Case Western Reserve Law Review

Volume 54 | Issue 3

2004

Spammers Clog In-Boxes Everywhere: Will the CAN-SPAM Act of 2003 Halt the Invasion ?

Erin Elizabeth Marks

SPAMMERS CLOG IN-BOXES EVERYWHERE:
WILL THE CAN-SPAM ACT OF 2003 HALT THE INVASION?

INTRODUCTION

Unsolicited commercial email ("spam"[1]) imposes substantial costs on all participants in the electronic mail system and invades the privacy of recipients. Recognizing the need to shift the costs of advertising and increase the privacy of email users, Congress enacted the CAN-SPAM Act of 2003.[2] The legislation, however, lacks bite to deal effectively with the problems spawned from spam. It particularly fails to stop spammers from invading the privacy of Americans. A significant reduction in spam and the corresponding invasion of privacy will ensue only with a combination of market-based initiatives and protective legislation.

I. THE PROBLEM WITH SPAM

A. Spam Imposes Substantial Costs on Email Users

Spam has become an enormous problem costing individuals and businesses a significant amount of time and money. Spam currently accounts for more than half of all email traffic.[3] Americans spent an estimated $10 billion this year taking care of the

---

[1] The name "spam" derived from a Monty Python comedy bit in which the word was repeated to the point of absurdity in a restaurant menu. *See* CompuServe Inc. v. Cyber Promotions, Inc., 962 F. Supp 1015, 1018 n.1 (S.D. Ohio 1997).

[2] *CAN-SPAM Act of 2003 Report of the Committee on Commerce, Science and Transportation on S.877*, S. REP. NO. 108-102, at 12-13 (2003) [hereinafter Legislative History], *available at* http://www.access.gpo.gov/nara/publaw/108publ.html. The full text of the CAN-SPAM Act of 2003 can be found at Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, Pub. L. 108-187, 117 Stat. 2699 (Dec. 16, 2003) [hereinafter CAN-SPAM Act], *available at* www.access.gpo.gov/nara/publaw/108publ.html.

[3] Jennifer Lee, *House Accepts Revisions on Antispam Bill*, N.Y. TIMES, Dec. 9, 2003, at C10.

abundance of unwanted electronic messages;[4] productivity losses accounted for nearly $4 billion of that total.[5] "The average worker receives 13.3 spam messages a day, which takes six and a half minutes to process. Do the math and that comes to 1.4 percent of their productive time."[6] Additionally, many business travelers and individuals living in rural areas incur either long distance fees or per minute surcharges when accessing the Internet.[7] Deleting spam thus imposes substantial direct costs on recipients in the form of both time and money.

Further indirect costs attributable to spam include machine resources, network bandwidth, and user fees.[8] Internet service providers ("ISPs") spend on annual labor, additional bandwidth, and software aimed at filtering spam out of networks and out of customers' in-boxes.[9] Every computer accessed in the transmission of a spam message uses time and energy to process that message; this time and energy takes away from each computer's ability to process other legitimate tasks.[10] Spam messages also clog the channels between machines and cause the entire Internet to operate at a slower pace.[11] ISPs thus incur significant costs in combating and processing this offensive marketing technique. These costs trickle down to each and every person who uses the Internet—an estimated 140 million Americans[12]—since Internet users subsidize spam and its prevention through their subscription fees. Research indicates that fighting spam adds an average of $2 per month to an individual's Internet bills.[13] On a global level, spam has had a similar effect and cost individuals an estimated $20.5 billion this past year.[14]

Spammers, on the other hand, bear a very low cost burden. They pay as little as 0.025 cents per email message due in part to the inexpensive methods used to compile address lists.[15] Deirdre Mulligan testified before Congress:

---

[4] Saul Hansell, *Totalling up the Bill for Spam*, N.Y. TIMES, July 28, 2003, at C1.

[5] Legislative History, *supra* note 2, at 7.

[6] Hansell, *supra* note 4 (quoting Rebecca Wetternmann, research director of Nucleus).

[7] Legislative History, *supra* note 2, at 7.

[8] CURTIS D. FRYE, PRIVACY-ENHANCED BUSINESS: ADAPTING TO THE ONLINE ENVIRONMENT 25 (2001).

[9] Carol Jones, *Email Solicitation: Will Opening a "Spam-Free" Mailbox Ever Be a Reality?* 15 LOY. CONSUMER L. REV. 69, 71 (2002).

[10] FRYE, *supra* note 8, at 25.

[11] *Id.*

[12] Legislative History, *supra* note 2, at 2.

[13] *Id.* at 6.

[14] Hansell, *supra* note 4 (referring to a study by the Radicati Group).

[15] *Id.* Notably, spammers obtain email lists using various techniques. In a "dictionary attack" the spammer reels in masses of computer generated potential email names to see which ones bite. "Harvesting" email addresses involves the use of software programs that crawl

> It is much less expensive to send bulk email than conventional mail. Each additional piece of conventional mail requires both another paper copy and additional postage. With email, however, the only cost to the sender is typing one more email address into the recipient list. The true cost of bulk email is shifted to other parties, such as the sender's ISP, the recipients' ISPs, and the recipients themselves. The sender never bears the additional costs imposed on the ISPs and the recipients.[16]

In addition, spam routinely contains some form of false or misleading information and consistently offends recipients by pushing investment scams, pornography, or pills. The Federal Trade Commission found that sixty-six percent of all spam contains false, fraudulent, or misleading information somewhere in the email's routing information, subject line, or message content.[17] Regarding the subject matter of spam messages, twenty percent of the messages promote "get-rich-quick" schemes, eighteen percent contain sexually explicit content, seventeen percent offer credit card deals, and ten percent push health care products and services.[18] Upon consideration of the enormous costs and objectionable content imposed by spammers on Internet users, it becomes evident that this problem cannot continue.

B. Spam Invades the Privacy of Individuals

> *"A man's home is his castle into which not even the king may enter."*[19]

Various cultures differ in their perspective on acceptable levels of personal space. Travel throughout Europe, the Middle East, Asia, and the United States and notice the varying norms of proximity. Personal space transcends the physical world. Varying cultures tolerate a range of personal space with respect to tangible as well as intangible space, including information like medical re-

---

through Web pages looking for the "@" symbol and record the type to the left and right of the symbol to put addresses together. Jack Hitt, *Confessions of a Spam King*, N.Y. TIMES, Sept. 28, 2003, § 6, at 48. To identify active email accounts, many spam messages contain "web bugs" or other technological mechanisms that notify the spammer when a recipient has opened a message. Legislative History, *supra* note 2, at 4.

[16] Sabra-Anne Kelin, *State Regulation of Unsolicited Commercial Email*, 16 BERKELEY TECH. L.J. 435, 437 n.11 (2001) (identifying Deirdre Mulligan as Staff Counsel for the Center for Democracy and Technology).

[17] *Id.* at 2.

[18] *Id.* at 4.

[19] Rowan v. U.S. Post Office Dep't, 397 U.S. 728, 737 (1970) (quotations omitted) (citing Camara v. Municipal Court, 387 U.S. 523 (1967)).

cords, credit histories, and financial documents.[20] Like the territorial art of the wild animal, the invisible boundary dividing personal from community space demands recognition and respect. Such a boundary provides a sense of comfort and security. The flouting of personal space evokes a sense of violation and assault. The invasion of one's personal space annihilates privacy.[21] Email in-boxes constitute personal space.[22] Spam functions to invade email in-boxes and therefore violates the privacy of email users.

Spam infringes on individuals' right to privacy, their right "to be let alone." In *Rowan v. United States Post Office Department*, the United States Supreme Court recognized an individual's right "to be let alone" and held that a mailer's right to communicate had to stop at the mailbox of an unreceptive addressee.[23] Appellants challenged the constitutionality of a statute that, in effect, banned sexually explicit mailings on the basis of First Amendment free speech.[24] In response, the Court pointed to the necessity that the right "to be let alone" must balance with the right of others to communicate.[25] "[I]ndividual autonomy must survive to permit every householder to exercise control over unwanted mail."[26] The Court relied on the ancient concept that "'a man's home is his castle' into which 'not even the king may enter.'"[27] Accordingly, the statute served to protect individuals' privacy and passed constitutional muster. The Court stated:

---

[20] *See* Global Internet Liberty Campaign, *Privacy and Human Rights: An International Survey of Privacy Laws and Practice*, *at* www.gilc.org/privacy/survey (providing details on the state of privacy laws in several countries throughout the world) (last visited Feb. 19, 2003).

[21] "Privacy is a limitation on the access of one or more entities to an entity that possesses experience." DAVID M. O'BRIEN, PRIVACY, LAW, AND PUBLIC POLICY 16 (1979) (quoting Roland Garrett, *The Nature of Privacy*, 18 PHIL. TODAY 263, 264 (1974)). One compromises another's privacy when he or she gains unwelcome access to another's experiences or engagements. One type of invasion of privacy refers to an intrusion upon one of an individual's engagements that influences that person's enjoyment of such engagement. Another type of invasion of privacy occurs when one gains unsolicited access to another through the accumulation and disclosure of personal information. In either case, individuals seek redress through litigation or the political process, leaving the government to decide what comprises an invasion of privacy, whether a reasonable expectation of privacy exists, and whether government protection best serves the public interest. *Id.* at 18.

[22] *See* Cyber Promotions, Inc. v. AOL, 948 F. Supp. 436, 442 (E.D. Pa. 1996) (rejecting plaintiff's argument that he had a right to send bulk commercial email to AOL customers because the online service qualified as a "company town" for purposes of access to its subscribers since the service did not perform any traditionally municipal or essential public services).

[23] *Rowan*, 397 U.S. at 736.

[24] That statute allowed individuals to "opt-out" of future sexually explicit mailings by providing the postal service with notice of such intention. *Id.* at 729.

[25] *Id.*

[26] *Id.* at 726.

[27] *Id.* at 737 (citing Camara v. Municipal Court, 387 U.S. 523 (1967)).

> In effect, Congress has erected a wall—or more accurately permits a citizen to erect a wall—that no advertiser may penetrate without his acquiescence. The continuing operative effect of a mailing ban once imposed presents no constitutional obstacles; the citizen cannot be put to the burden of determining on repeated occasions whether the offending mailer has altered its material so as to make it acceptable. Nor should the householder have to risk that offensive material come into the hands of children before it can be stopped.[28]

The Court rejected the argument that a vendor has a right to send unwanted mail into the home of another:[29] "[N]o one has a right to press even 'good' ideas on an unwilling recipient."[30] Even though our Constitution guarantees a right to free speech, individuals do not have to endure objectionable speech within the sanctuary of the home. Thus, the right of the mailer stops at the outer boundary of every person's domain.[31]

Similarly, the right of the spammer to communicate must stop at the outer boundary of every person's domain. The sanctuary of the home in the *Rowan* case subsumed the mailbox. A mailbox and an email in-box are analogous in that they serve the same purpose—to facilitate communication. Both function to send and receive communications. Moreover, individuals maintain a higher expectation of privacy with regard to email addresses due to the nonexistence of an email address directory similar to a phone book. Email addresses maintain anonymity, and certainly are not a matter of public record. Each recipient needs a password to access an in-box in cyberspace just as one needs a key to enter a domain in physical space. An in-box, however intangible, must therefore be considered part of the home and enjoy at least the same protected status as the mailbox. It follows that no one has the right to impose ideas on unwilling recipients in the sanctuary of their email in-box. Spammers do not have a basic right to send unsolicited commercial emails to individuals' in-boxes. Consequently, spam encroaches upon the personal space of individuals and violates their right "to be let alone," their right to be free from objectionable intrusion, their right to privacy.

Even without reliance upon the analogy between mail and email, email inboxes constitute personal, rather than community,

---

[28] *Id.* at 738.
[29] *Id.*
[30] *Id.*
[31] *Id.*

space and thus enjoy privacy protection. In *CompuServe Inc. v. Cyber Promotions, Inc.*, an ISP sought to enjoin a spammer from sending unsolicited commercial email to its subscribers based on a trespass to chattels claim.[32] The ISP asserted that the volume of messages generated by mass mailings placed a substantial burden on its equipment and storage capacity.[33] Further, defendant spammers ignored the ISP's notification that they were prohibited from continuing such activity and disregarded the ISP's request to cease and desist from sending unsolicited email to its subscribers. In fact, the defendant spammers modified their equipment and messages to circumvent the ISP's filtering software.[34] The ISP in *CompuServe* asserted that such action constituted a trespass upon its personal property. The court agreed, holding that "[t]he use of personal property exceeding consent is a trespass."[35] Electronic signals generated and sent by computer have been held to be sufficiently physically tangible to support a trespass cause of action.[36] Moreover, the court distinguished ISPs from common carriers and public utilities in response to the defendant's argument that the electronic access way was public property.[37] Given the determination that ISPs maintain private property, email in-boxes must therefore constitute personal private property rather than community or public property.

Furthermore, in *Cyber Promotions, Inc. v. AOL*, a federal district court rejected an argument that the ISP acted as a municipality and found that AOL had the right to prevent spammers from reaching its subscribers over the Internet.[38] Defendant spammers alleged that AOL's conduct had the character of state action to support that AOL had to respect their right to free speech.[39] They compared AOL's Internet email services to those of a company town, which the Supreme Court had previously held performed a public function.[40] The court, however, distinguished AOL from a company town. AOL did not exercise any "municipal powers or public services traditionally exercised by the State."[41] Even though AOL "technically" availed its email system to the public by

---

[32] 962 F. Supp. 1015, 1020 (S.D. Ohio 1997).

[33] *Id.* at 1019.

[34] *Id.*

[35] *Id.* at 1024.

[36] *Id.* at 1021.

[37] *Id.* at 1025-28.

[38] *Cyber Promotions*, 948 F. Supp. at 442 (citing Marsh v. Alabama, 326 U.S. 501 (1946)).

[39] *Id.* at 441.

[40] *Id.*

[41] *Id.* at 442.

connecting with the Internet, it did not open its property to the public by performing functions typically reserved for a municipality or State.[42] AOL's Internet email connection did not constitute an exclusive public function because several alternatives to email existed for commercial communication, such as the World Wide Web, U.S. mail, telemarketing, television, cable, newspapers, magazines, and leaflets.[43] Email in-boxes correspondingly constitute personal, rather than community, space and thus enjoy a right to privacy.

II. CAN-SPAM ACT

Congress acknowledged the importance of email and realized the insidious abuse by spammers through the passage of the CAN-SPAM Act, effective January 1, 2004.[44] In recognizing that many spammers purposely mislead recipients and often disguise their identity, Congress aimed to curb the widespread exploitation of the email system.[45] Congress set forth the rationale behind the law: there is a substantial government interest in regulating commercial email on a national level; spammers should not mislead recipients as to the source or content of electronic messages; and recipients of commercial email have the right to decline additional spam messages.[46]

The CAN-SPAM Act prohibits predatory and abusive commercial email. The law penalizes individuals who knowingly engage in the following behavior:

> 1) accessing a protected computer without authorization and intentionally initiating the transmission of multiple commercial email messages through that computer;
>
> 2) sending several multiple commercial email messages with the intent to deceive or mislead recipients, or any Internet access service, as to the origin of such messages;
>
> 3) materially falsifying header information in several commercial emails and intentionally initiating the transmission of such messages;
>
> 4) registering for five or more email accounts or online user accounts or two or more domain names using a false

---

[42] *Id.*
[43] *Id.* at 443.
[44] CAN-SPAM Act, Pub. L. 108-187, 117 Stat. 2699 (Dec. 16, 2003).
[45] *Id.* § 2(a).
[46] *Id.* § 2(b).

identification and intentionally sending spam from such accounts or domain names;

5) falsely representing oneself to be the registrant of five or more Internet Protocol addresses and intentionally initiating the transmission of spam.[47]

For participating in the above activities, an individual can face up to five years in jail and $6 million in fines.[48]

The Act contains an "opt-out" provision requiring commercial email messages to include a functioning return email address that a recipient may use to opt-out of future spam from the sender.[49] The email address provided must remain active for at least thirty days after the transmission of the original message.[50] Once a consumer effectively chooses to opt-out of future email messages, the sender must respect the decision. It will thereafter be unlawful for the initial sender or anyone acting on such person's behalf to transmit, or to assist in the transmission of, a commercial email message upon the expiration of ten business days after the receipt of the opt-out notice.[51] The initial sender and any person with knowledge of the opt-out request must refrain from selling, leasing, exchanging, or transferring the recipient's email address.[52] In addition, commercial email messages must provide clear and conspicuous identification that the message is an advertisement or solicitation, notice of the opportunity to decline to receive further messages, and a valid physical postal address of the sender.[53]

The Act also prohibits harvesting and dictionary attacks[54] and requires individuals to place warning labels on commercial emails containing sexually oriented material.[55] Email messages containing sexually explicit content must include in the subject line the marks or notices prescribed by the FTC.[56] Such messages must further ensure that the message when initially opened contains only the content required by the "opt-out" provision and instructions on how to access the sexually explicit material, unless the sender receives the prior affirmative consent of the recipient.[57] An

---

[47] *Id.* § 4(a).
[48] *Id.* §§ 4(b), 7(f)(3)(A)-(D).
[49] *Id.* §§ 5(a)(3)-(4).
[50] *Id.* § 5(a)(3)(A)(ii).
[51] *Id.* §§ 5(a)(4)(A)(i)-(iii).
[52] *Id.* § 5(a)(4)(A)(iv).
[53] *Id.* § 5(a)(5).
[54] *Id.* § 5(b)(1); *see supra* note 15 (explaining "harvesting" and "dictionary attacks").
[55] *Id.* § 5(d).
[56] *Id.* §§ 5(d)(1)(a), 5(d)(3).
[57] *Id.* §§ 5(d)(1)(B), 5(d)(2).

individual in violation of this provision can face up to five years in jail and/or fines.[58]

The CAN-SPAM Act limits the role of the states in combating spam. Enforcement actions lie primarily in the hands of the FTC.[59] State attorneys general can bring civil actions to seek injunctions or to obtain damages only if the alleged violation threatens the interests of a resident of the particular state.[60] The CAN-SPAM Act preempts or supersedes state laws that expressly deal with commercial emails.[61] States can only prohibit false and deceptive commercial email messages and can regulate issues such as computer crime, tort, and trespass.[62]

Congress also called for the FTC to submit reports about the effects of spam. Within six months of the effectiveness of Section 9, the FTC must present Congress with a report outlining a plan for the establishment of a national Do-Not-Email registry.[63] The report must include a timetable for implementation, an explanation of all FTC concerns, and an explanation of how such a registry would apply to children with email accounts.[64] The Act authorizes the FTC to implement a Do-Not-Email registry nine months from the date of enactment of Section 9.[65] By January 2006, the FTC must further submit a report assessing the effectiveness and enforcement of the provisions of the CAN-SPAM Act.[66] The report must include an analysis of the state of technology and the market in reference to the law, analysis and recommendations on how to eliminate spam on an international level, and analysis and recommendations on how to protect children from obscene or pornographic commercial email messages.[67]

A. Strengths of the CAN-SPAM Act

In response to the widespread spam problem, Congress importantly recognized a substantial government interest in creating a solution to the spam problem through the passage of the CAN-SPAM Act. This legislative action enjoyed rare overwhelming

---

[58] *Id.* § 5(d)(5).
[59] *Id.* § 7(a).
[60] *Id.* § 7(f).
[61] *Id.* § 8(b).
[62] *Id.* § 8(b).
[63] *Id.* § 9(a).
[64] *Id.* § 9(a). Section 16 sets the effective date as January 1, 2004, for all provisions except section 9.
[65] *Id.* § 9(b).
[66] *Id.* § 10(a).
[67] *Id.* § 10(b).

bipartisan support,[68] which signals legislative commitment to the issue and understanding of the severity of the problem. Given the overwhelming consistency in prior case law, the CAN-SPAM Act supports the individual's right "to be let alone" in balancing privacy with free speech rights and thus accords with the framework of the Constitution.[69] The CAN-SPAM Act will beneficially serve to deter spammers from sending fraudulent or misleading email messages, from concealing their identity, and from using obtrusive methods to collect email addresses. Email users will be able to identify spam messages as advertisements generally and as pornographic messages specifically due to the provisions of the Act. Congress identified the key issues regarding spam in calling for FTC reports analyzing a Do-Not-Email List, internationally harmonized legislation, and greater protection of children from the harms of obscene and pornographic commercial messages. Thus, the CAN-SPAM Act serves a valid and useful purpose in initiating legislative action, which will serve to stop spam, increase privacy of U.S. citizens with respect to their email in-boxes, and relieve them from the burdens of paying for unwanted advertising.

B. Weaknesses of the CAN-SPAM Act

"The bill doesn't can spam, it legalizes it . . . it is full of loopholes. It's difficult to enforce. It's weaker than many state laws."[70]

The CAN-SPAM Act does not create an effective solution to the enormous spam problem because it allows spammers to invade in-boxes, forces spam recipients to take an affirmative act to curtail future invasions, provides lenient requirements and inadequate enforcement mechanisms, voids stricter state anti-spam laws, and puts off the need for a global solution. Despite Congressional acknowledgment of the spam problem, recognition of the substantial government interest in remedying such a problem, and the bipartisan support for this federal anti-spam legislation,[71] Congress conceded to special interest groups and denied consumers adequate protection from such invasive marketing techniques.[72] Unified

---

[68] *See* Voting Record, 2003 H. ROLL NO. 671 (Nov. 21, 2003); 2003 SEN. VOTE NO. 404 (Oct. 22, 2003), *available at* www.senate.gov/legislative/LIS/roll_call_lists/roll_call_vote_cfm.cfm?congress=108&session=1&vote=00404.

[69] *See supra* Part I.B.

[70] Jennifer Lee, *Antispam Bill Passes Senate by Voice Vote*, N.Y. TIMES, Nov. 26, 2003, at C3 (quoting California State Senator Debra Bowen).

[71] Voting Record, *supra* note 68.

[72] Jennifer Lee, *Bush Signs Law Placing Curbs on Bulk Commercial Email*, N.Y. TIMES,

public opinion against spam motivated some sort of legislative action, albeit impotent. Anti-spam bills floated around Congress for four years before the adoption of the law,[73] and the law passed only after marketing organizations hopped on board to lobby for the weakest form of regulation.[74] The CAN-SPAM Act serves more as lip service to denote the government's identification of a widespread problem, rather than an effective solution to a costly and invasive problem.

The debate around spam legislation focuses on two conflicting approaches, the "opt-in" and the "opt-out" mechanisms.[75] The "opt-in" approach requires that all spammers obtain express permission before transmitting any email addresses.[76] The more lenient "opt-out" approach allows spammers to send messages as long as each message offers a legitimate link from which one can request that the spammer refrain from sending future emails.[77] Congress favors the "opt-out" approach because it provides marketers and businesses with the most breathing room.[78]

The "opt-out" method of regulation, however, fails to protect the privacy of individuals.[79] It allows uninvited and unwelcome messages to infiltrate in-boxes in homes and businesses, and then provides an antidote available for every infliction at the expense of the victim's time and money. Individual recipients are forced to take an affirmative step against each piece of unwanted mail; such step wastes more time and money than the problem itself. By implementing the "opt-out" approach, Congress has simply developed a medicine to treat the symptoms of spam, an elective treatment that imposes additional costs on individuals. Individuals need not a cumbersome and repetitive serum to counter spam. Individuals need Congress to stand up for the integrity of privacy by choosing a method that will eradicate the plague of spam that infects the worldwide email system.

In terms of privacy, the "opt-in" approach protects consumers in a significantly greater and more effective manner. The "opt-in" approach prohibits unsolicited intrusions and requires that spam-

---

Dec. 17, 2003, at C4; *see also Congressional Spam Filter*, N.Y. TIMES, Nov. 3, 2003, at A18.

[73] Cong. Info. Serv., Inc., Bill Tracking Report, 108th Cong., 1st Sess., U.S. Senate, *at* LEXIS, 2003 Bill Tracking S. 877.

[74] *Congressional Spam Filter*, *supra* note 72.

[75] Hitt, *supra* note 15.

[76] *Id.*

[77] *Id.*

[78] Legislative History, *supra* note 2, at 17-18.

[79] *See* David E. Sorkin, *Technical and Legal Approaches to Unsolicited Commercial Email*, 35 U.S.F. L. REV. 325, 352-55 (2000) (offering a brief analysis of the "opt-out" approach and concluding it an ineffective method to curb spam).

mers send invited messages only. Like a vaccine prevents a disease, the "opt-in" approach stops the widespread dissemination of spam. Rather than imposing the costs of the remedy on all email users for each uninvited message like the "opt-out" approach, the "opt-in" approach imposes costs on spammers and those interested in receiving spam. In other words, it shifts the burden of spam onto spammers. Spammers must ask permission to enter an in-box instead of entering and then being asked to leave. The "opt-in" approach would ultimately serve to reduce the enormous volume of contamination clogging networks and flooding the email system, and would halt the widespread waste of time and money directed at eliminating spam. Congress must adopt the "opt-in" approach to protect the privacy of email users and cure the disease infecting in-boxes–spam.

A Do-Not-Email list would perhaps quell many of the defects of the "opt-out" approach by arriving at an outcome similar to that of the "opt-in" approach—the widespread eradication of unsolicited email. This approach provides consumers with the ability to opt-out of all spam by registering their email addresses and, arguably, will result in a widespread reduction in spam. Opponents of the Do-Not-Email list idea, however, contend that such list would not elicit the results garnered by the do-not-call list because most spammers are illegitimate and crooked individuals unlikely to comply with any list.[80] Furthermore, a do-not-spam list would prove expensive to administer and vulnerable to hackers.[81] The FTC agrees that a do-not-spam list would be difficult to administer and enforce and thus not very useful or effective in the fight against spam.[82] Nevertheless, such an approach will not take effect in the near future anyway since the FTC has ample time to consider a Do-Not-Email list and submit its findings to Congress.[83]

The CAN-SPAM Act sidesteps the need for an internationally harmonized solution to spam by allowing the FTC two years to study the issue. The FTC has until January 2006 to analyze potential global solutions and make a recommendation to Congress on how to eliminate spam across the worldwide email system.[84]

---

[80] Saul Hansell, *The Bandwagon to Fight Spam Hits a Bump*, N.Y. TIMES, Aug. 11, 2003, at C1.

[81] *Id.*

[82] *See FTC Chief Doubtful of Antispam Legislation*, N.Y. TIMES, Aug. 21, 2003, at C30 ("A do-not-spam registry would be impossible to enforce, [Timothy J. Muris, FTC Chairman] said, because the senders of such email messages generally conceal their identities."); *see also* Hansell, *supra* note 80 ("Most spam is already clearly so illegitimate that senders are not likely to comply." (quoting J. Howard Beales III, Director of FTC Consumer Protection Bureau)).

[83] CAN-SPAM Act, Pub. L. 108-187, 117 Stat. 2699, § 9 (Dec. 16, 2003).

[84] *Id.* § 10(b).

European Commission officials alluded that the U.S. passage of the CAN-SPAM Act hampers efforts to form an international alliance to combat spam because the Act fails to prohibit spam entirely.[85] The U.S. and the EU currently have opposing legislation and will continue in such position until 2006, at least, when Congress considers a global agenda. The EU Directive, enacted in the fall of 2003, forbids email promotions unless the recipient gives the marketer prior consent.[86] The EU holds the position that an email account must enjoy privacy and thus requires businesses to obtain explicit permission before sending email messages.[87] To effectively stop spam from systematically compromising the privacy of email users, Congress must take action to harmonize the U.S. position on spam with that of the EU by supporting the "opt-in" approach.

With the passage of the CAN-SPAM Act, states lose their ability to regulate spam in a more restrictive manner than the federal law. Stripping the states of all legislative power in this area essentially paralyzes an entire faction willing and able to contribute to the anti-spam effort. Louis Brandeis articulated one of the most famous formulations in American law—that the states should be free to serve as "laboratories" of democracy.[88] He argued that

---

[85] *E-Privacy Directive: Directive 2002/58/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector*, 2002 O.J. (L 201) 37 (July 12, 2002) [hereinafter E-Privacy Directive]; *see also* Paul Meller, *World Business Briefing Europe: European Union: U.S. Help Sought on Spam*, N.Y. TIMES, July 16, 2003, at W1.

[86] E-Privacy Directive, *supra* note 85, at arts. 6(3), 13 (requiring the consent of recipients to send direct marketing solicitations).

[87] *Id.* ¶ 12 ("[T]his Directive is aimed at protecting the fundamental rights of natural persons and particularly their right to privacy."); *id.* ¶ 40 ("Safeguards should be provided for subscribers against intrusion of their privacy by unsolicited communications for direct marketing purposes in particular by means of . . . emails."); *see also* Hansell, *supra* note 80.

[88] New State Ice Co. v. Liebmann, 285 U.S. 262, 310-11 (1932) (Brandeis, J., dissenting). The pertinent portion of the dissent follows:

> Yet the advances in the exact sciences and the achievements in invention remind us that the seemingly impossible sometimes happens. There are many men now living who were in the habit of using the age-old expression: "It is as impossible as flying." The discoveries in physical science, the triumphs in invention, attest the value of the process of trial and error. In large measure, these advances have been due to experimentation. In those fields experimentation has, for two centuries, been not only free but encouraged. Some people assert that our present plight is due, in part, to the limitations set by courts upon experimentation in the fields of social and economic science; and to the discouragement to which proposals for betterment there have been subjected otherwise. There must be power in the States and the Nation to remould, through experimentation, our economic practices and institutions to meet changing social and economic needs. I cannot believe that the framers of the Fourteenth Amendment, or the States which ratified it, intended to deprive us of the power to correct the evils of technological unemployment and excess productive capacity which have attended progress in the useful arts.

the rational way to advance society was through "experimentation," the same process of trial and error used in the physical sciences.[89] States must enjoy the freedom to craft laws above and beyond those enacted at the federal level. With regard to spam, the states are willing and able to contribute their legislative efforts; thirty states enacted laws in an effort to resolve the spam problem.[90] California, for example, adopted an anti-spam law that required prior consumer consent ("opt-in") and allowed individuals to sue spammers in the event of government inaction.[91] Given the rapid pace of technological advance, Congress must provide states with the authority to regulate spam above and beyond the federal regulation, and allow states to utilize their resources to enforce such laws.

The CAN-SPAM Act lacks a provision guaranteeing individuals a private right of action to allow for adequate enforcement. Congress decided to take a top-down approach to enforcement by focusing on the detainment and trial of a few kingpins in the spam world.[92] The top-down tactic supposedly acts to scare mid- and low-level players into compliance. Even though ninety percent of spam messages are sent from two hundred individuals,[93] technology changes so quickly that spammers can easily escape government radar. Individuals must therefore have access to courts to control spam.

> To stay experimentation in things social and economic is a grave responsibility. Denial of the right to experiment may be fraught with serious consequences to the Nation. It is one of the happy incidents of the federal system that a single courageous State may, if its citizens choose, serve as a laboratory; and try novel social and economic experiments without risk to the rest of the country. This Court has the power to prevent an experiment. We may strike down the statute which embodies it on the ground that, in our opinion, the measure is arbitrary, capricious or unreasonable. We have power to do this, because the due process clause has been held by the Court applicable to matters of substantive law as well as to matters of procedure. But in the exercise of this high power, we must be ever on our guard, lest we erect our prejudices into legal principles. If we would guide by the light of reason, we must let our minds be bold.

Id.

[89] *Id.*; *see* Adam Cohen, *Brandeis's Views on States' Rights, and Ice-Making, Have New Relevance*, N.Y. TIMES, Dec. 7, 2003, § 4, at 12.

[90] *See* David E. Sorkin, Summary of State Spam Laws, *at* www.spamlaws.com/state/summary.html (last visited Apr. 5, 2004).

[91] CAL. BUS. & PROF. CODE § 17538.45 (2003).

[92] *See* Hitt, *supra* note 15.

[93] Saul Hansell, *Finding Solution to Secret World of Spam*, N.Y. TIMES, May 2, §C, at 8.

III. SOLUTION: A COMBINATION OF MARKET AND LEGISLATIVE EFFORTS

The eradication of spam will occur only through a comprehensive solution involving both market-based and legislative initiatives.

A. Market Forces

Market-based initiatives include self-help mechanisms and spam filtering systems.[94] For self-help, email users can always use the delete key or, under the CAN-SPAM Act, the "opt-out" mechanism to eliminate spam from their in-boxes.[95] These tactics allow users to get rid of unwanted emails only *after* receipt. On the other hand, spam filtering software programs are designed to prevent spam from penetrating in-boxes *before* receipt. One group estimates that eighty percent of companies will install spam filters on their email systems by the end of 2004, up from twenty percent in November 2003.[96] Due to the considerable amount of spam that congests in-boxes, many software experts contend that the most powerful way to clean in-boxes is to focus on identifying the legitimate email and filtering it into users' in-boxes.[97] Market forces react much more quickly than legislatures and must necessarily contribute to an effective answer to the spam problem.

Technical approaches alone are not enough to solve the spam problem. Self-help mechanisms insufficiently accomplish the desired goal of eliminating spam by wasting time and money and allowing the invasion of privacy to occur before action is taken to get rid of the spam. None of the filtering or blocking systems are perfect either; they cost a substantial amount of money to implement, interfere with legitimate message traffic, allow spam to penetrate in-boxes, and fail to relieve email users of the cost burdens associated with spam.[98] Further, spammers adapt their techniques to circumvent filters and other anti-spam technologies. Spammers have a substantial amount of time and resources to devote to their activities, especially given the insignificant costs associated with sending spam.[99] Since market-based initiatives alone cannot serve to relieve cost burdens and curb privacy invasions

---

[94] Jones, *supra* note 9, at 72-73.

[95] *Id.* at 72.

[96] Saul Hansell, *In War over Spam, One Company Is Happily Arming Both Sides*, N.Y. TIMES, Nov. 24, 2003, at C2.

[97] Saul Hansell, *Spam Fighters Turn to Identifying Legitimate Email*, N.Y. TIMES, Oct. 6, 2003, at C1.

[98] Sorkin, *supra* note 79, at 344-50.

[99] *Id.* at 356.

entirely, protective legislation must accompany market forces in realizing the goal of eliminating spam.

B. Protective Legislation

On the legislative side, Congress must prohibit the transmission of unsolicited commercial emails, provide individuals with a private right of action, and reverse the preemption of state anti-spam laws. A blanket prohibition of unsolicited emails requires the informed consent of consumers before the transmission of any spam message. This tactic ensures that individuals can enjoy their right to privacy, while businesses can continue to use the email system to send invited commercial messages. Arming individuals with a private right of action strengthens enforcement and adequately deters violations. Eradicating state preemption furnishes states with an opportunity to experiment with anti-spam laws. The junk fax law serves as a terrific model for this approach. The European Directive on Electronic Commerce corresponds with this method of regulation as well. By implementing the above suggestions modeled after the junk fax law, individuals will enjoy their right to privacy free from spam.

C. Junk Fax Law as a Model for Further Anti-Spam Legislation

Junk faxes present burdens similar to those stemming from spam. Recipients of both types of unsolicited marketing tools absorb many of the costs, while the senders take on relatively minimal expenses. For example, recipients of junk faxes provide the paper and maintain the machine for the transmission of a message, while recipients of spam supply the computer and support the ISP. Furthermore, repeatedly sifting through numerous messages, whether faxes or emails, takes up a significant amount of time, causes a decline in productivity, and leads to additional mistakes. Important messages can easily be overlooked in the case of faxes or deleted in the case of emails. Given the obvious similarities, effective solutions to the problems triggered from junk faxes and spam can mirror each other.

The Telephone Consumer Protection Act of 1991 ("TCPA"), more commonly known as the junk fax law, prohibits the use of fax machines, computers, or other devices to send unsolicited advertisements to fax machines.[100] The law defines unsolicited advertisements as "material advertising the commercial availability

[100] Telephone Consumer Protection Act of 1991, Pub. L. No. 102-243, 105 Stat. 2395 (codified at 47 U.S.C.S. § 227(b)(1)(C) (2003)) [hereinafter "TCPA"].

or quality of any property, goods, or services which is transmitted to any person without that person's prior express invitation or permission."[101] The junk fax law permits individuals to bring private rights of action as long as state law does not expressly prohibit such actions.[102] Congress also chose to avoid preemption in the enactment of the federal junk fax law; the law allows states to adopt more restrictive laws to prohibit the sending of unsolicited advertisements to fax machines.[103] These provisions of the junk fax law exemplify the means necessary to accomplish successful results in the legislative fight against spam.

1. Junk Fax Law and Free Speech

Moreover, several courts have upheld the constitutionality of the TCPA.[104] First Amendment free speech claims have failed because the TCPA does not totally ban fax advertising. Instead, it prohibits unsolicited advertising, which shifts advertising costs to non-consenting consumers.[105] The differentiation between unsolicited or unwanted pestering and invited or permitted soliciting leads to a finding that the TCPA constitutionally regulates commercial speech.

Courts applied the test articulated by the Supreme Court in *Central Hudson Gas & Electric Corp. v. Public Service Commission*[106] to determine the constitutional validity of the TCPA.[107] The *Central Hudson* test hinges on whether the restricted speech concerns unlawful activity or contains misleading information.[108] If the restricted speech does so, then the commercial speech does not enjoy First Amendment protection. If not, then the court considers whether there is a substantial government interest, whether the regulation directly and materially advances such interest, and whether it is not more restrictive than necessary to achieve such interest.[109] Since the regulation of junk faxes does not deal with

---

[101] *Id.* § 227(a)(4).

[102] *Id.* § 227(c)(5).

[103] *Id.* § 227(e)(1)(a).

[104] *See* Missouri v. Am. Blast Fax, Inc., 323 F.3d 649 (8th Cir. 2003); Destination Ventures v. FCC, 46 F.3d 54 (9th Cir. 1995), *aff'g* 844 F. Supp. 632 (D. Or. 1994); Texas v. Am. Blast Fax, Inc., 121 F. Supp. 2d 1085 (W.D. Tex. 2000); Kenro, Inc. v. Fax Daily, Inc., 962 F. Supp. 1162 (S.D. Ind. 1997); Kaufman v. ACS Sys., Inc., 110 Cal. App. 4th 886 (Cal. App. 2d Dist. 2003).

[105] *See Destination Ventures*, 46 F.3d at 56; *Texas*, 121 F. Supp. 2d at 1091; *Kenro*, 962 F. Supp. at 1167; *Kaufman*, 110 Cal. App. 4th at 892.

[106] 447 U.S. 557 (1980).

[107] *Missouri*, 323 F.3d at 652; *Destination Ventures*, 46 F.3d at 55; *Kenro*, 962 F. Supp at 1167.

[108] *Central Hudson*, 447 U.S. at 564.

[109] *Id.*

speech concerning unlawful activity or containing misleading information, courts employ the latter analytical framework.

a. Substantial Government Interest

The TCPA advances the substantial government interest of protecting consumers from the costs imposed by unsolicited fax advertisements.[110] Numerous state laws and the high costs absorbed by consumers support a finding of a substantial government interest.[111] Approximately half of the states have considered laws to prohibit unsolicited fax advertising, and unsolicited commercial faxes cost Californians $17 million per year.[112] Although the junk fax problem lacks substantial history and the TCPA fails to state expressly a substantial government interest, the TCPA constitutes a legitimate Congressional action to protect consumers from harm. The role of Congress in the relationship between advertiser and consumer is well-established,[113] while the legislative history contains sufficient testimonies outlining the real harms caused by unsolicited faxes.[114] A Congressional subcommittee found that:

> [A] [f]estering problem [had] arisen from the so-called "junk fax." Junk fax is more than merely irritating. It represents an unfair shifting of the cost of advertising from the advertiser to the unwitting customer . . . . [U]nsolicited and unwanted faxes can tie up a machine for hours and thwart the receipt of legitimate and important messages.[115]

Thus, the government has a substantial interest in protecting consumers from the economic harms imposed by junk faxes as evidenced by the well-established role of Congress as an intermediary between consumers and advertisers, the legislative history of the TCPA, the widespread state action on the issue, and the heavy costs imposed on consumers.

b. Direct and Material Advancement of Interest Through Regulation

When a substantial government interest is found, the court must determine whether "the challenged regulation advances [the

---

[110] *Kaufman*, 110 Cal. App. 4th at 914-15.

[111] *Id.* at 912.

[112] *Id.*

[113] *Id.*

[114] Destination Ventures v. FCC, 46 F.3d 54 (9th Cir. 1995), *aff'g* 844 F. Supp. 632 (D. Or. 1994).

[115] *Kaufman*, 110 Cal. App. 4th at 892 (quoting *Telemarketing/Privacy Issues: Hearing on H.R. No. 1304 and H.R. No. 1305 Before the Subcomm. on Telecommunications and Finance of the House Comm. on Energy and Commerce*, 102d Cong. 3-4 (1991); *see also* Missouri v. Am. Blast Fax, Inc., 323 F.3d 649 (8th Cir. 2003) (explaining the legislative history of the TCPA).

government's] interests in a direct and material way."[116] Given the government's substantial interest in protecting consumers from the economic harms inflicted through unsolicited commercial faxes, the subsequent banning of such faxes directly advances that interest.[117] The statutory focus on commercial faxes materially advances the government's substantial interest because commercial faxes constitute the bulk of all unsolicited faxes.[118]

c. Narrowly Tailored Test

To satisfy the third prong of the *Central Hudson* test, courts must find:

> [A] fit that is not necessarily perfect, but reasonable; that represents not necessarily the single best disposition but one whose scope is 'in proportion to the interest served,' that employs not necessarily the least restrictive means but . . . a means narrowly tailored to achieve the desired objective.[119]

Plaintiffs generally propose alternative, less restrictive, means of regulating junk faxes to prove that TCPA is too broad. Such alternatives include a do-not-fax list, limits on the sending of junk faxes with respect to volume, frequency, and time of day, and an "opt-out" mechanism. Advertisers under the TCPA, however, remain free to publicize their products or services through various legal marketing techniques, such as the telephone, direct mail, or in-person solicitation.[120] Fax advertisements differ from other forms of advertising because of the costs they impose on recipients.[121] Television and newspaper ads are never unsolicited; the access to such media requires an affirmative and voluntary action on part of the recipient. Direct mail likewise does not impose costs on recipients or interfere with the legitimate mail system.[122] Furthermore, the requirement does not have to impose the "least restrictive means" to comport with the narrowly tailored elements of analysis.[123] With consent, advertisers can continue to use the fax machine as a mechanism to advertise products and services.[124] The TCPA's prohibition on unsolicited faxes is thus narrowly tai-

---

[116] *Id.* at 637 (quoting Edenfield v. Fane, 113 S. Ct. 1792, 1798 (1993)).
[117] *Id.*
[118] *Missouri*, 323 F.3d at 658.
[119] *Id.* at 659.
[120] *Id.*
[121] Kenro, Inc. v. Fax Daily, Inc., 962 F. Supp. 1162, 1168 (S.D. Ind. 1997).
[122] *Id.*
[123] *Id.*
[124] Missouri v. Am. Blast Fax, Inc., 323 F.3d 649, 659 (8th Cir. 2003).

lored to achieve the desired objective of protecting consumers from the costs of unsolicited commercial faxes.

2. Comparative Analysis: Junk Faxes and Spam

Given the similarities between unsolicited commercial faxes and unsolicited commercial emails, the TCPA serves as an excellent model for spam regulation. Indeed, a federal anti-spam law based on such a model would be a great improvement to the CAN-SPAM Act. Even though Congress rightfully acknowledged the government's substantial interest in protecting email users from fraudulent and offensive emails and enacted legislation to curb the most egregious forms of spam, the Act contains weaknesses in several areas. The CAN-SPAM Act fails to curtail the invasion of privacy imposed by spam, burdens individuals with the option to refuse messages on a piecemeal basis, lacks adequate enforcement mechanisms, shortsightedly preempts state law, and delays the implementation of an internationally harmonized law. The TCPA contains provisions that, when applied to spam, would serve to strengthen the anti-spam legislation into a forceful piece of legislation capable of eradicating the widespread problem of spam. Such provisions include an "opt-in" mechanism, a private right of action, and an allocation of state's rights to supplement the federal legislation. Furthermore, several courts have upheld the constitutionality of the TCPA against free speech claims.[125] With the adoption of the proposed changes to the CAN-SPAM Act, courts will likely look to these cases for guidance and apply a similar legal analysis. The TCPA thus functions as an excellent model upon which Congress can draw to cure the weaknesses of the CAN-SPAM Act and ensure its accordance with the First Amendment. It must be noted, however, that the junk fax law serves primarily to relieve commercial enterprises from unwittingly absorbing the costs from unsolicited commercial fax messages,[126] while a sufficient anti-spam law must deal with both cost and privacy issues stemming from unsolicited commercial electronic messages. Nevertheless, the junk fax law serves as a useful model.

CONCLUSION

Spam presents significant problems: It imposes the costs of advertising on all participants in the electronic mail system and

[125] *See supra* note 104 (citing cases that have upheld the constitutionality of the TCPA).

[126] *See* Kaufman v. ACS Sys., Inc., 110 Cal. App. 4th 886, 914 (Cal. App. 2d Dist. 2003) ("The TCPA directly and materially advances the stated interests, namely, preventing cost shifting and permitting fax machine owners to control the operation of their machines.").

invades the privacy of recipients. Congress enacted the CAN-SPAM Act to alleviate email users from the burdens of spam, but the Act fails to deal effectively with the problem. It allows spammers to invade in-boxes and erode privacy, forces spam recipients to take affirmative action to curtail future invasions, provides lenient requirements and inadequate enforcement mechanisms, voids stricter state anti-spam laws, and puts off a global solution. A combination of market-based initiatives and protective legislation will ensure a significant reduction in spam and the corresponding invasion of privacy. Market-based initiatives have the aptitude to thwart the rapid technological advances made by spammers. In conjunction, protective legislation modeled after the junk fax law would serve to halt cost-shifting and protect the privacy of individuals by eradicating spam. Such legislation overcomes the weaknesses that currently taint the CAN-SPAM Act and comports with First Amendment free speech guarantees. By barring the transmission of unsolicited commercial email messages, giving individuals a private right of action, and permitting states to enact more stringent anti-spam legislation, individuals will enjoy their right to privacy free from the offensive, obtrusive, and uninvited plague that has infected the email system everywhere—spam.

ERIN ELIZABETH MARKS[†]

[†] J.D./M.B.A. Candidate, 2004, Case Western Reserve School of Law. Many thanks to Professor Jacqueline Lipton for her insightful feedback and to my husband, Ian, for his gracious support.