Boston College Law Review

Volume 50
Issue 5 *Publicity, Privacy, and Intellectual Property Meet the First Amendment*

Article 10

11-1-2009

Spam-A-Lot: The States' Crusade Against Unsolicited Email in Light of the CAN-SPAM Act and the Overbreadth Doctrine

Igor Helman

SPAM-A-LOT: THE STATES' CRUSADE AGAINST UNSOLICITED E-MAIL IN LIGHT OF THE CAN-SPAM ACT AND THE OVERBREADTH DOCTRINE

Abstract: The ever-increasing deluge of unsolicited e-mail, or spam, results in millions of dollars of economic loss, fosters criminal activity, causes untold user frustration, and threatens to undermine the viability of e-mail as a communication medium. Attempts to stem this tide have thus far been unavailing. The arrival of federal regulation on the scene has not helped matters and, by thwarting earlier state regulation, has created an intractable conflict. On the one hand, narrowly focused state anti-spam laws are now preempted by the federal act. On the other hand, broad attempts to regulate spam, although escaping preemption, collide directly with the First Amendment. This Note examines the marginal regulatory area left in place at the intersection of federal regulation and constitutional boundaries. It further reexamines several assumptions underlying the current case law and regulation of spam, and suggests that altering these assumptions may enable new approaches to deal with this pervasive problem.

Introduction

Unsolicited bulk electronic mail, otherwise known as spam,[1] is almost as old as the Internet itself.[2] Spam routinely frustrates and annoys

[1] *See* Adam Hamel, Note, *Will the CAN-SPAM Act of 2003 Finally Put a Lid on Unsolicited E-mail?*, 39 New Eng. L. Rev. 961, 963 (2005). There is some debate as to the actual definition of spam: whether it constitutes any unsolicited electronic mail (e-mail), unsolicited bulk e-mail, or only unsolicited commercial e-mail. *See id.*; David E. Sorkin, *Technical and Legal Approaches to Unsolicited Electronic Mail*, 35 U.S.F. L. Rev. 325, 327–36 (2001); *see also* Black's Law Dictionary 1430 (8th ed. 2004) (defining spam as unsolicited commercial e-mail); Lawrence Lessig, Code: Version 2.0, at 388 n.64 (2d ed. 2007) (suggesting that all three elements—unsolicited, bulk, and commercial—are necessary to the definition of spam). This Note uses spam to refer generally to unsolicited bulk e-mail ("UBE") and will refer to commercial spam where greater specificity is required. *Cf.* Hamel, *supra*, at 963–64. Spam is believed to have received its name from a skit by the British sketch-comedy troupe Monty Python. *See id.* at 963 n.18. In the skit, a restaurant served only Spam—the canned meat product from Hormel—and most menu items included Spam, such as "Spam, Spam, Spam, eggs, and Spam." *See Monty Python: Spam* (BBC television broadcast Dec. 15, 1970), *available at* http://www.youtube.com/watch?v=anwy2MPT5RE. The frequency and repeti-

users,[3] wastes both time and network resources,[4] and results in relevant messages being drowned out in the noise of unwanted, irrelevant, and oftentimes, fraudulent advertisements.[5] Far from being a mere nuisance, spam can be downright malicious, tricking less than savvy computer users into giving out their bank passwords, credit card information,[6] and even sending money to overseas dupers.[7]

---

tive quality of unsolicited bulk e-mail was similar to the mindless repetition of the word "spam" in the skit and the name stuck. *See* Hamel, *supra*, at 963 n.18.

[2] *See* Katie Hafner, *Billions Served Daily and Counting*, N.Y. Times, Dec. 6, 2001, at G1 (describing the creation of the first e-mail program by a scientist at a Cambridge engineering firm in 1971). The first spam is widely believed to have been sent in 1978 on a network called the Arpanet, which was developed by the Department of Defense Advanced Research Projects Agency and was a precursor to the modern Internet. *See* Andrew S. Tanenbaum, Computer Networks 56 (4th ed. 2002). The message was an advertisement sent by an employee of Digital Equipment Corporation, and the reaction to it was generally not favorable, not the least because the e-mail message strained the limited network resources of Arpanet and slowed down other communication. *See* Jonathan A. Zdziarski, Ending Spam 4–6 (2005). Spam made its resurgence in the early 1990s, most notably because of a husband and wife team of attorneys, who sent out an unsolicited message to roughly 6000 newsgroups advertising their legal services. *See id.* at 10. The advertisement generated nearly $100,000 for the attorneys. *See* Hamel, *supra* note 1, at 965. Some commentators consider this event to be the actual birth of spam. *See, e.g.*, Roger Allan Ford, Comment, *Preemption of State Spam Laws by the Federal CAN-SPAM Act*, 72 U. Chi. L. Rev. 355, 355 n.1 (2005).

[3] *See* Memorandum from Deborah Fellows, PIP Senior Research Fellow, on CAN-SPAM a Year Later to Pew Internet & American Life Project 2 (Apr. 10, 2005), *available at* http://www.pewinternet.org/~/media//Files/Reports/2005/PIP_Spam_Ap05.pdf.pdf ("67% of email users say spam has made being online unpleasant or annoying . . . .").

[4] *See* Cisco Systems, Annual Security Report 13 (2008), *available at* http://www.cisco.com/en/US/prod/collateral/vpndevc/securityreview12–2.pdf (finding about 100 billion messages per day, approximately eighty-five percent of all e-mail, to be spam).

[5] *See* S. Rep. No. 108-102, at 2 (2003), *reprinted in* 2004 U.S.C.C.A.N. 2348, 2348–49 (reciting the pervasiveness along with the generally fraudulent and misleading nature of unsolicited e-mail).

[6] *See* Jasmine E. McNealy, *Angling for Phishers: Legislative Responses to Deceptive E-Mail*, 13 Comm. L. & Pol'y 275, 275 (2008). The practice of "phishing" is a serious problem that stems from spam. Phishing consists of sending e-mail messages resembling those from well-known companies, such as banks, credit card providers, and online payment sites, in the hopes that the recipients click on the hyperlink in the message. *See id.* at 276. The hyperlink takes the unwitting recipient to a website designed to look like a legitimate website of that particular business, and will prompt the user to enter their confidential information, such as passwords and account numbers. *See id.* That information is then used to defraud the user. *See id.*; *see also* U.S. Dep't of Just., Report on Phishing 5 (2006), *available at* http://www.usdoj.gov/opa/report_on_phishing.pdf (citing statistics that as many as 20,000 phishing complaints were reported in August of 2006 alone, an 89% increase from the previous year). Phishing is integrally linked to spam, using unsolicited e-mail as a way to "lure" unsuspecting users to these impostor websites. *See id.* at 6.

[7] *See* Mitchell Zuckoff, *The Perfect Mark: How a Massachusetts Psychotherapist Fell for a Nigerian E-mail Scam*, New Yorker, May 15, 2006, at 36–43. (explaining how a fifty-seven year old ordained minister and Christian psychotherapist lost more than $40,000 and was sen-

As electronic mail ("e-mail") and the Internet have become more and more popular, spam has proliferated at an exponential rate.[8] Neither technological nor legal attempts to curb spam appear to have had any significant or lasting impact.[9] The majority of states and, more recently, Congress have attempted to regulate spam, but their efforts so far have been met with limited success.[10] The difficulties in trying to stop spam and catch its senders (known as spammers) stem from both technological and legislative challenges.[11] The technological challenges arise in part because spammers are very good at hiding themselves, often using viruses and other malware to take over computers of users and trick them into sending more spam.[12] The legislative efforts are complicated by the uncertainty of laws in this area and the difficulties enforcing these laws.[13]

States have attempted to regulate and limit spam without much success.[14] Congress also jumped into the fray in 2003, with the enactment of the Controlling the Assault of Non-Solicited Pornography and

---

tenced to two years in prison after he fell victim to a spam e-mail containing an advance-fee fraud, a swindle whose victims are asked to provide money, information, or services in exchange for a share of a promised fortune).

[8] *See* S. REP. NO. 108-102, at 2, *reprinted in* 2004 U.S.C.C.A.N. 2348, 2349 ("The volume of spam . . . today accounts for over 46 percent of all global e-mail traffic. . . . [I]n September 2001, spam only accounted for 8 percent of all e-mail sent . . . .").

[9] *See* LESSIG, *supra* note 1, at 262–64 ("[T]here's no good evidence the pollution of spam is abating.").

[10] *See, e.g.*, John Soma et al., *Spam Still Pays: The Failure of the CAN-SPAM Act of 2003 and Proposed Legal Solutions*, 45 HARV. J. ON LEGIS. 165, 165–66 (2008); Ford, *supra* note 2, at 356; Hamel, *supra* note 1, at 961.

[11] *See* David Dickinson, Note, *An Architecture for Spam Regulation*, 57 FED. COMM. L.J. 129, 130–31 (2004).

[12] *See* KEN DUNHAM & JIM MELNICK, MALICIOUS BOTS: AN INSIDE LOOK INTO THE CYBER-CRIMINAL UNDERGROUND OF THE INTERNET 1–4 (2009). Viruses and Trojans—malicious programs masquerading as legitimate software—may carry software that allows a remote user to exploit the infected computer, turning it into a "zombie." *See id.* at 4. Such zombies, also known as "bots," are then grouped into "botnets"—large networks of compromised computers that can be controlled by a single individual. *See id* at 1. These computers can then be used for any number of nefarious purposes, such as stealing the unsuspecting victims' credit card information, bringing down websites through denial of service attacks, and sending spam. *See id.* at 57, 58, 63. Spammers may even rent botnets, for as little as $4000 a month. *See id.* at 65; s*ee also* CONSUMER REPORTS, PROTECT YOURSELF ONLINE, STATE OF THE NET '07: NET THREATS—WHY GOING ONLINE REMAINS RISKY 28 (Sept. 2007) (explaining how networks of hijacked computers are used to send the majority of spam).

[13] *See generally* Rita Marie Cain, *When Does Preemption Not Really Preempt? The Role of State Law After CAN-SPAM*, 3 I/S: J.L. & POL'Y FOR INFO. SOC'Y 751 (2008); Michael Bailey, Comment, *The Spam Sham of* White Buffalo Ventures*: A Proposal for Cities and Municipalities to Regulate Spam on a Public Network*, 56 CATH. U. L. REV. 609 (2007); Ford, *supra* note 2.

[14] *See* Ford, *supra* note 2, at 379.

Marketing ("CAN-SPAM") Act.[15] The Act sought to create a uniform, nationwide set of regulations governing unsolicited commercial e-mail.[16] To achieve its goals, the Act preempts some, but not all, state law addressing unsolicited e-mail.[17] The Act preempts mild regulation of spam by the states, substituting in its place a nationwide framework of provisions that senders have to follow.[18] The Act also removes private causes of action and vests enforcement powers with the Federal Trade Commission ("FTC"), the states and their attorneys general, and private Internet Service Providers ("ISPs").[19]

Many critics consider the CAN-SPAM Act ineffective because it not only fails to prohibit or restrict the assault of spam itself, but, by preempting state regulation, it also deprives states of the ability to regulate spam.[20] These critics suggest that unfettered state regulation would stimulate growth and innovation in fighting spam because it would allow states to experiment with different solutions to this problem.[21] The Act, however, does contain an exemption provision, potentially leaving some state laws in place to create stronger remedies for combating spam.[22] The scope of the exemption, and therefore the extent of permissible state regulation, remains unclear.[23]

Additionally, the First Amendment may further limit the power of both the states and the federal government to regulate unsolicited e-mail.[24] A recent ruling by the Supreme Court of Virginia struck down a Virginia statute that criminalized sending unsolicited bulk e-mail because it violated the First Amendment.[25] The statute in question was

---

[15] Controlling the Assault of Non-Solicited Pornography and Marketing Act, 15 U.S.C. §§ 7701–7713 (2006).

[16] *See id.* § 7701 (setting out congressional findings and policy).

[17] *See generally* Ford, *supra* note 2.

[18] 15 U.S.C. § 7707(b)(1) (expressly superseding any state statutes that regulate the use of electronic mail to send commercial messages).

[19] 15 U.S.C. § 7706(d),(f),(g).

[20] *See, e.g.*, Lessig, *supra* note 1, at 264 ("The only federal legislative response, the CAN-SPAM Act, while preempting many innovative state solutions, is not having any significant effect.").

[21] *See* Cain, *supra* note 13, at 775, 776.

[22] 15 U.S.C § 7707(b)(1),(2) (2006) ("This chapter supersedes any statute, regulation, or rule of a State . . . except to the extent that any such statute, regulation, or rule prohibits falsity or deception . . . ."). The exemption provision is called a "savings clause" by some commentators. *See* Ford, *supra* note 2, at 371.

[23] *See, e.g.*, Ford, *supra* note 2, at 374.

[24] U.S. Const. amend. I ("Congress shall make no law . . . abridging the freedom of speech . . . .").

[25] *See* Jaynes v. Commonwealth, 666 S.E.2d 303, 314 (Va. 2008), *cert. denied*, 129 S. Ct. 1670 (2009).

not limited strictly to commercial e-mail and instead forbade sending any unsolicited e-mail with fake or inaccurate delivery information.[26] The court concluded that because such prohibitions can undermine the ability to speak anonymously on the Internet, they are not narrowly tailored to address the interests the statute seeks to protect and are therefore unconstitutional.[27] The U.S. Supreme Court has also invalidated regulations that single out commercial speech where the nature of the speech is unrelated to the legislative interests the regulation is trying to serve.[28] Thus, the CAN-SPAM Act serves as the floor and the First Amendment serves as the ceiling in defining a narrow area where state regulation may be allowed.[29]

This Note will examine what makes spam regulation effective and suggest additional approaches to controlling spam.[30] Part I will explain the underlying problem of unsolicited e-mail, catalog the costs associated with spam, and examine why purely technological attempts to combat spam have failed.[31] Part II will survey the current state and federal approaches to combating spam, and discuss why these approaches have likewise not been completely successful.[32] Specifically, it will explain both the recent interpretation of the preemption provision of the CAN-SPAM Act and the First Amendment concerns that arise in spam regulation.[33] Part III will analyze how the preemption provision of the CAN-SPAM Act and the overbreadth doctrine constrain state action in the area of regulation.[34] It will also reevaluate some fundamental assumptions about spam and how these assumptions affect the efficacy of legislative solutions to the problem of spam.[35] Part IV suggests how courts and legislatures, through flexibility and a realignment of incen-

---

[26] *See id.* at 305–06; *see also* VA. CODE ANN. § 18.2–152.3:1(A)(1) (West 2009) (applying to "any person who (1) Uses [computer networks] with the intent to falsify or forge electronic mail transmission information . . . in connection with the transmission of *unsolicited bulk electronic mail* . . .") (emphasis added).

[27] *See Jaynes,* 666 S.E.2d at 312–13; *see also* McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 357 (1995) ("Under our Constitution, anonymous pamphleteering is not a pernicious, fraudulent practice, but an honorable tradition of advocacy and of dissent. Anonymity is a shield from the tyranny of the majority.").

[28] *See* City of Cincinnati v. Discovery Network, Inc., 507 U.S. 410, 430 (1993).

[29] *See* 15 U.S.C §§ 7701–7713 (2006); *Jaynes,* 666 S.E.2d at 314.

[30] *See infra* notes 37–317 and accompanying text.

[31] *See infra* notes 37–104 and accompanying text.

[32] *See infra* notes 105–212 and accompanying text.

[33] *See infra* notes 115–212 and accompanying text.

[34] *See infra* notes 213–285 and accompanying text.

[35] *See infra* notes 248–285 and accompanying text.

tives, can modify their approach to fighting spam to better address this seemingly unending problem.[36]

I. The Spam Problem & Technological Attempts to Solve It

The widespread use of e-mail and the ease with which spam can be sent combine to create a uniquely challenging problem which imposes costs onto the recipients of spam.[37] Although the problem stems in part from the technological nature of e-mail, so far it has been resistant to technological attempts to remedy it.[38]

A. *Fraud, Obscenity, and Cost: Why Spam Poses a Problem*

Spam presents a problem for the recipient in both direct and indirect ways.[39] The most egregious direct effect of spam is often its fraudulent content, which may include malicious attachments, viruses, links to fraudulent "phishing" websites to steal confidential financial information, and sundry other scams.[40] Additionally, spam serves as a frequent carrier of pornography and other obscene material.[41] Because currently there is no way for spammers to determine the age of the e-mail recipients, minors may receive such objectionable material.[42]

Proponents of spam regulation also argue that spam harms consumers indirectly by raising the cost of e-mail and shifting the advertisers' costs to the recipients.[43] Unlike more traditional forms of advertising, the cost of sending spam is very low for the sender and is borne largely by its recipients, in the form of higher Internet charges, hard-

---

[36] *See infra* notes 286–317 and accompanying text.

[37] *See, e.g.*, Derek E. Bambauer, *Solving the Inbox Paradox: An Information-Based Policy Approach to Unsolicited E-mail Advertising*, 10 Va. J. L. & Tech. 5, ¶¶ 8–14 (2005).

[38] *See* Lessig, *supra* note 1, at 261–62.

[39] *See* Controlling the Assault of Non-Solicited Pornography and Marketing Act, 15 U.S.C. § 7701(a)(3)–(6) (2006); *see also* S. Rep. No. 108-102, at 5–7 (2003), *reprinted in* 2004 U.S.C.C.A.N. 2348, 2351–53 (listing fraudulent schemes, privacy risks, and objectionable content that is transmitted in spam).

[40] *See* Dunham & Melnick, *supra* note 12, at 1–4; McNealy, *supra* note 6, at 275; Zuchoff, *supra* note 7, at 36.

[41] *See* 15 U.S.C. § 7701(a)(5); S. Rep. No. 108–102, at 6 ("[T]he FTC estimates that 18 percent of all spam is pornographic . . . .").

[42] *See* Hamel, *supra* note 1, at 970.

[43] *See* S. Rep. No. 108-102, at 6 (citing a European Union study that found that spam costs Internet subscribers worldwide over nine billion dollars per year); Bambauer, *supra* note 37, ¶¶ 11–12, 11 n.61 (citing research conclusions that spam adds as much as two dollars per month in ISP fees); Soma et al., *supra* note 10, at 169.

ware and software expenses, and productivity costs.[44] ISPs claim that spam congests their networks, slows down the Internet service for all users, and forces ISPs to invest in otherwise unnecessary infrastructure.[45] Businesses, in addition to incurring the costs of network upgrades and spam solutions, also suffer from lost productivity because their employees spend at least some part of the business day sorting through spam.[46] Additionally, spam may disproportionately harm rural e-mail subscribers and business travelers, who pay per-minute connection charges to access their e-mail by dial-up modem.[47]

Lastly, there is an information cost of spam.[48] As more and more legitimate messages get lost amid the unending deluge of spam, e-mail users will be forced to either waste time sifting through the spam or risk missing important messages.[49] Ultimately, e-mail may become so flooded with spam that it will be rendered completely ineffective as a communication medium.[50]

B. *Why Spam Is Hard to Fight: Technology and Terminology*

In order to understand why spam poses a special challenge to regulators and legislators, it is useful to understand the currently existing e-mail technology and the assumptions underlying it.[51] A typical e-mail message consists of a header, body, and, occasionally, attachments.[52] The header contains information such as the message sender's address, the recipients' addresses, and the subject of the message.[53] The body con-

---

[44] *See* Steven Brody & Bruce E.H. Johnson, Advertising and Commercial Speech: A First Amendment Guide § 13:3.2(A) (2d ed. 2008) (estimating the cost to be as high as ten billion dollars per year); *see also* Bambauer, *supra* note 37, ¶¶ 11–12 (explaining associated costs).

[45] *See* S. Rep. No. 108-102, at 6. *But see* White Buffalo Ventures, LLC v. Univ. of Tex., 420 F.3d 366, 375 (5th Cir. 2005) (suggesting that ISP inefficiency is "among the most chronically over-used and under-substantiated interests asserted by parties . . . involved in Internet litigation . . .").

[46] *See* S. Rep. No. 108-102, at 7 (estimating cost to business from spam to be ten billion dollars in 2003).

[47] *See id.* (stating that for rural customers and business travelers, "spam is more than just a loss of time or productivity; it is actually an additional charge . . .").

[48] *See* Bambauer, *supra* note 37, ¶¶ 3–4 (recasting spam as an information problem).

[49] *See* Hamel, *supra* note 1, at 969–70.

[50] *See id.*; *see also* S. Rep. No. 108-102, at 6 ("Left unchecked at its present rate of increase, spam may soon undermine the usefulness and efficiency of e-mail as a communications tool.").

[51] *See* Bambauer, *supra* note 37, ¶ 4.

[52] *See* David H. Crocker, Standard for the Format of APRA Internet Text Messages 4 (1982), *available at* http://www.ietf.org/rfc/rfc822.txt.

[53] *See id.*

tains the main contents of the message.[54] Because senders can specify multiple recipients, they are able to send e-mail to a large number of people very quickly and cost-effectively.[55] Senders are typically not charged per message.[56]

Spammers are able to exploit the trust built into the e-mail protocols.[57] The sender's return address is supposed to correspond to the host computer that sent the message.[58] As the message travels from the sender to the recipient it goes through several e-mail servers, and in doing so, it builds up information about this transmission path, such as the numeric addresses of the servers it went through.[59] Spammers, however, can forge or falsify both the return address and transmission path information to disguise the source of the message, and this false information contributes to the problem of spam and the difficulty in trying to stop it.[60]

Information on the Internet travels in discrete packets of data that are sent to the proper destination by pieces of hardware called routers.[61] Because the Internet was designed to be a decentralized network that could withstand the loss of any one router, the message can take several paths en route from the sender to the recipient.[62] Very little authentication is built into the Internet e-mail protocols, and there is no central server or router that can verify the source or identity of any one message.[63] Although this design leads to a more robust network, it creates vulnerabilities that unscrupulous spammers can exploit.[64]

C. *Attempts to Stop Spam Through Software and Infrastructure*

Not content to wait for the government to address the problem of unsolicited e-mail, the private sector has attempted to decrease the flow of spam with technological approaches.[65] Several of these techniques

---

[54] *See id.*

[55] *See* Bambauer, *supra* note 37, ¶ 11.

[56] *See id.*

[57] *See id.* ¶ 8.

[58] *See* Dickinson, *supra* note 11, at 133.

[59] *See id.* (discussing forwarding of electronic mail by server).

[60] *See* Bambauer, *supra* note 37, ¶ 9; Hamel, *supra* note 1, at 970.

[61] *See* TANENBAUM, *supra* note 2, at 62.

[62] *See* Dickinson, *supra* note 11, at 145.

[63] *See* Bambauer, *supra* note 37, ¶¶ 8–9.

[64] *See id.* ¶ 9.

[65] *See, e.g.*, LESSIG, *supra* note 1, at 261–62. *See generally* ZDZIARSKI, *supra* note 2 (surveying technological approaches to fighting spam).

have been implemented and had varying degrees of impact on spam.[66] Additionally, the FTC evaluated several proposed techniques and concluded that they would be ineffective in controlling the assault of unsolicited e-mail.[67]

1. Existing Techniques: Filters and Blacklists

ISPs use sophisticated filtering software to try to identify spam and either flag or remove it from users' mailboxes.[68] Additionally, private websites create and maintain blacklists—lists of known spammers and ISPs that allow spam to be sent from their servers—which other ISPs use to block offending e-mail messages.[69] Although widely used, both these approaches suffer from several disadvantages that render them an incomplete solution to the problem of spam.[70]

a. *Filtering Spam with Software*

To reduce the amount of unwanted spam in their users' electronic mailboxes, ISPs often use software filters to catch offending messages.[71] These filters use a variety of approaches to try to classify incoming e-mail into two groups: spam and non-spam.[72] Initially relying on simple text matching, these filters have become much more sophisticated, using statistical and probabilistic algorithms to catch even the most clever spammer.[73] Filters can be used by both the ISP and the e-mail recipient, allowing individual users to change personal settings and make the filtering more effective.[74]

As these filters have improved, spammers have become more creative, altering both the subject line and the contents of the messages to make spam seem innocuous, thereby evading the filters.[75] Because most filtering algorithms are based on a probabilistic approach, there are necessarily false positives (non-spam that is flagged as spam) and false

---

[66] *See* ZDZIARSKI, *supra* note 2, at 26–38 (describing filtering, blacklisting, whitelisting, and other techniques).

[67] *See infra* note 87.

[68] *See* S. REP. NO. 108-102, at 6 (2003), *reprinted in* 2004 U.S.C.C.A.N. 2348, 2352.

[69] *See* LESSIG, *supra* note 1, at 263.

[70] *See id.* at 263–64.

[71] *See* Hamel, *supra* note 1, at 973.

[72] *See* ZDZIARSKI, *supra* note 2, at 45.

[73] *See id.* at 49, 63–64.

[74] *See id.* at 26.

[75] *See* LESSIG, *supra* note 1, at 263 (explaining the arms race between filter creators and spammers, who use those filters to ensure their messages can defeat such filters, spurring further filter development).

negatives (spam that is not flagged) created.[76] Because false positives result in legitimate messages potentially being deleted or lost, filters are usually set to be more lenient and disfavor flagging non-spam as spam.[77] Such settings result in looser algorithms that allow more false negatives, inundating users' e-mail boxes with unwanted solicitations.[78]

b. *Blacklisting Known Spammers*

Blacklists represent another weapon in the war on spam.[79] Once a spammer's e-mail or computer address ends up on one of these lists, all e-mail messages from that spammer can be filtered and deleted.[80] Likewise, ISPs that allow anonymous or unauthenticated e-mailing, known as "open relays," can also be blocked by adding them to the blacklist.[81] This technology has the dual benefit of excluding the open relays that send spam and forcing ISPs that do not want to be blacklisted to modify their server settings so as to close the open relays that spammers exploit.[82]

Unfortunately, blacklists are susceptible to the same overinclusive problems as filters.[83] By blocking any e-mail correspondence from ISPs which may have some spam, blacklists often block legitimate, solicited e-mail that happens to come from the same server.[84] Once an e-mail address ends up on such a blacklist, it can be difficult and time-consuming to have it removed, even if the address was added by mistake or is no longer a spam-friendly open relay.[85]

---

[76] *See* Paul Graham, Better Bayesian Spam Filtering (Jan. 2003) (unpublished manuscript, *available at* http://www.paulgraham.com/better.html); *see also* Zdziarski, *supra* note 2, at 46 (describing Bayesian filtering); Mehran Sahami et al., A Bayesian Approach to Filtering Junk E-mail (1998) (unpublished manuscript, *available at* http://robotics.stanford.edu/users/sahami/papers-dir/spam.pdf).

[77] *See* Hamel, *supra* note 1, at 973–74. Hamel describes an extreme case where e-mail messages containing the word "specialist" were being flagged as spam because the word contained within it the word "cialis," a common subject of spam. *Id.*

[78] *See id.*

[79] *See* Lessig, *supra* note 1, at 263; Zdziarski, *supra* note 2, at 27.

[80] *See* Zdziarski, *supra* note 2, at 27.

[81] *See id.* at 28.

[82] *See id.*; *see also* Lessig, *supra* note 1, at 263.

[83] *See* Zdziarski, *supra* note 2, at 28–29.

[84] *See id.*

[85] *See id.*; *see also* Lessig, *supra* note 1, at 263.

2. Other Technology-Based Approaches Rejected by the FTC

The FTC, as mandated by the CAN-SPAM Act,[86] has also investigated several proposed ways to combat spam and has reported to Congress on their viability.[87] These proposals centered on using governmental regulatory agencies—such as the FTC—in cooperation with e-mail users to reduce spam.[88] Some proposals were modeled after successful regulation of other communications media.[89] Due to the underlying architectural limitations of e-mail, however, the FTC found these proposals would be ineffective at best, and at worst could even exacerbate the problem of spam.[90]

a. *A Bounty System to Catch Spammers*

Professor Lawrence Lessig proposed using a well-regulated bounty system, in conjunction with laws requiring accurate labeling of e-mail, to address the problem of spam.[91] If e-mail messages were properly labeled, they could easily be sorted and filtered by software, without the kind of arms race and deception currently created by filtering.[92] In order to enforce such labeling, Lessig proposed creating private bounty hunters who would be "deputized" by the FTC to identify and report mislabeled e-mail.[93] Lessig argued that this system would change incentives for spammers, exposing them (or the entities that use spam to advertise their products) to such liability that would make spam more costly, and therefore less viable.[94]

---

[86] *See* 15 U.S.C. §§ 7709, 7710 (2006).

[87] *See generally* Fed. Trade Comm'n, A CAN-SPAM Informant Reward System: A Report to Congress (2004), *available at* http://www.ftc.gov/reports/rewardsys/040916rewardsysrpt.pdf [hereinafter Informant Reward System Report]; Fed. Trade Comm'n, National Do Not Email Registry: A Report to Congress (2004), *available at* http://www.ftc.gov/reports/dneregistry/report.pdf [hereinafter Do Not Email Registry Report]; Fed. Trade Comm'n, Subject Line Labeling As a Weapon Against Spam: A CAN-SPAM Act Report to Congress (2005), *available at* http://www.ftc.gov/reports/canspam05/050616canspamrpt.pdf [hereinafter Subject Line Labeling Report].

[88] *See* Informant Reward System Report, *supra* note 87, at 1–5; Do Not Email Registry Report, *supra* note 87, at i–ii; Subject Line Labeling Report, *supra* note 87, at i–ii.

[89] *See* Do Not Email Registry Report, *supra* note 87, at 14 (proposing a model based on the success of the Do Not Call Registry).

[90] *See id.* at 15–16 ("A National Do Not Email Registry containing individual e-mail addresses would suffer from a significant security weakness that would enable spammers to treat the Registry as the National *Do* Spam Registry, causing more spam . . . .").

[91] *See* Lessig, *supra* note 1, at 266.

[92] *See id.* at 264.

[93] *See id.* at 266.

[94] *See id.* at 267.

The FTC evaluated such a bounty system and found that it was unlikely to be effective for several reasons.[95] First, spammers use various methods to conceal their identities and the sources of their e-mail messages, making tracking and identifying them more difficult.[96] Second, proving individual spammer liability requires proving elements such as a requisite level of knowledge, a task complicated by the fact that spammers typically distance themselves from illegal activity through decentralized networks.[97] Furthermore, the individuals likely to have high-value information are those who are closely involved with the spammers themselves, such as "insiders" and "whistleblowers."[98] A successful bounty system would aim to encourage these "high-value" individuals to provide information while minimizing "low-value" information from ordinary spam recipients.[99] Designing an incentive system that differentiates between these two types of information is not easy.[100]

b. *National Do Not Spam Registry*

The FTC, per the CAN-SPAM Act's command, also investigated the feasibility of setting up a National Do Not Email Registry, akin to the National Do Not Call Registry.[101] The FTC found that such a registry would be ineffective due to inherent weaknesses in the e-mail protocols, namely lack of authentication and the ability to disguise one's identity.[102] Worse, until such an authentication standard is developed and implemented, the Do Not Email Registry would turn into a *Do* Email Registry, allowing spammers to harvest valid e-mail addresses of individuals.[103] The FTC recommended a series of steps that would help it establish a Do Not Email Registry, such as mandating an authentica-

---

[95] *See* Informant Reward System Report, *supra* note 87, at 28 (noting that the costs of a reward system may outweigh the benefits from it).

[96] *See id.* at 11.

[97] *See id.* at 16.

[98] *See id.* at 26.

[99] *See id.* at 23.

[100] *See id.* at 37.

[101] *See* 15 U.S.C. § 7708(a) (2006). The National Do Not Call Registry was set up by the Federal Communications Commission, pursuant to the Telephone Consumer Protection Act of 1991. 47 U.S.C. § 227 (2006). The U.S. Court of Appeals for the Tenth Circuit upheld the constitutionality of the Registry, finding that it was narrowly tailored because it only restricted speech aimed at unwilling recipients. *See* Mainstream Mktg. Servs., Inc. v. FTC, 358 F.3d 1228, 1242 (10th Cir. 2004).

[102] *See* Do Not Email Registry Report, *supra* note 87, at 8, 34.

[103] *See id.* at 15–16, 17 (calling any such registry a "Fort Knox" list for the criminal spammer).

tion standard, but it is unlikely that these recommendations will be implemented in the near future.[104]

II. Legislative Efforts to Reduce Spam

The failure of technological solutions alone to check the exponential increase in spam and the rejection of governmental regulatory solutions as ineffective have led to an increased interest in addressing the spam problem at a legislative and judicial level.[105] Both the states and Congress have responded to the call to reduce spam, and both have been less than successful.[106]

A. *State Legislation to Reduce Spam*

Nevada became the first state to pass laws regulating and prohibiting the sending of unsolicited commercial electronic mail in 1997, and an increasing number of states followed suit shortly thereafter.[107] By 2004, when the federal CAN-SPAM Act went into effect, thirty-six states had some type of anti-spam law.[108]

States varied in their approaches to regulating spam.[109] Some states passed strict opt-in laws, requiring the user to essentially subscribe to receiving unsolicited e-mail; whereas others mandated clear labeling in the subject lines to make filtering more accurate; still others relied on opt-out provisions.[110] Some states created a cause of action for an individual to sue a spammer under the state statute or regulation.[111]

It remains unclear why these state laws were ineffective in reducing the volume of spam.[112] Some courts have suggested that disparate state laws made compliance impractical because of the nature of e-mail itself.[113] Other scholars have argued that stronger state laws would have

---

[104] *See id.* at 36–37.

[105] *See* Lessig, *supra* note 1, at 262–63.

[106] *See, e.g.*, Zdziarski, *supra* note 2, at 23 (noting that the CAN-SPAM Act has not had a significant effect on spam); Ford, *supra* note 2, at 356.

[107] *See* Hamel, *supra* note 1, at 976.

[108] *See id.*; *see also* David E. Sorkin, Summary of Spam Laws, http://spamlaws.com/state/summary.shtml (last visited Nov. 4, 2009) (containing a comprehensive list of state spam laws).

[109] *See* Hamel, *supra* note 1, at 976–79.

[110] *See id.* at 976–78.

[111] *See* Cain, *supra* note 13, at 773 (noting that most state anti-spam laws provide attorney's fees in addition to providing private causes of action).

[112] *See* 15 U.S.C. § 7701(a)(11) (2006).

[113] *See* Omega World Travel, Inc. v. Mummagraphics, Inc., 469 F.3d 348, 355 (4th Cir. 2006). A sender cannot determine the geographic location of the recipient from their e-

been more effective had they not been preempted by the passage of the comprehensive federal law.[114]

B. *The Federal CAN-SPAM Act and Its Preemption of State Law*

Recognizing the need for uniform regulation, Congress enacted the CAN-SPAM Act in 2003, which President George W. Bush signed into law.[115] The Act contains several provisions to deal with the onslaught of unsolicited commercial e-mail, such as prohibiting messages with materially false or misleading header information,[116] prohibiting misleading subject lines,[117] and providing recipients with the ability to opt out of receiving such messages.[118] Although some of these provisions are similar to their state-law counterparts, they are generally considered to be weaker.[119]

The Supremacy Clause of the Constitution gives Congress the power to preempt state law in a particular field of regulation.[120] The CAN-SPAM Act contains an express preemption clause, whereby it "supersedes any statute, regulation, or rule of a State or political subdivision of a State that expressly regulates the use of electronic mail to send commercial messages, except to the extent that any such statute, regulation or rule prohibits falsity or deception in any portion of a commercial electronic mail message."[121] This type of preemption, embodied in the first clause of the provision, is the clearest expression of

---

mail address, and therefore a sender must either comply with the strictest state law in any state, or risk inadvertently violating the law. *See id.* at 355, 356.

[114] *See* Hamel, *supra* note 1, at 978–79. Some commentators have suggested that fear of strong state legislation, such as "opt-in" provisions, may have been an impetus for the CAN-SPAM Act, and that several marketing industry groups lobbied Congress to pass a weaker national bill. *See, e.g.*, Stefanie Olsen, *Ad Groups Lobby for Antispam Law*, CNET NEWS, Nov. 13, 2003, http://news.cnet.com/Ad-groups-lobby-for-antispam-law/2100–1024_3–5107059.html; Andrea Stone, *Marketers Trying to Influence Congress on Spam*, USA TODAY, Nov. 10, 2003, http://www.usatoday.com/news/washington/2003–11–10-spam-congress_x.htm ("[Lobbyists fear] a tough anti-spam law will destroy the Internet as a burgeoning marketplace . . . ."). Additionally, such strong laws may not survive a constitutional challenge. *See* Hamel, *supra* note 1, at 979.

[115] *See* 15 U.S.C §§ 7701–7713.

[116] *Id.* § 7704(a)(1).

[117] *Id.* § 7704(a)(2).

[118] *Id.* § 7704(a)(5).

[119] *See* Soma et al., *supra* note 10, at 165–66. For instance, the CAN-SPAM Act does not create a cause of action for an individual aggrieved by receiving unsolicited e-mail, instead giving a cause of action only to certain federal agencies, states, and ISPs. *See* 15 U.S.C. § 7706; *see also Mummagraphics*, 469 F.3d at 357 n.3.

[120] U.S. CONST. art. VI, cl. 2.

[121] 15 U.S.C. § 7707(b)(1).

congressional intent to supersede state law, but still requires judicial interpretation as to both the scope and the effect of preemption.[122]

1. Exemption of Some State Laws from the CAN-SPAM Act

While this provision of the Act appears to expressly preempt any prior state regulation of spam, there are three important qualifications.[123] First, only state regulation of commercial e-mail is preempted.[124] This limitation suggests that state regulation of electronic mail that is not strictly commercial may survive preemption.[125] Second, the CAN-SPAM Act preserves state statutes and regulations if they deal with falsity or deception in e-mail messages.[126] This exemption, embodied in the second clause of the provision, may leave substantial state law in place, depending on how broadly the scope of the exemption is interpreted.[127] Lastly, because the Act exempts ISPs, Congress may have intended to allow state entities operating as ISPs to regulate spam as they see fit.[128]

Courts have differed over the interpretation of the exemption, and subsequently, over which law—state or federal—governs the cause of action.[129] Such decisions have significant implications for spam regulation because state and federal laws vary widely with respect to elements like standing and available remedies.[130] Thus, the applicability *vel non* of

---

[122] *See* Ford, *supra* note 2, at 366–67.

[123] *See* 15 U.S.C. § 7707(b),(c).

[124] *See* 15 U.S.C. § 7707(b)(1) ("This chapter supersedes any statute, regulation, or rule of a State or political subdivision of a State that expressly regulates the use of electronic mail to send *commercial* messages . . . .") (emphasis added).

[125] *See* Jaynes v. Commonwealth, 666 S.E.2d 303, 313 (Va. 2008), *cert. denied*, 129 S. Ct. 1670 (2009). Broad regulation of electronic mail by the states, however, may nonetheless encounter other challenges. *See infra* notes 171–212 and accompanying text.

[126] *See* 15 U.S.C. § 7707(b)(1) (stating that the CAN-SPAM Act preempts state statutes "except to the extent that any such statute . . . *prohibits falsity or deception* in any portion of [an e-mail] message") (emphasis added).

[127] *Compare Mummagraphics*, 469 F.3d at 348 (holding that the CAN-SPAM Act preempts state law), *with* Beyond Sys., Inc. v. Keynetics, Inc., 422 F. Supp. 2d 523 (D. Md. 2006) (upholding state law because it compliments the purposes of the CAN-SPAM Act).

[128] *See* White Buffalo Ventures, LLC v. Univ. of Tex., 420 F.3d 366, 369 (5th Cir. 2005) (holding that a state university that provides e-mail to its students was exempt from the CAN-SPAM Act under that provision). Congress may not have anticipated this effect when drafting the Act. *See id.* at 373–74.

[129] *See Mummagraphics*, 469 F.3d at 356; *Beyond Sys.*, 422 F. Supp. 2d at 538.

[130] *See* 15 U.S.C. § 7706; *Mummagraphics*, 469 F.3d at 356. For example, individuals do not have standing under the CAN-SPAM Act to bring suits against spammers, but may have such standing under state laws. *See Beyond Sys.*, 422 F. Supp. 2d at 538.

state laws turns on how broadly courts interpret the phrase, "falsity or deception in any portion of a commercial electronic mail message."[131]

a. Beyond Systems, Inc. v. Keynetics, Inc.*: A Broad Reading of Exemption*

In 2006, the U.S. District Court for the District of Maryland took a broad reading of the exemption provision in *Beyond Systems, Inc. v. Keynetics, Inc.*, when it held that the Maryland Commercial Electronic Mail Act ("MCEMA") was not inconsistent with the CAN-SPAM Act.[132] MCEMA, like the CAN-SPAM Act, prohibits the use of false or misleading information about the origin or the transmission path of commercial e-mail messages, as well as messages which contain false or misleading subject lines.[133] The plaintiff, Beyond Systems, Inc. ("BSI") alleged that it received over 6000 e-mail messages from the defendants, all of which were false and misleading with regard to either their origin, transmission path, or subject line information.[134] BSI also alleged that the defendant spammers conspired to send such unsolicited bulk e-mail in violation of the MCEMA.[135]

The court, relying in part on other state law decisions, held that because the MCEMA regulated falsity and deception in the e-mail message and did not frustrate the goals of the federal legislation, it fit under the exemption to the CAN-SPAM Act.[136] Furthermore, because the statute made it illegal to conspire, to initiate, or to assist in the transmission of unsolicited e-mail, the court allowed the action to proceed, as there was no equivalent to the conspiracy or assistance element under the federal Act.[137] The court found that the civil remedies provided

---

[131] *See* 15 U.S.C. § 7707(b)(1); *Mummagraphics*, 469 F.3d at 356; *Beyond Sys.*, 422 F. Supp. 2d at 538.

[132] *See* 422 F. Supp. 2d at 538.

[133] Md. Code Ann., Com. Law § 14-3002(b) (LexisNexis Supp. 2004); *see generally* MaryCLE, LLC v. First Choice Internet, Inc., 890 A.2d 818 (Md. App. 2006) (interpreting MCEMA).

[134] *See Beyond Sys.*, 422 F. Supp. 2d at 528. BSI was described by the court as an ISP, and therefore would have standing under the CAN-SPAM Act without the need to resort to state statutes. *See id.* The district court, however, read the MCEMA to provide a civil remedy to individuals who are not ISPs as well. *See id.* at 535.

[135] *See id.* at 528.

[136] *See id.* at 535, 538 ("[I]t is readily apparent that MCEMA . . . *is in no way inconsistent with CAN-SPAM.* At most it supplements the federal law. . . . [T]he preemption doctrine simply does not apply."). The court found that the plaintiff had pled the elements of falsity with sufficient particularity to fall under the state law provision. *See id.* at 541–42.

[137] *See id.* at 538.

by the state were "fully in harmony with CAN-SPAM's enforcement mechanisms."[138]

Such a broad interpretation of the "falsity or deception" element of the exemption provision may be problematic.[139] At best, it supplements the CAN-SPAM Act with the full array of state legislation aimed to protect the recipients.[140] At worst, such an overinclusive interpretation completely eviscerates the Act, rendering it irrelevant.[141]

b. Omega World Travel, Inc. v. Mummagraphics, Inc.*: A Narrow Reading*

In contrast, the U.S. Court of Appeals for the Fourth Circuit took a narrow view of the exemption provision in the CAN-SPAM Act in *Omega World Travel, Inc. v. Mummagraphics, Inc.* in 2006.[142] Mummagraphics was an Oklahoma corporation that received unsolicited e-mail messages advertising vacation packages.[143] The headers in these messages were alleged to have false and misleading information, but the body of the message contained an electronic opt-out link, as well as a mailing address to which the recipient could write to ask to be removed from the electronic mailing list.[144] Mummagraphics, in bringing suit under both the CAN-SPAM Act and an Oklahoma statute governing false and misleading electronic mail, argued that state law was not preempted because the CAN-SPAM Act allows states to prohibit falsity and deception.[145]

In its analysis of whether the Oklahoma law was preempted by the CAN-SPAM Act, the Fourth Circuit looked to Congress's purpose in enacting the Act.[146] The court found that although these were indeed inaccuracies in the message, they did not make the message "materially false or materially misleading."[147] Reasoning that Congress' enactment of the CAN-SPAM Act was not intended to create a strict liability stan-

---

[138] *See id.*

[139] *See id.* at 535 ("Getting the State Attorney General to undertake an action [under CAN-SPAM] against . . . out-of-state spammers is much easier said than done."); *cf.* Donald G. Gifford, *Impersonating the Legislature: State Attorneys General and* Parens Patriae *Product Litigation*, 49 B.C. L. REV. 913, 919 (2008) (questioning whether "our constitutional framework vests [enforcement] power in state attorneys general").

[140] *See Beyond Sys.*, 422 F. Supp. 2d at 535–36.

[141] *See Mummagraphics*, 469 F.3d at 355–56.

[142] *See id.* at 354.

[143] *See id.* at 350–51.

[144] *See id.* at 351.

[145] *See id.* at 350, 353. Because Mummagraphics was considered an ISP, it was able to bring suit under the CAN-SPAM Act. *See id.* at 357 n.3.

[146] *See id.* at 355.

[147] *Mummagraphics*, 469 F.3d at 354.

dard for errors, the court held that allowing the Oklahoma law to coexist with the CAN-SPAM Act would have precisely that effect.[148] The expansive multi-state nature of spam makes it likely that those wanting to comply with spam regulations would have to comply with the strictest provisions, thereby imposing this standard onto all other states.[149] Because the message bodies contained information on how to identify and contact the sender, the court held that the alleged inaccuracies could not have impaired any party from raising a CAN-SPAM claim to find the offending company and presumably opt out of further mailings.[150] Therefore, the plain intent of Congress in passing the CAN-SPAM Act was to preempt the Oklahoma law and consequently an action under such law could not be maintained.[151]

Because the CAN-SPAM Act does not create a private cause of action, such a narrow reading of the "false or misleading" element effectively prevents individuals from suing under their state laws except where such falsity rises to the level of being "material."[152] As a result, the Fourth Circuit's *Mummagraphics* decision has been criticized as frustrating consumers' self-help measures and favoring spammers over spam recipients.[153] But, because Congress was aware of private rights of action and purposely chose to exclude them from the CAN-SPAM Act, the Fourth Circuit's interpretation of the preemption clause is arguably more in agreement with congressional intent.[154]

2. Unanticipated Consequences of the CAN-SPAM Act

The exemption provision of the Act, for better or worse, creates an unforeseen possibility for state or municipal regulation of spam.[155] Be-

---

[148] *See id.*

[149] *See id.* at 356.

[150] *See id.* at 358.

[151] *See id.* at 355. The court further found that errors in the spam were not actionable under the CAN-SPAM Act because they were not substantial enough to make the headings "materially false or materially misleading." *See id.* at 357.

[152] *See id.* at 359 ("The CAN-SPAM Act . . . does not make every error or opt-out request into grounds for a lawsuit."); *cf.* Michael K. Avery, *Whose Rights? Why States Should Set the Parameters for Federal Honest Services Mail and Wire Fraud Prosecutions*, 49 B.C. L. Rev. 1431, 1442 (2008) (describing circuit court precedent where violation of underlying state law was used as a basis for federal wire and mail fraud prosecution).

[153] *See* Katherine Wong, *The Future of Spam Litigation After* Omega World Travel v. Mummagraphics, 20 Harv. J. L. & Tech 459, 476–77 (2007).

[154] *See Mummagraphics*, 469 F.3d at 355–56.

[155] *See* Bailey, *supra* note 13, at 611.

cause the Act does not affect the policies of ISPs,[156] a state acting as an ISP, not a regulator, would be allowed to implement technological policies that are not specified by the CAN-SPAM Act.[157] This may allow a state actor to continue experimenting with different approaches to fighting spam, such as requiring subject-line labeling, rejecting e-mail from blacklisted senders, and more drastic measures, like blocking all unsolicited e-mail—effectively requiring users to opt-in to receive messages from particular senders.[158]

This approach is seen in *White Buffalo Ventures, LCC v. University of Texas*, where, in 2005, the U.S. Court of Appeals for the Fifth Circuit held that the University of Texas fell within the ISP exemption because it provided e-mail accounts and e-mail access to students and faculty.[159] In that case, White Buffalo, an online dating site targeting college students, sent several e-mail blasts to the University of Texas community, prompting complaints.[160] Although the e-mails complied with the CAN-SPAM Act, the University nonetheless decided to block further incoming e-mail originating from the specific addresses used by White Buffalo.[161] White Buffalo argued that because its spam was not fraudulent and complied with the requirements of the CAN-SPAM Act, that the University—a "political subdivision" of the state for CAN-SPAM purposes—could not create rules that authorized the use of filters to block the spam.[162]

The Fifth Circuit, however, refused to apply preemption where the University of Texas was both an ISP and a state actor, concluding that the ambiguity in the CAN-SPAM Act exempted state-run ISPs from its purview and allowed them to implement filtering rules.[163] By expressly preempting state regulation while at the same time expressly exempting Internet providers from preemption, Congress failed to take into

---

[156] *See* 15 U.S.C. § 7707(c) (2006) ("Nothing in this chapter shall be construed to have any effect on the lawfulness or unlawfulness . . . of the adoption, implementation, or enforcement *by a provider of Internet access service* of a policy of declining to transmit, route, relay, handle, or store certain types of electronic mail messages.") (emphasis added).

[157] *See White Buffalo*, 420 F.3d at 373.

[158] *See* Jason A. Smith, Comment, *Spam (Supremacy Clause, Public Forums, and Mailings): The Fifth Circuit's Interpretation of the CAN-SPAM Act in* White Buffalo v. University of Texas, 38 ST. MARY'S L.J. 553, 588 (2007).

[159] *See White Buffalo*, 420 F.3d at 373.

[160] *See id.* at 369.

[161] *See id.* at 369 & n.5.

[162] *See id.* at 371.

[163] *See id.* at 372–73.

account situations where those two entities are one and the same.[164] The court was therefore unwilling to overrule the typically strong "presumption against preemption of state law" where the plain language of the statute created such ambiguity.[165]

This interpretation leaves open the possibility that states and their subdivisions who want to regulate spam may do so by becoming ISPs.[166] Many cities and municipalities planning to provide Internet access to their residents may find such an approach attractive.[167] This solution has been criticized, however, as frustrating congressional intent in passing the CAN-SPAM Act.[168] Other commentators suggest that states should not compete with private e-mail providers—thereby angering a potential ally in the fight against spam—and should instead encourage private advancement in technology.[169] Such criticisms are somewhat circular because neither the CAN-SPAM Act nor private efforts to stem the tide of spam have been successful.[170]

C. *Constitutional Concerns*

Regulation of spam, and of e-mail in general, may raise constitutional concerns because the First Amendment prohibits federal and state governments from making laws abridging the freedom of speech.[171] The U.S. Supreme Court, however, has recognized that the government's interest in regulating some commercial speech may outweigh First Amendment concerns and commercial speech may be entitled to fewer protections.[172] This speech is afforded less protection because it typically occurs in the context of commercial transactions, which are traditionally subject to more government regulation and more prone to fraud.[173]

---

[164] *See id.* The court "doubt[ed] that . . . legislators responsible for passing the [Act's definition of ISPs] gave serious consideration" to the possibility of a state actor and an ISP being one and the same. *See id.* at 373.

[165] *See White Buffalo*, 420 F.3d at 370 & n.9, 373–74.

[166] *See* Bailey, *supra* note 13, at 610–12.

[167] *See id.* at 611; *see also* Julia DiPasquale, Comment, *Currents: Cities Providing Wi-fi to Residents—Broadband Socialism or Wireless Freedom*, Univ. of Pitt. J. of Tech L. & Pol'y, Feb. 16, 2007, http://tlp.law.pitt.edu/SP_DiPasquale_BroadbandSocialism.htm; Anna Broache, *Senators Can't Agree on Municipal Broadband Rules*, Cnet News, Feb. 15, 2006, http://news.cnet.com/Senators-cant-agree-on-municipal-broadband-rules/2100-1034_3-6039636.html.

[168] *See* Smith, *supra* note 158, at 573–74.

[169] *See* Bailey, *supra* note 13, at 644.

[170] *See* Soma et al., *supra* note 10, at 165; Ford, *supra* note 2, at 356.

[171] U.S. Const. amend. I; *see* Gitlow v. New York, 268 U.S. 652 (1925) (applying First Amendment protections to the states).

[172] *See* Bolger v. Youngs Drug Prods. Corp., 463 U.S. 60, 64–65 (1983).

[173] *See* Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n, 447 U.S. 557, 562–63 (1980).

1. The *Central Hudson* Test: Regulation of Commercial Speech

Because commercial speech is based on a more economic—rather than expressive—interest, commercial speech that deceives the public may be banned or restricted.[174] Thus, the government may regulate false, deceptive, or misleading commercial speech without running afoul of the First Amendment, and may likewise prohibit commercial speech related to illegal behavior.[175]

In *Central Hudson Gas & Electric Corp. v. Public Service Commission*, the U.S. Supreme Court first articulated a four-part test to determine whether commercial speech is protected by the First Amendment: 1) whether the speech concerns lawful activity and is not misleading; 2) whether the asserted governmental interest is substantial; 3) whether the regulation directly advances the governmental interest asserted; and 4) whether there is a "reasonable fit" between the regulation and the interest it aims to serve.[176] The burden falls on the party seeking to restrict commercial speech to justify such a restriction.[177]

2. Applying the *Central Hudson* Test to Spam Regulation

Spam that is fraudulent, misleading, or unlawful falls outside the scope of the First Amendment and may therefore be prohibited.[178] Regulation of non-fraudulent or lawful spam must meet the other three requirements of the *Central Hudson* test.[179] To meet the second element of the test, the party seeking to regulate spam must show a government interest in restricting commercial speech.[180] In the case of spam regulation, the government interest usually centers on the direct and indirect costs to e-mail users.[181] Government regulations that directly advance this specific interest satisfy the third element of the *Central Hudson*

---

[174] *See id.* at 563.

[175] *See Bolger*, 463 U.S. at 69.

[176] *See* Bd. of Trs. v. Fox, 492 U.S. 469, 476, 480 (1989) (modifying the fourth prong of the *Central Hudson* test); *Cent. Hudson*, 447 U.S. at 564.

[177] *Bolger*, 463 U.S. at 71 n.20 (citing *Cent. Hudson*, 447 U.S. at 570).

[178] *See Cent. Hudson*, 447 U.S. at 562–63 ("The First Amendment's concern for commercial speech is based on the informational function of advertising. Consequently, there can be no constitutional objection to the suppression of commercial messages that do not accurately inform the public about lawful activity.") (internal citation omitted).

[179] *See White Buffalo*, 420 F.3d at 374 (proceeding with the *Central Hudson* test because White Buffalo's spam was legal and contained factually accurate information).

[180] *See, e.g.*, 15 U.S.C. § 7701(a) (2006).

[181] *See supra* notes 39–50 and accompanying text. In *White Buffalo*, the University put forth two main arguments, that of "user efficiency" and "server efficiency," which roughly correspond to the direct and indirect costs of spam. *See* 420 F.3d at 374–75.

test.[182] It is generally easy to show that regulation of spam directly advances the interest of lowering costs imposed on e-mail users by spam.[183] Lastly, there must be a reasonable fit between the legislation's goal of reducing spam and the means chosen to achieve that goal.[184] Although this issue has not yet come up in the context of spam, dictum in the *White Buffalo* decision suggests that too much singling out of commercial speech may run into constitutional limitations.[185]

Although the Supreme Court has yet to rule on the constitutionality of the CAN-SPAM Act, it has been upheld by several lower courts.[186] According to these courts, several factors contribute to its constitutionality.[187] First, because Congress may freely regulate or prohibit false or fraudulent spam, provisions of the CAN-SPAM Act prohibiting false or misleading transmission information and deceptive subject headings will surely survive constitutional scrutiny.[188] Second, the Act is limited to commercial spam, an area that Congress has a significant interest in regulating, due to spam's enormous economic impact.[189] Third, such regulation aims to promote this interest by reducing the costs of spam.[190] Lastly, because the CAN-SPAM Act does not prohibit, but merely seeks to regulate, the transmission of spam, it is likely to satisfy

---

[182] *See Cent. Hudson*, 447 U.S. at 566.

[183] *See* Vivek Arora, *The CAN-SPAM Act: An Inadequate Attempt to Deal with a Growing Problem*, 39 COLUM. J.L. & SOC. PROBS. 299, 305 (2006); *see also White Buffalo*, 420 F.3d at 375.

[184] *See Fox*, 492 U.S. at 480.

[185] *See White Buffalo*, 420 F.3d at 376 ("We reject, however, the proposition that the [spam-blocking] policy is no more extensive than necessary to secure the state's . . . substantial interest, which is the efficiency of its *servers*."). The court indicated that such a policy, which blocked all of White Buffalo's spam, may not be a reasonable fit to the University's stated goals of promoting server efficiency because other alternatives, such as restricting commercial spam to off-peak hours, may be less restrictive and more constitutionally acceptable. *See id.* at 377. Such reasoning may pose challenges to state regulation of spam as the Supreme Court has also struck down commercial speech regulation when it seems unrelated to the interest asserted by the state. *See* City of Cincinnati v. Discovery Network, Inc., 507 U.S. 410, 428 (1993) (holding that, despite the nuisance factor posed by news racks on streets, the city could not make commercial publications bear the entire brunt of the regulation, because news racks created safety and aesthetic blights regardless of their content, and the notion that commercial speech is per se less important could not justify such a restriction).

[186] *See, e.g.*, *Mummagraphics*, 469 F.3d at 359; *White Buffalo*, 420 F.3d at 378.

[187] *See White Buffalo*, 420 F.3d at 374–78.

[188] *See* 15 U.S.C. § 7704(a)(1), (2) (2006); *Cent. Hudson*, 447 U.S. at 562–63.

[189] *See* 15 U.S.C. § 7701(a)(3)–(5); S. REP. NO. 108-102, at 3–7 (2003), *reprinted in* 2004 U.S.C.C.A.N. 2348, 2349–54 (detailing Congressional findings of fact about the cost of spam to consumers, businesses, and ISPs).

[190] *See* S. REP. NO. 108-102, at 7–8 (explaining how the CAN-SPAM Act tries to address the problem of spam).

the "reasonable fit" requirement because it is less restrictive than a total ban on spam.[191]

3. Overbreadth, Anonymity, and the Limits of Speech

Because spam necessarily implicates speech concerns, additional First Amendment limitations—apart from commercial speech doctrines—may affect the constitutionality of spam regulation.[192] Specifically the overbreadth doctrine, which allows courts to facially invalidate a statute even though it would be valid as it applied to a particular defendant, may serve to invalidate spam regulation.[193]

a. *The Overbreadth Doctrine, Spam, and Commercial Speech*

The overbreadth doctrine is needed in the First Amendment context because the threat of enforcement of an unconstitutional statute may "chill" otherwise protected speech.[194] This doctrine, however, is considered "strong medicine" because it creates an exception to the general rule that a person may not challenge a statute that is constitutional when applied to them merely because it is unconstitutional when applied to others.[195] The potentially vast reach of the overbreadth doctrine is limited in three significant ways.[196] First, the overbreadth must be substantial when judged in relation to the statute's plainly legitimate sweep, and the doctrine's reach attenuates as the behavior in question moves from "pure speech" into conduct which falls within otherwise valid criminal laws.[197] Second, the doctrine does not typically apply to commercial speech, least of all to commercial speech that proposes an unlawful or fraudulent transaction.[198] Third, the statute in question can

---

[191] *Compare Jaynes*, 666 S.E.2d at 313 (prohibiting complete ban of unsolicited e-mail), *with Mummagraphics*, 469 F.3d at 359 (allowing regulation of commercial e-mail).

[192] *See Jaynes*, 666 S.E.2d at 313, 314.

[193] *See id.* at 314; *see also* United States v. Williams, 128 S. Ct. 1830, 1838 (2008).

[194] *See* Broadrick v. Oklahoma, 413 U.S. 601, 612 (1973).

[195] *See Williams*, 128 S. Ct. at 1838 ("[I]nvalidating a law that in some of its applications is perfectly constitutional—particularly a law directed at conduct so antisocial that it has been made criminal—has obvious harmful effects.").

[196] *See id.*

[197] *See id.*; *Broadrick*, 413 U.S. at 615.

[198] *See* Bates v. State Bar of Ariz., 433 U.S. 350, 380 (1977) ("[T]he justification for the application of overbreadth analysis applies weakly, if at all, in the ordinary commercial context."). Commercial speech is thought to be hardy enough to withstand overly broad statutes because of the "economic self-interest" of the speaker to continue speaking. *See Cent. Hudson*, 447 U.S. at 564 n.6.

often be saved through a narrowing construction to avoid the overbroad effect on speech.[199]

Thus, statutes that aim to not just regulate, but to effectively eliminate, broad categories of spam may run afoul of the overbreadth doctrine.[200] The state of Virginia took such a broad approach in attempting to control spam: it criminalized the sending of unsolicited bulk electronic mail with falsified or forged transmission information.[201] Unlike Congress and other states, Virginia chose not to limit its statute strictly to commercial spam, applying it instead to all unsolicited bulk e-mail.[202] Thus speech that is non-commercial in nature could have subjected its sender to criminal penalties if it was sent to recipients in Virginia and contained false header information obscuring the identity of the sender.[203]

b. Jaynes v. Commonwealth*: The Limit of Spam Regulation*

Jeremy Jaynes, a notorious spammer from North Carolina,[204] was prosecuted and convicted under the Virginia statute for sending over 10,000 e-mail messages to users of America Online.[205] On appeal, Jaynes raised the claim that the Virginia statute was unconstitutionally overbroad because it impermissibly restricted anonymous speech.[206] After a rehearing in 2008, the Supreme Court of Virginia agreed, and in *Jaynes v. Commonwealth* struck down the statute because it prohibited

---

[199] *See Williams*, 128 S. Ct. at 1846.

[200] *See, e.g.*, CAL. BUS. & PROF. CODE § 17529.2 (West 2008) (requiring users to opt-in to receiving spam); Hamel, *supra* note 1, at 979 (suggesting this requirement would face constitutional challenge).

[201] VA. CODE ANN. § 18.2–152.3:1 (West 2008) (prohibiting all unsolicited e-mail with falsified transmission information, regardless of its commercial nature). Virginia is home to AOL, a large and heavily spammed ISP. *See* Zachary A. Goldfarb & Sam Diaz, *AOL Moving Executives, Headquarters to New York*, WASH. POST, Sept. 18, 2007, at A1.

[202] *See* VA. CODE ANN. § 18.2–152.3:1(A)(1) (applying to "any person who (1) Uses [computer networks] with the intent to falsify or forge electronic mail transmission information . . . in connection with the transmission of *unsolicited bulk electronic mail* . . .") (emphasis added).

[203] *See* VA. CODE ANN. § 18.2–152.3:1(B) (defining felony offenses under the statute).

[204] *See* Candace Rondeaux, *Anti-Spam Conviction Is Upheld*, WASH. POST, Sep. 6, 2006, at B3.

[205] *See Jaynes*, 666 S.E.2d at 305. Jaynes tried to conceal his identity by falsifying the header information in the e-mails, but was nonetheless discovered through the use of a sophisticated investigative database. *Id.* at 305 & n.4. He was eventually sentenced to a total of nine years in prison. *Id.* at 306. His conviction was initially affirmed, but after his petition for rehearing was granted, the court reversed the conviction and held the Virginia statute to be unconstitutional. *Id.* at 303 n.1.

[206] *See id.* at 308.

the anonymous transmission of *all* unsolicited bulk e-mail.[207] The court found that the statute would thus ban e-mail messages containing political, religious, or other types of speech protected by the First Amendment.[208]

The *Jaynes* court did not dispute that the statute was enacted to control predominantly unsolicited commercial e-mail.[209] The court concluded that the statute was substantially overbroad on its face because it could impermissibly restrict core protected speech, such as political or religious speech.[210] Specifically, the statute would ban anonymous noncommercial speech and in this regard it was unconstitutional.[211] Furthermore, no reasonable interpretation would narrow the statute enough to save its constitutionality and the court refused to encroach on the province of the legislature by essentially rewriting it.[212]

III. An Analysis of the Existing Framework for Spam Regulation & a Reevaluation of Some Underlying Assumptions

States seeking to regulate spam are thus faced with a dilemma.[213] If their statutes are narrowly drafted to regulate only unsolicited commercial e-mail, such statutes may be preempted by the CAN-SPAM Act, which deprives states of the ability to impose stricter requirements, tougher sanctions, or grant private rights of action to their citizens.[214] Even if regulations only concern false or misleading message information, the narrow reading of the falsity exemption in *Omega World Travel, Inc. v. Mummagraphics, Inc.* may effectively render state anti-spam laws preempted.[215] Such a narrow interpretation would permit deceptive subject lines and false sender addresses as long as the body of the spam

---

[207] *See id.* at 314.

[208] *See id.* at 312.

[209] *See id.* at 313.

[210] *See id.*

[211] *See Jaynes*, 666 S.E.2d at 314. The court, drawing an analogy to the publication of the *Federalist Papers*, found that this statute would prohibit their dissemination by e-mail and that such expansive scope of the statute is unconstitutional. *See id.*

[212] *See id.*

[213] *See* Omega World Travel, Inc. v. Mummagraphics, Inc., 469 F.3d 348, 359 (4th Cir. 2006); Jaynes v. Commonwealth, 666 S.E.2d 303, 314 (Va. 2008), *cert. denied*, 129 S. Ct. 1670 (2009).

[214] *See Mummagraphics*, 469 F.3d at 359 ("[A]llowing a state to attach liability [through their spam statutes] would be inconsistent with the Federal Act . . . .").

[215] *See supra* notes 142–154 and accompanying text.

contained some correct information, such as a mailing address where one could send requests to unsubscribe.[216]

Alternatively, if states draft broad statutes that escape preemption, they risk violating the First Amendment.[217] Even legislation regulating false or misleading sender information may not be actionable because, as the *Jaynes v. Commonwealth* court noted, the right to engage in anonymous speech is constitutionally protected.[218] Thus states that want to continue experimenting with novel approaches to safeguarding their citizens from spam need to exercise caution in drafting specific provisions broad enough to be meaningful alongside the CAN-SPAM Act, while narrow enough to be constitutional.[219]

A. *Existing Options for Regulation*

1. The Choice Between Regulating Commercial and All Speech

The express preemption provision of the CAN-SPAM Act makes it difficult, if not impossible, for states to only regulate commercial e-mail without being preempted.[220] Therefore, states that seek to protect their residents from the onslaught of spam may have greater success regulating all unsolicited e-mail rather than merely commercial e-mail.[221] Such regulation will not be bound by the limitations of the CAN-SPAM Act if it can survive First Amendment scrutiny.[222]

Such all-encompassing statutes must be carefully drafted to avoid being overbroad.[223] The Supreme Court of Virginia was troubled by the

---

[216] *See Mummagraphics*, 469 F.3d at 359. Because of the instantaneous nature of e-mail communication, having to mail written requests to opt-out of further spam is unlikely to be effective and will impose further costs on the recipients. *Cf.* Rowan v. U.S. Post Office Dep't, 397 U.S. 728, 738 (1970) (upholding statute that allows removal of one's name from a publisher's mailing list via post because the Court "categorically reject[ed] the argument that a vendor has a right under the Constitution or otherwise to send unwanted material into the home of another").

[217] *See Jaynes*, 666 S.E.2d at 314 ("[The] statute is unconstitutionally overbroad on its face because it prohibits the anonymous transmission of all unsolicited bulk e-mails including those . . . protected by the First Amendment . . . .").

[218] *See id.* at 312 (citing McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 342 (1995)).

[219] *See Mummagraphics*, 469 F.3d at 359; *Jaynes*, 666 S.E.2d at 312.

[220] *See* 15 U.S.C. § 7707(b)(2)(B) (2006).

[221] *See* Dickinson, *supra* note 11, at 152–53. A beneficial side-effect of trying to regulate all, not just commercial, spam is that such laws could address all annoying unsolicited e-mail because it is arguably the unsolicited nature of the e-mail that makes it a nuisance, not merely the fact that it is commercial. *See id.*; Memorandum from Deborah Fellows, *supra* note 3, at 5.

[222] *See Jaynes*, 666 S.E.2d at 314.

[223] *See id.* at 313.

fact that the statute in *Jaynes* would bar anonymous speech, because preserving anonymity in an e-mail necessarily involves falsifying the sender's address.[224] While the anonymous nature of spam makes enforcement more difficult, this aspect is not the main problem with receiving unsolicited e-mail.[225] Both named and anonymous e-mail may, among other things, waste ISP resources, increase costs to the end-users, and result in valuable e-mail going unnoticed.[226] Thus, a statute seeking to regulate all spam should not make a distinction based on the anonymity of the sender.[227]

Additionally, instead of banning unsolicited e-mail altogether, states can attempt to merely regulate the time, place, and manner of the spam.[228] The U.S. Court of Appeals for the Fifth Circuit, in analyzing the government interest in regulating spam, suggested that if unsolicited e-mail is a drain on computer server resources, it could be limited to certain times, such as off-peak hours.[229] Furthermore, given the enormity of the spam problem and the availability of ample alternative channels for anonymous speech on the Internet, the government interest in such regulations should be considered substantial.[230]

2. Regulation in the Form of Consumer Protection

Alternatively, states seeking to regulate commercial e-mail may do so through their general consumer protection laws because the CAN-SPAM Act expressly leaves state regulation of "acts of fraud or computer

---

[224] *See id.*

[225] *See* 15 U.S.C. § 7701(a)(3)–(4). *But see* 15 U.S.C. § 7701(a)(7)–(8) (suggesting that spammers include misleading information to induce recipients to view the message).

[226] *See* S. REP. No. 108-102, at 7 (2003), *reprinted in* 2004 U.S.C.C.A.N. 2348, 2353 (detailing increased connection costs to consumers in remote areas and business travelers).

[227] *See Jaynes*, 666 S.E.2d at 314.

[228] *See* Va. State Bd. of Pharmacy v. Va. Citizens Consumer Council, Inc., 425 U.S. 748, 771 (1976) ("We have often approved [time, place, and manner] restrictions . . . provided that they are justified without reference to the content of the regulated speech, that they serve a significant governmental interest, and that in so doing they leave open ample alternative channels for communication of the information.").

[229] *See* White Buffalo Ventures, LLC v. Univ. of Tex., 420 F.3d 366, 377 (5th Cir. 2005). At the very least such a regulation would allow individuals to prioritize important (solicited) e-mail over unimportant (unsolicited) e-mail. *See id.* It may also result in lower access fees if the spam is downloaded and read during off-peak hours. *Cf.* S. REP. No. 108-102, at 7.

[230] *See e.g.*, Electronic Frontier Foundation, How to Blog Safely (About Work or Anything Else), http://www.eff.org/wp/blog-safely (last visited Nov. 5, 2009) (describing anonymous blogging). Blogs are simple, easy-to-use websites that the author updates periodically. *See* James Curry, *Joining the Blogosphere*, POPULAR MECHANICS, June 2005, at 158. If Publius wanted to publish the *Federalist Papers* anonymously, he could have done so on his blog. *Cf. Jaynes*, 666 S.E.2d at 314.

crime" in place.[231] By tying commercial e-mail to broader anti-fraud laws, states would be exempt from preemption by the federal act.[232] Because the CAN-SPAM Act did not intend to displace comprehensive state anti-fraud and anti-computer crime law, statutes dealing with fraud and deception in e-mail do not raise the same concerns as statutes requiring specific labeling, formatting, or other express e-mail regulation.[233]

This carve-out may not allow the full range of remedies that states were free to impose on spam before the CAN-SPAM Act.[234] The narrow interpretation of falsity and deception by the U.S. Court of Appeals for the Fourth Circuit—requiring material falsity in the offending e-mail—has a dual effect of making it easier to preempt state law while making it harder to establish a cause of action under the CAN-SPAM Act.[235] Such a narrow interpretation therefore creates more difficulty for plaintiffs to establish a cause of action under state fraud laws.[236] Thus, the receiver of the spam in *Mummagraphics* was not entitled to relief under either the state or the federal statute when he alleged that by violating Oklahoma's commercial e-mail laws, the unsolicited e-mail also violated Oklahoma's consumer protection laws.[237] The court noted that the CAN-SPAM Act's preemption of state laws also meant that such claims could not give rise to subsequent violations of general state fraud and consumer protection laws.[238]

3. States and State Agents as Internet Service Providers

Because of the conflict within the CAN-SPAM Act's clauses, states may attempt to regulate spam through technological means in their capacity as ISPs, rather than through legislative means.[239] State-run institutions, such as universities, provide Internet access to the public that they serve.[240] Additionally, many cities, towns, and other municipalities

---

[231] *See* 15 U.S.C. § 7707(b)(2)(B) (2006).

[232] *See* S. REP. NO. 108-102, at 22 ("[T]here would be no preemption of State laws that do not expressly regulate e-mail, such as State common law, general anti-fraud law, and computer crime law.").

[233] *See id.*

[234] *See Mummagraphics*, 469 F.3d at 356.

[235] *See supra* notes 142–154 and accompanying text.

[236] *See Mummagraphics*, 469 F.3d at 353 n.1.

[237] *See id.*

[238] *See id.*

[239] *See supra* notes 155–170 and accompanying text.

[240] *See White Buffalo*, 420 F.3d at 373. The Fifth Circuit Court of Appeals in *White Buffalo* expressly recognized that the University of Texas was an "Internet Access Provider" to its

are planning to offer wireless Internet access to residents and visitors.[241] The state as ISP can then create regulations designed to eliminate, or at least minimize, spam.[242] Such regulations may be as drastic as blocking all e-mail from specific addresses, as the University of Texas did in *White Buffalo Ventures, LLC v. University of Texas*, or as mild as limiting unsolicited e-mail to a particular time of day, as the U.S. Court of Appeals for the Fifth Circuit suggested.[243] Even less-restrictive regulations would have the desired effect of limiting spam by making it easier to categorize and therefore eliminate.[244]

These less-restrictive alternatives laid out in the preceding parts may not fully solve the spam problem, however, because the use of such avenues to circumvent the CAN-SPAM Act depends on the courts interpretation of the preemption clause in the Act.[245] Furthermore, the strict scrutiny standard that courts apply in examining whether speech regulation violates the First Amendment means that states may not be allowed to use blanket prohibitions on unsolicited e-mail.[246] This notion, combined with the recognized, albeit lesser, interest in protecting commercial speech and the willingness by the courts to apply the overbreadth doctrine to spam, requires any solution to be very carefully crafted.[247]

B. *Challenging Assumptions About Spam*

Legislatures drafting anti-spam legislation rely on assumptions about spammers and the nature of spam.[248] If these assumptions are in-

---

students and faculty, and therefore its regulation of unsolicited e-mail was not preempted by the CAN-SPAM Act. *See id.*

[241] *See, e.g.*, Debra McCown, *Free Wi-Fi Goes Live in Abingdon*, Bristol Herald Courier (Va.), Oct. 2, 2008, http://www2.tricities.com/tri/news/local/article/wifi_goes_live_in_abingdon/14562; Free Wireless Access, Albuquerque Official City Website, http://www.cabq.gov/wifi/ (last visited Jan. 21, 2009); *see also* Bailey, *supra* note 13, at 609–10.

[242] *See White Buffalo*, 420 F.3d at 369, 373.

[243] *See id.* at 377.

[244] *See id.* For example, a city providing Internet access, citing the desire to protect its network infrastructure from heavy load, could limit spam to off-peak hours, such as from one to four o'clock in the morning. *See id.* All e-mail arriving during these hours, unless from senders previously known to the recipient, would be flagged as spam. *See id.* Senders violating this provision could simply be blocked, which is exactly what the University of Texas was allowed to do under the CAN-SPAM Act. *See id.*

[245] *See Mummagraphics*, 469 F.3d at 353 & n.1, 354.

[246] *See Jaynes*, 666 S.E.2d at 313.

[247] *See* Bolger v. Youngs Drug Prods. Corp., 463 U.S. 60, 68 (1983) (finding that commercial speech enjoys qualified but nonetheless substantial protection); *see also* City of Cincinnati v. Discovery Network, Inc., 507 U.S. 410 (1993) (striking down commercial speech regulation that was not substantially related to the state interest).

[248] *See, e.g.*, 15 U.S.C. § 7701(a) (2006).

correct, however, resultant legislation is unlikely to be effective in combating the spam problem.[249] Reexamination of the underlying assumptions can create more powerful incentives to attack spam.[250]

1. Spam Is Costly to Internet Service Providers

Most discussion and legislation concerning unsolicited e-mail assume that the economic loss that ISPs suffer from spam will create incentives for them to help fight this problem.[251] One reason Congress created a cause of action for ISPs in the CAN-SPAM Act is the belief that these large industry players would be able to fight spam more effectively than many individual recipients.[252] And in fact, some large ISPs have gone after spammers.[253]

Still, this assumption may not be completely correct.[254] If spam is a problem for all ISPs, they may be able to pass these costs onto consumers without being economically hurt, and therefore the cost of spam may thus be factored into the cost of using e-mail in general.[255] For instance, connection and access fees for data downloaded, either by connection time or by volume of data, are passed directly to the consumer.[256] Although paying to download spam is certainly frustrating to the consumer, it may create an increased profit for the service provider.[257] Furthermore, the switch to broadband services and the growth of bandwidth-heavy content, such as video, make e-mail a relatively small component of the overall network traffic.[258]

---

[249] *See* Soma et al., *supra* note 10, at 181.

[250] *See infra* notes 302–317 and accompanying text.

[251] *See* 15 U.S.C. § 7701(a)(6); S. REP. No. 108-102, at 6 (2003), *reprinted in* 2004 U.S.C.C.A.N. 2348, 2352–53.

[252] *See* 15 U.S.C. § 7706(g)(1).

[253] *See* Mitch Wagner, *AOL, Microsoft, and Yahoo Form Anti-Spam Alliance*, INFO. WEEK, Apr. 28, 2003, *available at* http://www.informationweek.com/news/management/showArticle.jhtml?articleID=9400072 ("The alliance will focus on ways to block spam and will work with legal authorities on enforcement.").

[254] *See* Soma et al., *supra* note 10, at 186–87.

[255] *See* S. REP. No. 108-102, at 6 (citing reports that spam adds two dollars per month to individual users' Internet bills); *see also* Soma et al., *supra* note 10, at 192–93 (suggesting that the marginal cost of transmitting spam is as low for ISPs as it is for spammers).

[256] *See, e.g.*, Dialup Provider Options, Campus Info. Tech. & Educ. Servs., Univ. of Illinois at Urbana-Champaign, http://www.cites.illinois.edu/dialup/isp_options.html (last visited Nov. 5, 2009).

[257] *See* S. REP. No. 108-102, at 7 (citing effect on dial-up customers).

[258] *See* Ian Williams, *Image Size Doubles Average File Size*, VNUNET.COM, Mar. 26, 2007, http://www.v3.co.uk/vnunet/news/2186424/image-spam-doubles-spam-file (noting an increase in the size of an average e-mail message from six kilobytes (KB) to eleven KB). By contrast, the average size of a video file on YouTube is twelve megabytes (MB), roughly one thou-

Furthermore, ISPs may be able to profit from spam in a number of ways.[259] By offering consumers superior spam protection, such as better filtering, ISPs are able to differentiate their services from those of other providers.[260] The popularity of web-based e-mail programs, such as Yahoo! and Google's GMail, gives ISPs a way to harness the extra time users spend on their websites due to spam.[261] These e-mail providers are able to display other advertisements inside their e-mail applications, and even target these ads to the content of the e-mail being checked, including spam.[262]

Thus, the fundamental assumption about the behavior of ISPs in combating spam may be unfounded.[263] ISPs may choose to act only in the most egregious cases, failing to bring enforcement actions against less malicious spammers even though they have been granted such power by the CAN-SPAM Act.[264] Therefore, viewing ISPs as allies in the crusade against spam may be a mistake.[265]

2. Only Unsolicited Commercial E-Mail Is Harmful and Annoying

Another fundamental assumption made in the spam discussion is that it is spam's commercial nature that is causing problems.[266] While commercial spam in undoubtedly annoying, and oftentimes more likely to be fraudulent, other types of spam are not made any less annoying

---

sand times larger than an e-mail message. *See* Wes Simpson, *Can the Internet Handle Broadcast TV?*, TVTECHNOLOGY.COM, July 11, 2007, http://www.tvtechnology.com/article/16108.

[259] *See* Soma et al., *supra* note 10, at 192.

[260] *See id.*; *see also* Paul Davidson, *AOL Steps Up Efforts to Block Spam*, USA TODAY, Apr. 16, 2003, http://www.usatoday.com/money/industries/technology/2003-04-16-aol_x.htm; Google, Protect and Secure Your Existing E-mail System, http://www.google.com/postini/email.html (last visited Feb. 26, 2009).

[261] *See* Michael Liedtke, *Yahoo Addresses E-Mail Concerns with New Domains*, ABC NEWS, June 19, 2008, http://abcnews.go.com/Technology/wireStory?id=5199101 (describing Yahoo as having 266 million users, followed by Microsoft, with 264 million, and Google, with 101 million). This suggests that as many as half of global web users use some form of web-based e-mail. *See* Press Release, ComScore, Global Internet Audience Surpasses One Billion Visitors (Jan. 23, 2009), http://www.comscore.com/press/release.asp?press=2698 (reporting that global Internet audience reached one billion users).

[262] *See, e.g.*, *Google's Gmail Could Be Blocked*, BBC NEWS, Apr. 13, 2004, http://news.bbc.co.uk/2/hi/business/3621169.stm.

[263] *See supra* notes 248–262 and accompanying text.

[264] *See* 15 U.S.C. § 7706(g) (2006); Soma et al., *supra* note 10, at 167. While the plaintiffs in both *Mummagraphics* and *Beyond Systems, Inc. v. Keynetics, Inc.* were ISPs, they were relatively small ones and both tried to proceed under an individual cause of action under state law. *See Mummagraphics*, 469 F.3d at 350; *Beyond Sys.*, 422 F. Supp. 2d at 525, 528.

[265] *See* Soma et al., *supra* note 10, at 186–93 (advocating giving ISPs the ability to sue those ISPs that allow spammers to use their networks for sending unsolicited e-mail).

[266] *See* 15 U.S.C. § 7701(a)(3),(5)–(6).

by their noncommercial nature.[267] Spam that makes appeals for charity or political commentary is no more solicited than offers of miracle products or time-share deals.[268]

The nature of the spam, whether commercial or not, does not affect the reasons why spam is problematic.[269] Any type of spam still creates more Internet traffic and increases the load on ISP resources.[270] Furthermore, noncommercial spam also forces recipients to spend time sorting their e-mail, causes legitimate messages to be drowned out in the sea of spam, and may even contain computer viruses.[271] Noncommercial spam, however, is outside the scope of the CAN-SPAM Act, as well as a number of state laws.[272] Because religious or political speech has typically enjoyed strong First Amendment protection, legislators may be afraid to target spam of that nature.[273]

Because spam is being sent directly to recipients, most often in their homes, any First Amendment concerns start coming into conflict with the sanctity that the home has typically enjoyed in American jurisprudence.[274] Thus, the general rule that the burden is on the viewer to avert their eyes from unwanted speech does not apply to unwanted

---

[267] *See* Press Release, Sophos, Politicans Add to the Spam Problem in Run-up to US Elections (Nov. 9, 2006) http://www.sophos.com/pressoffice/news/articles/2006/11/political-spam.html; *see also* THE STATE OF SPAM: MONTHLY REPORT, SYMANTEC MESSAGING AND WEB SECURITY 10 (Jan. 2009), *available at* http://eval.symantec.com/mktginfo/enterprise/other_resources/b-state_of_spam_report_01-2009.en-us.pdf [hereinafter THE STATE OF SPAM] (describing holiday "E-card" spam).

[268] *See* Bob Sullivan, *German Political Spam Spread by Virus*, MSNBC, May 16, 2005, http://www.msnbc.msn.com/id/7874164/. There is no basis in thinking that noncommercial spam is any less dangerous to the e-mail recipient because nothing prevents noncommercial spam from containing viruses, either inadvertently or because of malicious intent, for instance to disrupt one's political opponents. *See, e.g.*, Alert, U.S. Presidential Malware, Barack Obama Interview Lure, http://securitylabs.websense.com/content/Alerts/3229.aspx (last visited Nov. 5, 2009).

[269] *See* S. REP. No. 108-102, at 6–7 (2003), *reprinted in* 2004 U.S.C.C.A.N. 2348, 2352–53 (detailing costs that spam inflicts on ISPs and businesses without specifying the nature of the spam).

[270] *See id.*

[271] *See* Jack M. Germain, *Spiritual Spam Becoming More Active*, TECHNEWSWORLD, Dec. 18, 2004, http://www.technewsworld.com/story/38962.html (explaining that the format of some religious spam makes it possible for "spyware"—malicious software—to slip into the recipient's computer). The spam messages may also be a way for spammers to verify e-mail addresses. *See id.*

[272] *See* 15 U.S.C. § 7702(2)(A) (2006).

[273] *See* Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n, 447 U.S. 557, 563 (1980).

[274] *See, e.g.*, Frisby v. Schultz, 487 U.S. 474, 484 (1988) ("The State's interest in protecting the well-being, tranquility, and privacy of the home is certainly of the highest order in a free and civilized society.").

speech in the home, where the recipient of the speech constitutes a "captive audience."[275] Although the government may not be able to initiate the blocking of unwanted material, it should be able to regulate the time, place, and manner of all unsolicited bulk e-mail in the home without great constitutional difficulties.[276]

3. Tough Spam Regulation Will Make Spammers Move Abroad

The assumption that spammers will move overseas is frequently raised in response to proposals to regulate domestic companies.[277] Although there are significant amounts of spam coming from overseas, this argument is not as persuasive as it seems.[278] The United States is currently responsible for the largest percentage of all spam: twenty-seven percent.[279] Spammers need access to the telecommunications infrastructure in order to send spam, and foreign locations with antiquated or unreliable Internet connections are unlikely to be attractive to them.[280] Furthermore, there is no guarantee that other countries will be receptive to spammers.[281]

A recent example illustrates this proposition: McColo, a U.S.-based web-hosting firm located in California, was forced offline after convincing evidence surfaced that it was responsible for as much as seventy-five percent of spam.[282] The Internet providers that connected McColo to

---

[275] *See* FCC v. Pacifica Found., 438 U.S. 726, 748 (1978) (upholding FCC regulation of the radio broadcast of profane monologue); *see also Rowan*, 397 U.S. at 736–37 ("[A] mailer's right to communicate must stop at the mailbox of an unreceptive addressee.").

[276] *See* Lamont v. Postmaster Gen., 381 U.S. 301, 307 (1965) (invalidating federal statute prohibiting delivery of communist materials unless the recipient specifically requested them in writing, as such an obligation was likely to have a deterrent effect); *cf. Rowan*, 397 U.S. at 737–38 (recognizing the ability of Congress to give individuals the power to stop unwanted communications from entering the home).

[277] *See* Jonathan Zittrain, *Internet Points of Control*, 44 B.C. L. Rev. 653, 669 (2003); Hamel, *supra* note 1, at 1000.

[278] *See, e.g.*, Zuckoff, *supra* note 7, at 36; Federal Bureau of Investigation, Nigerian Letter or "419" Fraud, Common Fraud Schemes, http://www.fbi.gov/majcases/fraud/fraudschemes.htm (last visited Oct. 1, 2009) (describing specific type of e-mail fraud typically originating in Nigeria).

[279] *See* The State of Spam, *supra* note 267, at 6. China and Brazil are tied for second, with merely seven percent each. *See id.*

[280] *See* S. Rep. No. 108-102, at 5 (2003), *reprinted in* 2004 U.S.C.C.A.N. 2348, 2351 (speculating that many spammers may be in the United States, but disguise the origin of their spam).

[281] *See* Hamel, *supra* note 1, at 1000. Hamel also suggests that spammers who sell physical products are unlikely to relocate overseas because of the increased shipping costs. *See id.*

[282] *See* Brian Krebs, *Internet Providers Cut Off Host of Spam E-mail*, L.A. Times, Nov. 13, 2008, at C5, *available at* http://articles.latimes.com/2008/nov/13/business/fi-spam13.

the rest of the Internet severed its connections, and e-mail users immediately noticed a significant drop in spam.[283] McColo was also believed to be involved in other aspects of cyber-crime, including fake pharmacy sites, child pornography, and running "botnets"—networks of virus infected "zombie" computers that are used to send spam.[284] The ISPs used by McColo are large, dedicated companies with their own high-speed connections—the kind that may be harder to find overseas.[285]

IV. Judicial and Legislative Proposals to Encourage More Effective Spam Regulation

The lack of authentication in e-mail messaging protocols, the inexpensive nature of bulk e-mail communication, the ineffectiveness of strictly technological solutions to unsolicited e-mail, and the confusing jumble of state and federal law have created the "perfect storm" for spam.[286] It is likely that adequate solutions will not come quickly and, when they do, will involve a mix of legislative and technological approaches.[287] Because spam is a relatively new phenomenon, many potential solutions must be created, implemented, tested, and evaluated for effectiveness.[288] Therefore, the courts and legislatures should initially proceed with caution.[289] The following suggestions address how each branch may want to consider approaching the problem.

---

[283] *See* McColo Takedown Nets Massive Drop in Spam, SecurityFocus, Nov. 13, 2008, http://www.securityfocus.com/brief/855; *see also* The State of Spam, *supra* note 267, at 7 (charting the significant drop in spam during November of 2008).

[284] *See* Brian Krebs, *A Closer Look at McColo, in Security Fix*, Wash. Post, Nov. 13, 2008, http://voices.washingtonpost.com/securityfix/2008/11/major_source_of_online_scams_a.html; *see also* Dunham & Melnick, *supra* note 12, at 4.

[285] *See* Jeff Goldman, *Hurricane Electric's International Network Is the Tenth Largest in the World*, ISP-Planet, Jan. 2, 2008, http://www.isp-planet.com/resources/backbones/hurricane_electric.html.

[286] *See supra* notes 37–154 and accompanying text.

[287] *See* Lessig, *supra* note 1, at 262 (suggesting that "the key to good policy in cyberspace is a proper mix of modalities").

[288] *See* Soma et al., *supra* note 10, at 179; Hamel, *supra* note 1, at 1001. Although some critics have argued that Congress jumped the gun by enacting the CAN-SPAM Act, a national solution is one of the possibilities that should be tested and evaluated. *Cf.* Hamel, *supra* note 1, at 997–98.

[289] *See* Bailey, *supra* note 13, at 644–45.

A. *Breathing Room for State Regulation*

Courts must recognize the value in allowing states to augment the provisions of the CAN-SPAM Act for handling unsolicited e-mail.[290] Different states are going to be responsive to different constituencies and this diversity may not fully manifest itself on the national level.[291] Therefore, when faced with different options for applying various anti-spam laws, courts should pick the approach that creates significant opportunity for experimentation.[292] At the same time, courts must be careful not to retread the regulatory schemes previously ruled out by either Congress or the FTC.[293]

1. A Broader Reading of Exemption

The U.S. Court of Appeals for the Fourth Circuit's narrow reading of the preemption provision of the CAN-SPAM Act effectively suppresses any novel approaches that states may wish to investigate.[294] Other courts—those not bound by Fourth Circuit precedent—should interpret the preemption provision more broadly.[295] Such breathing room will allow states to fine-tune their anti-fraud and computer-crime laws to find the ones most effective at fighting spam.[296] At the same time, the courts must be mindful of the original purposes of the CAN-SPAM Act and ensure that frivolous litigation does not become as prevalent as spam itself.[297]

---

[290] *See* Beyond Sys. Inc. v. Keynetics, Inc., 422 F. Supp. 2d 523, 538 (D. Md. 2006) (augmenting the CAN-SPAM Act with state law to include conspiracy).

[291] *See* Hamel, *supra* note 1, at 967–78. For instance, Virginia, which is home to large ISPs, such as America Online, may have a different understanding of spam than Texas, home to large universities that provide e-mail to their students and faculty. *Compare* Jaynes v. Commonwealth, 666 S.E.2d 303, 306 (Va. 2008), *cert. denied*, 129 S. Ct. 1670 (2009), *with* White Buffalo Ventures, LLC v. Univ. of Tex., 420 F.3d 366, 368 (5th Cir. 2005).

[292] *See, e.g.*, *Beyond Sys.*, 422 F. Supp. 2d at 538 (concluding that state provisions that create conspiracy liability are consistent with, and complement, the CAN-SPAM Act).

[293] *See supra* notes 86–104 and accompanying text.

[294] *See* Omega World Travel, Inc. v. Mummagraphics, Inc., 469 F.3d 348, 355 (4th Cir. 2006).

[295] *See Beyond Sys.*, 422 F. Supp. 2d at 538; *see also* Wong, *supra* note 153, at 476–77 (advocating a broader interpretation).

[296] *See* Wong, *supra* note 153, at 477.

[297] *See, e.g.*, Gordon v. Virtumundo, Inc., No. 06-0204-JCC, 2007 WL 2253296, at *5 (W. D. Wash. Aug. 1, 2007) (granting defendant spammer's motion for attorney's fees because "it is obvious that Plaintiffs are testing their luck at making their 'spam business' extraordinarily lucrative by seeking statutory damages through a strategy of spam collection and serial litigation").

2. Requirement of Substantial Overbreadth

The courts must also provide constitutional breathing room for e-mail regulation by respecting the requirement that any overbreadth be substantial.[298] The overbreadth must not only be "substantial in the absolute sense, but also relative to the statute's plainly legitimate sweep."[299] Because the overwhelming majority of spam is commercial or fraudulent in nature, any minute amount of political or religious spam cannot rise to the level of substantiality required by the overbreadth doctrine.[300] Furthermore, the negative associations recipients have formed from fraudulent, commercial, and obscene spam have effectively "poisoned the well" for any legitimate political or religious messages sent via e-mail.[301]

B. *A Realignment of Legislative Incentives*

Legislators should adjust the anti-spam statutes by taking into account the current judicial interpretation of existing statutes as well as the changing nature of the underlying assumptions.[302] Better incentives for warriors in the battle against spam should help to achieve a greater victory.[303]

1. Clarifying the State-as-ISP Loophole

The CAN-SPAM Act's potential loophole allows states acting as ISPs to regulate spam with less restrictions than Congress may have intended.[304] Because this loophole would allow various state instrumen-

---

[298] *See* United States v. Williams, 128 S. Ct. 1830, 1838 (2008). This is the argument that the Commonwealth of Virginia raised in its petition for certiorari to the U.S. Supreme Court. *See* Petition for a Writ of Certiorari, Virginia v. Jaynes, No. 08-765, 2008 WL 5232723, at *14–23 (U.S. Dec. 11, 2008). The Supreme Court rejected the petition. *See* Virginia v. Jaynes, 129 S. Ct. 1670 (2009).

[299] *Williams*, 128 S. Ct. at 1838.

[300] *See supra* notes 266–276 and accompanying text; *see also* THE STATE OF SPAM: A MONTHLY REPORT, *Symantec Messaging and Web Security*, Nov. 2008, at 4, *available at* http://eval.symantec.com/mktginfo/enterprise/other_resources/b-state_of_spam_report_11-2008.en-us.pdf (finding that the largest amount of political spam in November of an election year to be only three percent).

[301] *See, e.g.*, James Barron, *Nine Jewish Leaders Say Email Spread Lies About Obama*, N.Y. TIMES, Jan. 16, 2008, *available at* http://www.nytimes.com/2008/01/16/us/politics/16letter.html. Anonymous e-mail, however, may not have been the only mode of expression. *See* Mike Madden, *Debunking Anti-Obama E-Mails*, SALON.COM, Aug. 20, 2008, http://www.salon.com/news/feature/2008/08/20/obama_emails/ (suggesting that, in addition to e-mail, messages were posted on blogs and Internet message boards).

[302] *See supra* notes 248–301 and accompanying text.

[303] *See infra* notes 304–317 and accompanying text.

[304] *See White Buffalo*, 420 F.3d at 372–73.

talities to have different sets of laws, compliance with any particular law would be difficult, given the nature of e-mail.[305] Such a loophole may therefore undermine the uniformity that Congress aimed to achieve by creating national legislation in the CAN-SPAM Act.[306] Conversely, Congress should clearly announce its intent if it wants to allow those state actors and municipalities that operate ISPs to experiment with various spam fighting techniques.[307] Such experimentation may help to create the breathing room that effective solutions to spam require.[308]

2. Realigning Incentives for Internet Service Providers

If ISPs lack incentive to reduce spam and spammers are unlikely to move to remote locations due to their reliance on high-bandwidth Internet connections, the view of ISPs' role in the fight against spam should be modified.[309] ISPs cannot be seen as allies if they have no incentive to rein in unsolicited e-mail, or worse, are actively contributing to spam.[310] Therefore, states may be justified in regulating ISPs, such as McColo, to prevent them from either intentionally or inadvertently contributing to the volume of spam.[311] The threat of heavy criminal and financial sanctions should dissuade malicious ISPs, like McColo, from engaging in spamming and spam-promoting activities.[312]

3. A Bounty System to Target Rogue Internet Service Providers

At the same time, funds from sanctioning the violations can be used to create an incentive system to reward cooperating ISPs and other investigative bodies in their efforts to curb spam.[313] The resulting system would be similar to the bounty system proposed by Lawrence Lessig, but without some of the negative factors highlighted in the FTC's report.[314] Because the hunt for the individual spammer is hindered by the anonymity of the Internet, shifting the focus away from

---

[305] *See Mummagraphics*, 469 F.3d at 355–56.

[306] *See* 15 U.S.C. § 7701(a)(11) (2006); *see also Mummagraphics*, 469 F.3d at 355.

[307] *See* Bailey, *supra* note 13, at 627–28.

[308] *See supra* notes 290–297 and accompanying text.

[309] *See supra* notes 251–285 and accompanying text.

[310] *See* Soma et al., *supra* note 10, at 186.

[311] *See id.*

[312] *See id.*; *see also* Krebs, *supra* note 284 (capturing the reaction of an ISP to evidence of major spamming operation as, "We looked into it a bit [and] saw the size and scope of the problem . . . . Within the hour we had terminated all of our connections to [McColo].").

[313] *See* Lessig, *supra* note 1, at 265–67 (proposing a bounty system for individuals that may not take advantage of specialized information that the ISPs possess).

[314] *See supra* notes 91–100 and accompanying text.

them and instead to spam-promoting and contributing ISPs should assist the battle against spam.[315] ISPs are in a better position to fight spam because they are closer to the source of the spam and are able to gather greater and more meaningful information about the spammers from their networks than individual recipients could.[316] Enforcement would thus fall on larger web-hosting companies, which are not only essential to spammers, but also able to more effectively combat unsolicited e-mail.[317]

Conclusion

The problem of unsolicited e-mail is a fairly recent phenomenon. E-mail's popularity, coupled with the low cost, lack of authentication, and relative anonymity of the medium has fueled the growth of spam, which now threatens to severely curtail usefulness of the very medium that spawned it. Neither technological nor legislative solutions have been able to reverse the trend thus far. In fact, the complexity of the interaction between state and federal law in this area makes enforcement of any provisions more difficult.

Because no single approach to this problem has proven to be successful, state legislatures tackling the spam problem need to carefully draft legislation to augment, rather than compete with, the Federal CAN-SPAM Act. At the same time the courts, in interpreting the overlap between state and federal legislation, need to give some "breathing room" to state laws seeking to curtail spam. The assumption that only commercial spam should be regulated must be reexamined in light of the fact that if spam is allowed to grow at its current pace, it may effectively destroy e-mail as a communications medium by rendering it useless.

Additionally, states must focus on effective ways of combating spam by creating systems that properly align the incentives for all the parties involved in this problem, including the ISPs. Addressing the problem of spam by state regulation of ISPs appears both more promising and less encumbered by federal limitations. States must ensure, however, that such legislation is neither preempted by the CAN-SPAM Act nor precluded by constitutional limitations.

Igor Helman

---

[315] *See* Soma et al., *supra* note 10, at 186–93.

[316] *See id.* at 186.

[317] *See supra* notes 248–265 and accompanying text.