another sender. Violations of these requirements by using automated email address generation or collecting addresses from public spaces are aggravated offenses subject to increased punishments.

CAN-SPAM provides three means of enforcement. First, the FTC is authorized to pursue fraudulent activity and enforce other provisions, while other federal agencies have jurisdiction over special groups of senders, such as banks. Second, state attorneys general can bring civil lawsuits for injunctions and damages, which are trebled for willful or aggravated offenses. Finally, ISPs themselves can sue for injunctions and damages, also subject to trebling. Critics claimed that, without the right to sue, individuals were dependent on the FTC to pursue their claims. However, individuals may also rely on ISPs and state attorneys general to defend their rights. If these routes are inadequate, users can also still use existing state and federal law for private lawsuits. (Additionally, in theory, a user could set up his own mail server, making him into an ISP with standing under CAN-SPAM.)

It is worth noting that a private right of action could however become valuable against a user’s own ISP, which could spam its recipients. Spam from an ISP or its partners, such as Hotmail’s Bonded Sender messages, is just a term of service under CAN-SPAM, left entirely out of the law’s scope. This problem forces a value decision. Is CAN-SPAM trying to reduce spam to a manageable level, or is it expressing a right to refuse information? CAN-SPAM expresses both goals, but both are alienable: the former by not opting out of mailings, the latter by affirming ISP filtering policies. ISP spamming has been limited and not empirically problematic because of competition in the market, which is probably why Congress failed to carve out an exception for

122. See id. § 7704(a)(3).
123. See id. § 7704(a)(4).
124. See id. § 7705(b).
125. See id. § 7706(a).
126. See id. § 7706(c)-(d).
127. See id. § 7706(g).
128. See id. § 7706(f).
129. See id. § 7706(f)(3)(C).
130. Matthew Yglesias, Friends of Spam, AM. PROSPECT, Jan. 2004, at 8 (stating that consumers were “blissfully unaware of how close they came to spam-free serenity before federal legislators rode to the rescue”).
this action. If ISPs become problematic spammers, an amendment to allow
individual or class action lawsuits against ISPs is conceivable, but fierce
competition for spam-wary customers will likely solve this problem faster than
legislation.

Finally, Senator John McCain added a special enforcement mechanism for
CAN-SPAM that holds businesses responsible for their ads\textsuperscript{136} and allows the
FTC to “follow the money.”\textsuperscript{137} This means businesses cannot avoid liability by
delegranting responsibility for advertising\textsuperscript{138} or hiring overseas marketing
companies.\textsuperscript{139} This provision forces responsible advertising practices and also
creates an affirmative burden on businesses to investigate the services their
advertisers provide.\textsuperscript{140}

CAN-SPAM explicitly preempted state-specific regulations of content or
labeling requirements for commercial email.\textsuperscript{141} Labeling has been a
controversial issue and merits some discussion. In the years before CAN-
SPAM, the FTC had found that labeling was virtually non-existent even though
existing laws required it.\textsuperscript{142} By 2003, several states required labeling: For
example, Indiana required “ADV: ADLT” on sexually explicit commercial e-
mails,\textsuperscript{143} while Kansas required “ADV” on all commercial mail.\textsuperscript{144} These
requirements were filling theoretically compliant subject lines quickly.

CAN-SPAM pared labeling requirements down to one set, delegating
labeling to the FTC for rulemaking.\textsuperscript{145} The FTC now requires a label on
“sexually oriented” material. This label, “SEXUALLY-EXPLICIT,” must be
written verbatim with no deceptive encoding to trick filters.\textsuperscript{146} Harsh penalties
for unlabeled spam should deter further unlabeled adult spam, which would
help parents and adults better filter email,\textsuperscript{147} and this particular label might
actually attract its target audience’s attention. Then again, this label might just
hurt the senders who actually comply with the law.

The FTC rejected a general spam label in a June 2005 advisory report to

\textsuperscript{136} Id. § 7705(b) (West Supp. 2005).
for Email Advertising, COMPUTER & INTERNET L., Feb. 2004, at 1, 3.
\textsuperscript{139} Johnson, supra note 69, at 8-9.
\textsuperscript{140} Id. at 8. The McCain Amendment has yet to be enforced. This could be because it is quite
complicated, or it could be that enforcement efforts are already at capacity.
\textsuperscript{141} S. REP. No. 108-102, at 21 (2003).
\textsuperscript{142} FTC FRAUD REPORT, supra note 34, at 15.
\textsuperscript{143} IND. CODE § 24-5-22-8 (2) (West Supp. 2005).
\textsuperscript{144} KAN. STAT. ANN. § 50-6107(c)(1)(C) (2003).
\textsuperscript{147} Reduction in Distribution of Spam Act of 2003: Hearing on H.R. 2214 Before the H. Comm.
United States).
Opting Out of Spam

Congress. The FTC felt a more generic label, such as ADV, would hurt businesses actually trying to comply by labeling them as advertisers for painless filtering as well as blocking their subject line speech. Critics argue that compliance with labeling requirements effectively increases costs for spammers. For example, advocates claim that if ninety percent of spammers comply, their costs will increase by nine times, but this ignores powerful filters. Spammers who comply will likely have their costs increase by much more, since obediently labeled mail will be instantly blocked by filters. Spammers who do not comply have no cost change at all. The concept of helpful labeling depends on the false assumption that the least valuable spammers want to comply and also a misunderstanding of the effectiveness of modern filtering.

Assume for a moment that filters are already ninety percent effective, and a random ninety percent of spammers comply with an ADV label. For a spam-intolerant ISP, this would lower costs for filtering, and would enable the ISP to filter the ninety percent that is labeled plus ninety percent of the remaining mail—or ninety-nine percent total. However, compliance is not random, and the spammers who complied likely also sent the mail that was most valuable and legitimate. Valuable, non-fraudulent mail would be blocked because of its ADV label. Thus, law-abiding mailers will give up altogether, only rogue unlabeled spam will exist, the costs of filtering will increase again, and the most valuable speech will have been lost. Labeling certainly lowers costs to recipients, but raises them for valuable mailers.

The most outspoken advocate of labels is Professor Lawrence Lessig of Stanford Law School. He has proposed an ADV labeling scheme plus a small bounty for cyber-sleuths, and was so confident about this system that he promised to quit his job if the system was codified and did not work. Representative Lofgren and Senator Corzine introduced Lessig's plan—which would have set statutory damages of up to $10 per email and awarded the reporter twenty percent of the FTC's fine—but the legislation failed. Lofgren and Corzine did get a provision into CAN-SPAM calling for an investigation

152. Filters are generally more effective than this, but as implemented by ISPs, their results are secret.
into a policy similar to that in their bill, and the FTC was given nine months to make a report about a possible twenty percent bounty.

Ultimately, that report did not support Lessig's view. The FTC's technical expert on cybersleuthing concluded that individuals with no insider information would have no valuable information about spammers' identities. The FTC's legal expert further concluded that of the three kinds of information about spam—forwarded emails, individual sleuthing based on those emails, and insider information—only insider information was valuable and risky enough to warrant bounties. The first kind of information, questionable email, is gathered in bulk from the FTC's email collection at spam@uce.gov, its spam database, and the FTC's generic complaint form. Individual sleuthing contributions were seen as not sufficiently valuable, if valuable at all, to reward. The FTC recommended rewards for insider information only, ranging from $100,000 to $250,000. This insider bounty has yet to be awarded, but it likely does increase risk for secretive spam operations. Whereas legitimate marketers feared a small bounty for anyone dragging them into court every day, a bounty for insiders raises risks only for email operations with something to hide, which is a more efficient outcome.

To be sure, CAN-SPAM did not please everyone. Spam legislation always balances speech and privacy, freedom and costs. CAN-SPAM was criticized for being too weak to decrease the amount of spam within a month, under-

---

157. Dan Boneh, The Difficulties of Tracing Spam Email, at 10-11 (Sept. 9, 2004), http://www.ftc.gov/reports/rewardsys/expertrpt_boneh.pdf (concluding that without inside information, "all but the most incompetent spammers can avoid being identified by [individual] cybersleuths").
159. The FTC receives about 300,000 samples forwarded to this address by users per day. Fed. Trade Comm'n, Spam Homepage, http://www.ftc.gov/bcp/conline/edcams/spam/report.html (last visited Apr. 18, 2006).
Opting Out of Spam

enforced, too vague, too harsh, and not harsh enough. However, CAN-SPAM has made great progress toward actually suing and collecting damages from the worst spammers.

B. Enforcing CAN-SPAM

CAN-SPAM targets fraudulent mail, and mail sent to recipients who have expressed lack of utility from that mail, that is, users who have opted out. Enforcement started quickly and continues, bankrupting and imprisoning the most egregious spammers. It has been the most effective spam law in the world.

First, CAN-SPAM has been used to protect published email addresses via "honeypot" accounts. While CAN-SPAM does not directly forbid scanning the Internet for public email addresses (harvesting), if a violator of another section used harvested addresses, the violation is aggravated and subject to harsher penalties. Mail providers have been using honeypot accounts, fictional email accounts, to monitor spamming activity, for quite some time. Brightmail operates some two million of these accounts in twenty countries to improve its filtering and blocking. Honeypot accounts are generally published in public places, such as a website or a message board, and then collected by specialized programs called spam bots. These programs quickly run through webpages looking for email addresses to harvest. Collectors then sell the addresses to spamming operations.

A Chicago spam consulting firm has started an ambitious project called Project Honey Pot to track harvesters and pressure spam accomplices. The service is a webpage linked invisibly and thus only for robots; the page issues an email address visible only by the robot and unique to the IP address of the visiting robot. When mail is sent to that address, both the sender and associated sending servers can be tied to the harvesting IP addresses. To date, Project Honey Pot has identified almost one thousand harvesters; some of these

172. Leung, supra note 150, at 6.
IP addresses were not previously affiliated with spamming operations. 174

Administrators could do a few things with this kind of data. They could block the harvesters’ IP addresses or notify ISPs about the behavior of their subscribers. Better yet, they could notify companies using the services of the spammers that their address lists are harvested. This warning, in addition to the McCain amendment to CAN-SPAM, should cause legitimate companies to question their direct advertiser and to change to more legitimate (and expensive) address-gathering techniques. Thus, clever use of CAN-SPAM plans to cut off spam’s supply lines—the lists.

Using CAN-SPAM, ISPs driven by economic and reputational incentives to legal action have filed hundreds of lawsuits. 175 Many of these lawsuits have already settled, 176 others are pending trial, 177 and yet others have resulted in large default judgments. 178 State attorneys general have also sued using CAN-SPAM. 179 Those who predicted no enforcement have been proved sorely wrong. 180 These lawsuits target fraudulent senders and often incorporate other fraud and intellectual property claims. CAN-SPAM has allowed ISPs more effectively to pursue spammers with a federal civil right of action they have embraced with gusto. 181 AOL recently won $5.3 million in summary judgment from a former spammer, Christopher William Smith. 182 A notoriously defiant spamming operation, Scott Richter’s Optinrealbig, recently declared bankruptcy in anticipation of a Microsoft lawsuit. 183 In the words of Richter’s


178. Devon Gillespie’s default judgment was $1.4 million. Zeller, supra note 22.


180. Scott Bradner, Enforcing the Permission-To-Spam Act, NETWORK WORLD, Apr. 26, 2004, at 38 (“It is likely to be the end of time before we see any effective enforcement.”).


183. Griffin, supra note 177.
father and legal counsel, "Optin is profitable but for these lawsuits."184 The final party with civil standing is the FTC, which has also filed some twenty lawsuits.185 Finally, criminal enforcement of CAN-SPAM has begun in earnest. So far, the Department of Justice has started four prosecutions, all resulting in guilty pleas, and more investigations are underway.186

CAN-SPAM’s enforcement compares very favorably with regimes abroad. For one, government action is only part of the larger United States strategy to deal with spam, unlike in Australia or the U.K., where enforcement is primarily by a government agency. The Australian Communications and Media Authority has exclusive authority to enforce its Spam Act, and has focused on issuing a deluge of formal warnings.187 The ACMA has now asked 350 companies to stop spamming, fined a few, and charged exactly one.188

CAN-SPAM’s enforcement has been more effective even though it is theoretically more difficult to implement than the blanket prohibitions on unsolicited mail coupled with opt-in regimes imposed by the EU189 and Australia.190 Though the EU requires an opt-in for all mail, the sparse enforcement in Europe has focused only on fraudulent mail.191 Appalled that mailers could send an initial message with no penalty, critics in the EU and elsewhere criticized CAN-SPAM’s opt-out regime.192 In practice though, the opt-in distinction has meant nothing, since even the strictest laws, such as the Italian laws which include large fines and prison time,193 have gone un-enforced.

C. Other Laws Still in Effect

Critics of CAN-SPAM also resented its preemption of stronger state

184. Id.
185. FTC UPDATE, supra note 179, at 1.
186. Id. at A-2.
190. Spam Act, 2003 (Austl.).
192. The Spamhaus Project, supra note 169.
laws.\textsuperscript{194} For its part, Congress assessed the preemption as "minimal" since CAN-SPAM does not preempt most of the laws previously used against spammers.\textsuperscript{195} In particular, its preemption excludes laws related to "fraud or computer crime,"\textsuperscript{196} which many states now have.\textsuperscript{197} In other words, most state spam laws are still in effect.

For example, Virginia's harsh spam laws were the most actively enforced before CAN-SPAM; Virginia had used its criminal spam laws and its long-arm jurisdiction twice.\textsuperscript{198} This kind of law against fraudulent spammers has been held not to be a regulation of interstate commerce, and states still have jurisdiction over fraudulent email.\textsuperscript{199} Virginia recently extradited a spammer from North Carolina, Jeremy Jaynes, who had amassed a $24 million fortune, and was sentenced to nine years in prison on a fraud conviction.\textsuperscript{200} Virginia's tough spam laws were not preempted by CAN-SPAM. Similar laws in other states\textsuperscript{201} have also been upheld, and so states continue the battle against fraudulent mail. Before CAN-SPAM, only one state lawsuit had used generic state spam laws not based on fraud,\textsuperscript{202} so state laws maintain at least their pre-CAN-SPAM impact. Lawsuits using traditional intellectual property and unfair competition claims also march on.\textsuperscript{203} CAN-SPAM has thus taken very little ground from existing law.

On the other hand, CAN-SPAM has done an unparalleled job targeting spammers with the worst mailing practices and putting them out of business. CAN-SPAM's prohibitions on fraud and trickery cover the worst kinds of spam. Dedicated ISPs and law enforcement are pursuing these offenders, armed with CAN-SPAM's provisions. But there is a gentler kind of spam from more law-abiding senders, which I argue CAN-SPAM handled inadequately, and to which this Note now turns.

\begin{itemize}
\item[195.] S. REP. NO. 108-102, at 10 (2003).
\item[197.] The explanation of this exception is that liability results from "sending of the e-mail plus some other action, such as violation of contractual terms, acts of fraud or deception in connection with initiating the transmission of the e-mail, or inclusion of fraudulent content in the e-mail message." S. REP. NO. 107-318, at 13-14 (2002).
\item[199.] Ferguson v. Friendfinders, Inc., 115 Cal. Rptr. 2d 258 (2002); see also Verizon, Inc. v. Ralsky, 203 F. Supp. 2d 601 (E.D. Va. 2002) (ruling that Virginia has long-arm jurisdiction over spammers sending mail through Virginia networks); Tricia Bishop, \textit{Judge Affirms Spam Suits Md. Appellate Ruling Upholds Tool Against Unsolicited E-Mail}, BALTIMORE SUN, Jan. 27, 2006, at 1A (chronicling a similar result in Maryland litigation).
\item[201.] See, e.g., State v. Heckel, 93 P.3d 189 (Wash. App. 2004).
\item[203.] Heather Won Tesoriero, \textit{Microsoft Joins Pfizer To Fight "Viagra" Spam}, WALL ST. J., Feb. 11, 2005, at B1 (reporting Viagra violations via ICANN, as well as other Microsoft efforts).
\end{itemize}
IV. COMPLETING THE PICTURE: DO-NOT-SPAM LISTS

Inboxes and email addresses have never been protected by privacy laws or property law. Users have no right to sue, and have only an ex post remedy for unwanted mail. CAN-SPAM has protected inboxes ex ante from the worst kinds of spam, but ignored the rights of users to refuse unwanted advertising, despite the success of Junk Fax and the Do-Not-Call Registry in analogous media. This Part addresses this deficiency of CAN-SPAM, and proposes a domain-level Do-Not-Spam Registry.

A. Mail, Fax, and Telemarketing

It is helpful to start by looking at opt-out protections for other kinds of unsolicited commercial speech. To opt out of most advertising, such as radio and television, a consumer can simply not pursue the communication. Other kinds of Internet advertising, such as websites and banners, are similarly "pull" advertising which users can avoid by not seeking it out. Regulations about more invasive "push" media depend on the characteristics of the medium involved, namely invasiveness and cost.

In the mail context, there are two ways for postal customers to opt out of advertising mailings by notifying the post office. The first is to notify the post office that a recipient or her children do not wish to receive "sexually oriented" advertising. This material is defined broadly in the statute. In practice, the post office also applies this opt-out to violence-inciting materials and some types of mail relating to lotteries. A consumer can also opt out of mail sent by any sender. The Postal Service will issue an order to an offending mailer forbidding any further mails to the particular addressee, regardless of content. The statute intentionally allows a subjective standard, applied at a recipient's discretion; the Supreme Court affirmed this user-based standard with no review by the Postal Service in a 1970 case concerning birth control advertisements. A recipient can exercise both rights by filing Postal Service...
Form 1500.\textsuperscript{213}

In 1991, Congress implemented a complete ban on unsolicited commercial faxes, so-called Junk Faxes.\textsuperscript{214} This law is enforced, among other ways, with a private right of action to receive $500 damages for such faxes\textsuperscript{215} (a lucrative hobby for the litigious and annoyed). It is possible to opt back in by soliciting the faxes, which is an affirmative defense for the sender.\textsuperscript{216}

Automated telemarketing using pre-recorded or artificial messages is expressly illegal,\textsuperscript{217} as is automated dialing of cellular telephones.\textsuperscript{218} Other telemarketing is now governed by the Do-Not-Call Registry, which is an opt-out system.\textsuperscript{219} The Do-Not-Call Registry did face well-publicized legal obstacles. After the logistics were in place, a federal district court ruled the FTC did not have the authority to establish the Do-Not-Call Registry.\textsuperscript{220} Congress reacted within a week, codifying the FTC’s authority.\textsuperscript{221} In the words of Senator Charles Schumer, “[f]ifty million people can’t be all wrong.”\textsuperscript{222}

After the statute was passed, another district court ruled the list was unconstitutional because of its treatment of non-commercial speech.\textsuperscript{223} A few days later, the Tenth Circuit stayed the injunction on the list, and four months later, the Tenth Circuit upheld the constitutionality of the list.\textsuperscript{224} The Tenth Circuit reasoned that the list was constitutional because it (1) restricted only commercial speech; (2) targeted privacy-invading speech; (3) was an opt-out system; and (4) furthered a government interest in preventing abusive telemarketing and invasion of privacy.\textsuperscript{225} The Tenth Circuit’s ruling relied on the Supreme Court’s support for opting out of physical mailings for the similar system in telemarketing.\textsuperscript{226}

\textsuperscript{213} U.S. Postal Serv., Application for Listing and/or Prohibitory Order, Postal Service Form 1500 (July 2005), http://www.usps.com/forms_pdf/ps1500.pdf.


\textsuperscript{215} Id. § 227(b)(3) (2000).

\textsuperscript{216} S. REP. No. 102-177, at 11 (1991).


\textsuperscript{218} See id. § 227(b)(1)(A)(iii).


\textsuperscript{222} Caroline E. Mayer, Call List is Again Blocked in Court: Order Comes After Congress Votes To Protect Registry, WASH. POST, Sept. 26, 2003, at A1.

\textsuperscript{223} Mainstream Mkting. Servs. Inc. v. FTC, 283 F. Supp. 2d 1151, 1168 (D. Colo. 2003), stay denied by 284 F. Supp. 2d 1266 (D. Colo. 2003), stay granted by 345 F.3d 850 (10th Cir. 2003), rev’d, 358 F.3d 1228 (10th Cir. 2004).

\textsuperscript{224} 345 F.3d 850; 358 F.3d 1228.

\textsuperscript{225} 358 F.3d at 1233.

\textsuperscript{226} “We therefore categorically reject the argument that a vendor has a right under the Constitution or otherwise to send unwanted material into the home of another. If this prohibition operates to impede the flow of even valid ideas, the answer is that no one has a right to press even ‘good’ ideas on an unwilling recipient. That we are often ‘captives’ outside the sanctuary of the home
Opting Out of Spam

Mail, telephony, and fax, unlike email, are one-to-one communications. These communications are differentiated in policy decisions by invasiveness and cost. “Push” advertising to the most expensive recipient communications, cellular phones and faxes, is flatly prohibited. Automated telemarketing’s very low marginal cost and high invasiveness also warranted a blanket ban. However, for communications with higher barriers to entry, such as telemarketing and mail, the law allows recipients to opt out of communications rather than imposing a flat ban. Mail also has a special preemptive opt-out for sexually oriented materials, despite the high cost of entry.

How does email compare to these other media? A family interrupted during dinner can hang up on a telemarketer, but the harm is already done. The same seems to be true for an email recipient of, for example, an unwanted pornographic commercial message. Most people do not need to see this mail to know they do not want it, especially in categories like pornography and prescription drugs. Also, users do not want to opt out of mail as CAN-SPAM demands, fearing that confirming their address will cause even more unwanted mail. Consumers need a better way to opt out, and it should be before the damage is done.

Indeed, surveying this landscape of varying approaches, only email allows commercial speakers to claim an affirmative right to send that first message despite attempts to opt out ex ante. CAN-SPAM only prohibits transmission after a recipient opts out by using a specific sender’s link in a received communication. This entitlement is misplaced. Even compared to the most reputable and expensive emailing campaign, physical mail is more than five times the cost of email. Illogically, the medium with the least marginal cost, email, has an affirmative right to that first communication, whereas media with significantly higher barriers, such as telemarketing, must respect recipients’ ex ante wishes. Commercial speech should be less important than a consumer’s expressed desire to not receive the push communications.

Further, email imposes external costs physical mail could never tolerate. The most notorious spammers claim response rates from only one-quarter percent to two percent, while the industry representative Direct Marketing

and subject to objectionable speech and other sound does not mean we must be captives everywhere.” Rowan v. U.S. Post Office Dep’t, 397 U.S. 728, 738 (1970).

227. DMA RATE REPORT, supra note 16, at 9 (“It is very important to keep in mind that the highest response rate does not always translate into the highest return on investment (ROI) and vice versa.”).


229. FTC UPDATE, supra note 179, at A-13 to A-14.


231. See Baker, supra note 43.

232. Wendland, supra note 17.

233. The “Cajun Spammer,” Ron Scelson, also a ROSKO known spammer, testified before Congress as the “most disliked person in this entire room” that his company has a one to two percent...
Association (DMA) claims a 1.12% response rate.\(^{234}\) Email processing companies estimate a 0.00036% overall response rate.\(^{235}\) Even when not sending to randomly generated addresses, spam firms send to vast databases, sometimes larger than AOL's membership\(^{236}\) (in less upright cases, the AOL membership list itself).\(^{237}\) In the best case scenario of a non-fraudulent, non-offensive product with a high response rate, the sender, two percent of the recipients, and those who valued reading the mail, have directly benefited. The majority of recipients will have neutral to negative utility from annoyance, wasted time, and processing costs. Even under this optimistic view of spam, the vast majority of recipients have incurred unwanted costs. This group is now a strong majority; sixty-five percent of users find spam "very annoying," and seventy-four percent favor making it illegal.\(^{238}\) Even for legitimate, non-offensive products, some users are so irritated by spam that they even send offensive items to spammer's residences.\(^{239}\) This leaves one group always benefiting from spam: the senders. And they are an isolated group, since one advocacy organization claims that over eighty percent of spam can be traced to about 200 known spam operations.\(^{240}\)

Given that analysis, a Do-Not-Spam registry would clearly find public support. Certainly, the Do-Not-Call Registry is wildly popular. In one poll, eighty-three percent of respondents thought the registry was a good idea, and even sixty-six percent of those who did not plan to sign up considered it a good idea.\(^{241}\) The Do-Not-Spam registry is also a popular idea. Shortly after the Do-Not-Call List was implemented in 2003, eighty-three percent of Americans indicated that they would sign up for a similar FTC Do-Not-Spam list.\(^{242}\)

B. Problems With Do-Not-Spam Lists

Drawing on the immense popularity and success of the Do-Not-Call list,

---

\(^{234}\) DMA RATE REPORT, supra note 16, at 12.


\(^{239}\) Madigan, supra note 15.

\(^{240}\) The Spamhaus Project, supra note 109.


Opting Out of Spam

CAN-SPAM delegated a decision about a similar Do-Not-Email list to the FTC.243 This Note refers to this list as a Do-Not-Spam list because it is limited to unsolicited commercial email. The Do-Not-Call list is an opt-out regime, like CAN-SPAM itself.244 A Do-Not-Spam registry would act similarly in principle, making that opt-out more methodical and making it an ex ante decision. The FTC was empowered to start a list like the Do-Not-Call List a few months after CAN-SPAM was passed,245 and conducted a thorough investigation with the input of eighty experts and data from the largest ISPs.246 But it ultimately rejected such a list. In its CAN-SPAM report to Congress, the FTC emphasized that the problem was the lack of an authentication system for email.247 The report also outlines a host of technical, legal, and policy problems with the list; it is an unambiguous rejection of the proposal.248

Experts agreed on the basic problems with the list: the list would be traded and used against those who opted out; it would be technically impossible to "scrub" the lists and filter anonymously;249 protections for third party, or trusted, mailers would be a disaster to implement;250 there would be no privacy for those who signed up, and for those who did sign up, their spam problems would increase. The FTC highlighted all of these concerns in explaining why a list of email addresses was technically problematic, if not impossible.251

However, the push for Do-Not-Spam Lists continued in states, with several states using children's protective registries to limit emailing.252 Michigan implemented a children's registry in November 2004, while Utah's went into effect in July 2005.253 These lists are expensive to comply with, and even


247. Id.


251. FTC REGISTRY REPORT, supra note 248, at 21-34.

252. See Prince, supra note 248.

companies who do not actually do business in these states must pay for the lists because their messages may enter the jurisdiction. Some experts estimate this acts like a tax for bulk mailers at seven one-hundredths of a cent per address.\textsuperscript{254} Further, the same security concerns arise with the children’s list; spammers can easily triangulate for live addresses.\textsuperscript{255} And these laws are already under attack: For example, an adult-entertainment trade group has gathered many free speech advocates to challenge the Utah law.\textsuperscript{256} Even if they are constitutional, such lists are expensive to comply with and insecure. But these laws do manifest a powerful desire for control over inboxes, especially when it comes to sexually oriented material. This goal could be achieved with a more general Do-Not-Spam List.

C. Domain Level Do-Not-Spam Lists

There was no policy or statutory reason that the Do-Not-Spam list had to mirror the Do-Not-Call List’s structure of live addresses, such as johnsmith@hotmail.com. It could have been a list of domains, for example @hotmail.com addresses or @yale.edu addresses.\textsuperscript{257} The domain as a whole could opt out of spam, or in a more complicated implementation opt out by category of spam, such as pornographic spam or prescription drug spam. For example, Hotmail could opt out of all spam, all pornographic spam, or some combination.\textsuperscript{258} Subdomains, such as kids@hotmail.com, might also have additional restrictions.\textsuperscript{259}

Because A Do-Not-Spam List of domains (aol.com, hotmail.com, yale.edu, law.yale.edu) is much less valuable to spammers than a list of live addresses (mary.smith@hotmail.com, rebecca.bolin@yale.edu), this system would allow users to declare ex ante their preferences while maintaining their privacy.\textsuperscript{260}

\begin{itemize}
  \item \textsuperscript{254} Ed Felten, Michigan Email Registry as a Tax on Bulk Emailer, FREEDOM TO TINKER, July 13, 2005, http://www.freedom-to-tinker.com/?m=200507 (July 13, 2005).
  \item \textsuperscript{255} Id.
  \item \textsuperscript{256} Kesmodel, supra note 253.
  \item \textsuperscript{257} The "\texttt{.com}" or "\texttt{.edu}" is the top level domain, "\texttt{hotmail}" or "\texttt{Yale}" is the second level domain. Here, I use "\textit{domain}" to refer to what is usually a second-level domain, and I use "\textit{subdomain}" to refer to what is usually a third-level domain, such as law.yale.edu. In some cases, a second-level domain acts more like a top-level domain, such as ".co.uk." The discussion of administering domains is beyond the scope of this Note, but the FTC does have authority and competence to differentiate this kind of second-level domain. Many Americans own domains within foreign top-level domains, such as ".tv" or ".md," and many foreign parties own American-administered domain. The complication of territorial domains and online jurisdiction is beyond the scope of this Note. I will assume all registrants are in the United States using U.S. top-level domains.
  \item \textsuperscript{258} In this case, Hotmail is the agent of its customers, and should not be subject to the restrictions of the top-level domain, "\texttt{.com}" in this case. The FTC has the authority to handle this distinction and should be able to restrict registration to second-level domains, or in some cases even third- or fourth-level domains.
  \item \textsuperscript{259} The Do-Not-Spam Registry should not function as an opt-out list and an opt-in list. Subdomains should be able to add but not remove restrictions.
  \item \textsuperscript{260} Reduction in Distribution of Spam Act of 2003: Hearing on H.R. 2214 Before the H. Comm.
\end{itemize}
Opting Out of Spam

People want to opt out of messages they dislike; sixty-four percent of recipients would trust marketers more if they could control the kinds of communication they received. The most inexpensive way to do this is by letting domains publish their preferences.

Such a domain-level Do-Not-Spam Registry would meet Henry Smith’s critical factor for property right notifications: low information intensity. Smith himself uses telemarketing and spam as examples of communications with high externalized costs and intrusiveness that require better markers of willingness than most rights. Thus a targeted list is sufficiently inexpensive notice, given an invasive medium with high external costs. The Domain Do-Not-Spam Registry is roughly as informationally intensive as the telemarketing list. Do-Not-Call requires requesting the list, and scrubbing a calling list for each phone number. There are now over 100 million U.S. telephone numbers on the registry. Compare this to eighty-six million domains registered worldwide. A central database of the registered domains would thus be on the order of the Do-Not-Call Registry, and completely workable. In addition to the official central database, the information could also be decentralized in domain servers (DNS servers), which already contain routing and other information. In fact, AOL has carried such a notice for years. This system lacks the privacy concerns of the Do-Not-Call Registry, since the Do-Not-Spam Registry could be downloaded at will. As a technical matter, a domain level Do-Not-Spam List would be easy and inexpensive to administer.

A Domain Do-Not-Spam list could be content-specific to commercial email, and it could include subcategories. The most obvious is the “sexually

---

263. Id. at 1137-38, 1142, 1153.
264. Alena Tugend, 2 Years of Dinnertime Quiet, Thanks to the Do-Not-Call Registry, N.Y. TIMES, Nov. 26, 2005, at C5.
265. VERISIGN, THE DOMAIN NAME INDUSTRY BRIEF 2 (2005), http://www.verisign.com/static/036316.pdf. Obviously, including subdomains could raise the number of domains suitable for registration, but the list’s length would remain similar to that of the Do-Not-Call Registry.
267. Id. at 25 (“America On-line and its affiliated companies do not authorize the use of its proprietary computers and computer networks to accept, transmit or distribute unsolicited bulk e-mail sent from the Internet.”)
268. CARL MALAMUD, A NO SOLICITING SIMPLE MAIL TRANSFER PROTOCOL (SMTP) SERVICE EXTENSION (2004), http://rfc3865.x42.com. However, both of these proposals are subject to forgery or malicious changing of the data. As a legal matter, their notice is not verifiable, so a centralized list is the most reliable way to ensure the message is not distorted.
269. But see Zitter, supra note 228, at 2821-22 (arguing that opt-out systems that discriminate by
An "oriented" material category already required to be labeled by the FTC. In fact, this label exactly mirrors the postal service labeling requirements for sexually oriented physical mail advertising, but without the corresponding opt-out list. Other categories are possible also, such as prescription drugs, herbal enhancements, mortgage pitches, and others. Subcategories would increase the informational intensity because advertisers would have to determine which list to use for each product, but would allow more refined consumer choice. For the case of sexually explicit advertising, the list has no added informational intensity as labeling is already required on these messages and the list is inexpensive to process.

This Note does not propose an opt-in system like that in Europe and Australia because this system loses the value of unsolicited speech that many actually do want. Domain opt-out is an inexpensive way to identify users that do not value certain kinds spam while not shutting down the speech entirely, like the Do-Not-Call Registry. CAN-SPAM's opt-out system coupled with a Do-Not-Call system offers the best of all worlds at minimal cost to senders, the easy violation detection of an opt-in regime along with the freedom to receive unrestricted emails of an opt-out regime for those who choose it.

The punishment should be larger than actual damages, but not over-high; the $500 figure for Junk Fax seems like the high upper bound. CAN-SPAM's statutory damages are either $25 or $100 per email. These damages seem reasonable, and could either go to ISPs or to individuals. Like Junk Fax and CAN-SPAM, consent is always an affirmative defense. As an individual cause of action, the Do-Not-Spam Registry starts to look quite a bit like Lessig's small bounties for mislabeled mail—the kind of broad, small, strict liability action he believes will stop spam.

Though a major lobbying group proposed this domain-level implementation exactly, with no class action options, only one of the FTC technical experts, Ed Felten, even mentioned this idea in his report. The FTC dedicated a paltry...
Opting Out of Spam

377 words to this most promising kind of list while rejecting it. Their concerns were not technical, but rather under-explained legal questions. The FTC claimed that the “ineffectiveness of the opt-in regime instituted in the United Kingdom illustrates the inherent weakness of a domain-level Registry without effective domain-level authentication” and that this list would put the “government’s imprimatur on ISPs’ existing anti-spam policies without reducing the scope of spam.” This Note next addresses these concerns and others.

D. Practical Concerns

The Domain Do-Not-Spam List lacks the capacity to deal with the basic enforcement problems that plague spam law. Identity-masking through spoofing, open relays, proxies, and zombies makes spam difficult to trace, and even then it is difficult to get data routed through other countries. Spammers are often untraceable or judgment proof, and the list cannot change that. The list also cannot handle fraudulent or malicious spammers. This Note has argued that CAN-SPAM already deals with this type of mail, and the Do-Not-Spam Registry is targeted at more honest mailers, an admittedly small minority at this time. The list is intended to express a right to refuse unwanted advertising from reputable mailers, and rogue spammers will disregard that in the same way that they disregard other laws. Low compliance and respect for the law does not mean the values it expresses are unimportant. For that first unsolicited message, the Do-Not-Spam List expresses a right, and is a recipient’s only legal defense.

The list itself also cannot handle the problem of users opting back into mail; senders must keep track of that information themselves and use it as an affirmative defense. Recipients can never be forged in SMTP, so the responsibility is always on the sender to ensure that he is sending legal material. And senders are responsible under CAN-SPAM to verify a user’s consent when mailing to a recipient who has opted back in after opting out. Just as in Junk Fax, the sender relies on consent as a legal defense, and as a technical assent to mail despite a previous proscription. The same situation would arise if a user opts in to spamming despite his domain’s preferences. Of course, this can be difficult or impossible to implement given ISP filtering, but from the sender’s perspective, it is known whom he is legally permitted to

277. Id. at 27.
278. FTC UPDATE, supra note 179, at 24.
280. Levine & Shafranovich Interview, supra note 266, at 36.
281. Id. at 27.
Senders also bear the burden of determining the category of their spam, just as they must now determine whether they are sending sexually explicit material.

The FTC cited the experience in the U.K. to demonstrate how ineffective a domain-level list would be. But comparing any opt-out system to the U.K.'s makes little sense. The U.K. is bound by an EC directive that puts a flat ban on unsolicited commercial email, like the United States Junk Fax law, and requires users to opt in to unsolicited mail. Thus, the U.K. is not administering a Do-Not-Spam Registry because, in effect, everyone is already on it. Also, the U.K. implementation of the directive entrusted most enforcement powers to one government agency, the Information Commissioner, and then grossly underfunded it. Indeed, one year later, it had not issued a single fine or charge. And while there is a right of action for individuals to win actual damages, it has been successful only once, settling out of court. A larger penalty or an ISP right might have led to greater private sector enforcement, like ISP enforcement of CAN-SPAM. Further, the Information Commissioner does not even seem to want data about spam emails, as the only way to complain is via a five-page written form that must be physically mailed to the commissioner. Using the U.K. as an empirical example of failure of domain-level opt-out is thus misleading because the U.K. was not operating an opt-out system, has an entirely different enforcement mechanism than CAN-SPAM or a Do-Not-Spam list, and has failed to enforce its own laws.

E. Agency Concerns

As for the FTC's concerns about lending the government's imprimatur to filtering policies, CAN-SPAM was explicitly intended to be a legal codification of best mail practices, as both a technical and business mandate. CAN-SPAM intended to replace industry standards with official, legal standards for anonymizing mail and opt-out procedures, and legally enforceable

---

282. This problem already exists when a user's preference does not match the ISP filter's. Hotmail users, for example, cannot opt in to mail that is deleted by the filter.


284. There were warnings before the anti-spam legislation that the Information Commissioner did not have the resources to enforce the law. Graeme Wearden, Information Commissioner "Low on Power" for Spam Fight, ZDNET U.K., Oct. 7, 2003, http://news.zdnet.co.uk/intemet/ecommerce/0,39020372,39116979,00.htm.


288. FTC REGISTRY REPORT, supra note 248, at 34.

289. FTC UPDATE, supra note 179, at 1-2.
spam preferences are simply the next logical step.

ISPs are already deciding what speech subscribers receive, since they delete a large majority of mail before users even see it. This practice is explicitly authorized by federal law; indeed it must be for mail systems to work. ISPs are not common carriers, since they set the rules of what kind of mail they will tolerate. In fact, most ISPs have already expressed the values of the Do-Not-Spam Registry in their terms of service. Some domains are even opting into private domain level Do-Not-Spam Registry, which claims legal authority.

In a trivial sense, a domain that signed up for the Do-Not-Spam List would be setting the values for the user, so the user would not always be able to get exactly what she wants. This might have more symbolic meaning than an aggressive filter, but it has little practical impact. ISPs control content like web authors—that is, their services are even more targeted than, say, a television channel, which also makes value judgments about what its users receive. These judgments, this Note argues, make the ISP the agent of the community, not a dictator of morality.

ISPs also already act as the statutory speakers for classes of users in CAN-SPAM. ISPs do the filtering, and ISPs—not users—have standing to sue, and receive damages. CAN-SPAM awards ISPs $25 or more per infringing message, after users opt out. This reflects the fact that ISPs bear the cost of spam and that filtering policies, in general, represent collective choices by a community about what kind of speech they wish to receive. Complaints about missed legitimate mail and delivered spam enforce ISP accountability. Especially since ISPs have no authority to enforce filtering policies using cybertrespass, a Do-Not-Spam List is the only way to give clear notice about and enforce these choices. This list would be the only way email communities can post a legally enforceable “No Solicitation” sign.

Under this regime, users could opt back into mailings because the sender is responsible for verifying what kind of message he is sending. For example, a sender knows if he is sending transactional messages which fall outside CAN-SPAM, and if he could therefore ignore the domain’s opt-out. The same

290. See supra note 29.
292. Levine & Shafranovich Interview, supra note 266, at 21.
295. Levine & Shafranovich Interview, supra note 266, at 20.
298. Id. § 7706(g)(3)(A) (setting statutory damages for misleading header information at $100 per message, and capping damages for other violations at $1,000,000).
300. Levine & Shafranovich Interview, supra note 266, at 27.
could hold true for a user who affirmatively opted in despite the registry. These affirmative defenses would be akin to the same defenses in CAN-SPAM for sending mail after an opt-out or sending transactional messages.

The Do-Not-Spam List would make consumer choice between ISP spam policies more educated. Filtering policies are opaque in a way that the Do-Not-Spam Registry would not be. The registry would make the market competition more robust and rational because it would be so much more informed. The Do-Not-Call list is somewhat confidential, and telemarketers are required to purchase the list and scrub using their own software. The domain opt-out would instead be actively public. Domains would have to answer to their users about why they have not (or have) opted out of spam or categories of spam. The list could also alert consumers when ISPs break their own stated preferences by contracting them into spam affiliations, like Bonded Sender programs.

Users can and already have changed the policies of their ISPs through competition, and users can choose an email system that has publicly announced a viewpoint users share. Given that a majority of users are willing to switch ISPs for better spam filtering, it follows consumers would switch if the Do-Not-Spam list selections did not match their preferences. It is easy for consumers to get additional email addresses and change domains. Thus, consumers who value pornographic spam could seek a domain that also does. This preference would not impose external costs on the other members of the domain. Today, users have many mail options, and often maintain multiple addresses. Even groups like the AFL-CIO weigh in on ISP choices. The solution proposed by this Note thus piggybacks on an already robust market.

If there are still concerns about ISP agency over filtering, an easy way to remove the perceived imprimatur would be to give individuals a private right of action for violations of the Do-Not-Spam list, as they have under the Junk Fax statute. This would allow an individual to profit from the codification of the community’s filtering policies, but it would allow users who agreed to, or even sought out, specific opt-outs to enforce the norms in their community. When CAN-SPAM was passed, a private right of action was already in place in Utah and was set to begin in California. Advocacy groups proposed that the successful private right of action against malicious junk faxes could translate to spam. For example, a technology policy group recommended a right of

302. Claburn, supra note 78.
303. See supra note 54.
304. Levine & Shafranovich Interview, supra note 266, at 21.
Opting Out of Spam

action based on this pattern, with no class action options.\textsuperscript{307}

However, class action lawsuits against spammers were rejected by CAN-SPAM for good reason. ISPs act as effective class representatives already, bearing most economic costs of the class. While a group of users could probably show substantial damages, this kind of class action has proven to be too tempting to abuse. During Utah’s brief tenure with a private right of action, a specialized class-action plaintiff firm filed hundreds of lawsuits against “low-hanging fruit,” or established companies for accidental oversight or highly technical violations.\textsuperscript{308} CAN-SPAM views ISPs as the agents of users, competent to do everything but declare their communities spam-free zones.

ISPs are not intended as recipients of messages, but the community served by an ISP’s servers is. ISPs already can and do enforce community norms, which are checked by competition and complaints about lost mail, too much spam, or particular kinds of spam. ISPs are not anonymous corporations; rather, they are groups of mail recipients, often with similar values, sharing mail servers. The Domain Do-Not-Spam Registry would allow communities to express their ex ante preferences, as with the Do-Not-Call Registry, but in a legally enforceable and realistic way.

CONCLUSION

Spam significantly burdens both ISPs and users, and it degrades the medium of email. The efforts of the law and markets to block spam have made a large impact, but have not done enough. CAN-SPAM, criticisms notwithstanding, has done a remarkable job stopping the most abusive spamming, and has put many fraudulent spamming operations out of business.

However, CAN-SPAM has left a gaping hole in users’ rights over their mailboxes. A user should have the right to refuse commercial speech he does not want, and the way to do that at minimal interference to speech and minimal cost is a Do-Not-Call Registry, but at the domain rather than the address level. A Domain Do-Not-Spam Registry, enforced like Junk Fax and CAN-SPAM, imposes minimal cost on senders, and best protects the values of the community.

