The Need for New Federal Anti-Spam Legislation

Matthew Sipe[1]

The CAN-SPAM Act of 2003 was passed in an attempt to stop "the extremely rapid growth in the volume of unsolicited commercial electronic mail" and thereby reduce the costs to recipients and internet service providers of transmitting, accessing, and discarding unwanted email.[2] The Act obligates the senders of commercial email to utilize accurate header information, to "clear[ly] and conspicuous[ly]" identify their emails as "advertisement or solicitation," and to notify recipients of the opportunity to opt-out of receiving future emails.[3] Once an individual has opted out, that sender is then prohibited from emailing them further.[4] Despite high hopes, the Act has largely been considered a failure for four reasons: 1. It eliminates many pre-existing private causes of action against senders,[5] 2. it does not require senders to receive permission before initiating contact,[6] 3. it relies upon a system of opt-out links that are both distrusted and frequently abused,[7] and 4. it has been under-enforced.[8]

---

[1] J.D. Candidate 2015, Yale Law School.
[2] 15 U.S.C. § 7701(a)(2)-(3), (6) (2012).
[3] *Id*. § 7704(a)(1)-(2), (5).
[4] *Id.* § 7704(a)(4)(A).
[5] *See* Amit Asaravala, *With This Law, You Can Spam*, WIRED (Jan. 23, 2004), http://www.wired.com/techbiz/media/news/2004/01/62020 (quoting Lawrence Lessig as saying the Act "is an abomination . . . . It's ineffective and it's affirmatively harmful because it preempts" other causes of action).
[6] *See Statement on CAN SPAM*, COAL. AGAINST UNSOLICITED COMMERCIAL EMAIL (Dec. 16, 2004), http://www.cauce.org/2004/12/cauce-statement-on-can-spam-act.html (noting that by adopting an opt-out system, "[CAN-SPAM] gives each marketer in the United States one free shot at each consumer's e-mail inbox . . . .").
[7] *See* Daniel Solove, *What Exactly Is a "Spammer"?*, CONCURRING OPINIONS (Jan. 7, 2007), http://www.concurringopinions.com/archives/2007/01/what_exactly_is.html ("It is common knowledge that you shouldn't click the opt out link on an unsolicited email because many spammers use that trick as a way to verify that people have read the spam and will then send people even more spam.").

In the absence of comprehensive federal legislation, alternative solutions to the spam problem have proliferated, including state-by-state statutory regimes, decentralized private regulation, and restraints on the acquisition of email addresses itself. This paper examines some of the shortcomings of these alternative approaches, advocating instead for a new, more complete federal statutory regime.

I. State Solutions: Low Compliance, Low Enforcement

Some states have tried statutory approaches to curtailing spam.[9] These regimes vary widely, ranging from completely prohibiting all "unsolicited commercial email,"[10] to permitting unsolicited commercial emails but requiring that they contain certain keywords in the subject line,[11] to merely requiring truthfulness in the sender and subject lines,[12] to seemingly no regulation whatsoever.[13] These broad categories have further differentiation—some states' laws only apply to email sent to more than a certain number of recipients,[14] for example—so that the result is a substantially heterogeneous patchwork of regulation across the country.

Since email addresses, unlike physical addresses, offer no indication of the location of the recipient, complying with each state's particular laws becomes all but impossible for senders of commercial email. The result is low voluntary compliance, with weak enforce-

[8] *See* Jonathan K. Stock, *A New Weapon in the Fight Against Spam*, MONDAQ (Oct. 8, 2004), http://www.mondaq.com/article.asp?article_id=28901 ("The [CAN-SPAM] Act has largely gone unenforced.").

[9] *See, e.g.*, Washington v. Heckel, 24 P.3d 404 (Wash. 2001) (finding Heckel liable for sending unsolicited commercial email by applying Washington's Commercial Electronic Mail Act, codified at WASH. REV. CODE § 19.190 (2012)).

[10] CAL. BUS. & PROF. CODE § 17529.2(a)-(b) (West 2013).

[11] *See, e.g.*, 815 ILL. COMP. STAT. 511/10(a)(a-15) (2012) (mandating use of "ADV" and "ADV:ADLT" in "unsolicited electronic mail advertisement's subject line[s]"); ALASKA STAT. § 45.50.479 (2012) (mandating the use of subject line keywords only for sexually explicit content); WIS. STAT. § 944.25 (2012) (same).

[12] *See, e.g.*, NEV. REV. STAT. §§ 205.492, 205.511 (2012); N.D. CENT. CODE § 51-27-01 (2012); WASH. REV. CODE §§ 19.190.010 to .110 (2012).

[13] Hawaii, for example, "has no statutes addressed specifically to commercial email and spam." Legal Information Institute, *Hawaii*, CORNELL L. SCH., http://www.law.cornell.edu/wex/inbox/hawaii (last accessed Nov. 17, 2013).

[14] *See, e.g.*, LA. REV. STAT. ANN. §§ 14:73.1, 14:73.6 (only applying to "electronic message[s] . . . sent in the same or substantially similar form to more than one thousand recipients").

ment mechanisms—low-incentive private causes of action[15] and underfunded state investigators[16]—unable to pick up the slack. Uniform federal legislation against spam that preempts these state regimes, includes greater incentives for bringing private action, and allocates funding for investigations would increase compliance and improve enforcement across the country.[17]

II. Decentralized Private Regulation: Anticompetitive Concerns

Private internet service providers (ISPs) have also stepped in, generating lists of websites that they believe "send or support the sending of spam," and "blocking transmission" between those websites and the addresses in its own system.[18] This decentralized process of private regulation may be more flexible and adaptive to changing technology,[19] but it creates significant anticompetitive concerns.[20]

[15] Many states, for example, only allow plaintiffs to recover actual damages or a predetermined maximum amount; these are likely insufficient to incentivize the costly and time-consuming process of obtaining a lawyer, filing suit, and litigating. *See, e.g.*, R.I. GEN. LAWS § 6-47-2(h) (2012) (capping what plaintiffs may receive at $100, plus legal fees); PA. STAT. ANN. § 2250.7(a)(1) (West 2013) (same); ME. REV. STAT. tit. 10 § 224.1497(7)(B) (2012) (allowing for recovery of actual damages or $250, whichever is greater); MO. REV. STAT. § 407.1129 (2012) (allowing for recovery of actual damages or $500, whichever is greater).

[16] *See Electronic Crime Needs Assessment for State and Local Law Enforcement*, NAT'L INST. OF JUSTICE (Mar. 2001), https://www.justnet.org/pdf/186276.pdf, at iv (voicing "serious concerns about the capability of [state] law enforcement resources to keep pace" with a wide variety of computer crimes).

[17] One might argue that senders of unsolicited commercial email ought to simply identify the strongest state law, obey it, and then they will be safe in every state. The result of this, however—uniform anti-spam law across the country—is more legitimately achieved through federal legislation than a single state's unilateral action. Some states, for one reason or another, may not want stronger anti-spam laws. The federal legislative process would balance these interests, and take different states' desires into account.

[18] Media3 Technologies v. Mail Abuse Prevention System, No. 00–CV–12524–MEL.,
2001 WL 92389, at *2 (D. Mass. Jan. 2, 2001).

[19] *See* David G. Post, *Of Black Holes and Decentralized Law-Making in Cyberspace*, 2 VAND. J. ENT. L. & PRAC. 70 (2000).

[20] Decentralized private regulation also raises the same compliance concerns outlined above. There are many different possible definitions of spam, let alone what constitutes "supporting" the sending of spam. Since ISPs may cover residents of multiple states, and states may have multiple ISPs, the result is a patchwork of pri-

The criteria for blacklisting can be quite elastic—despite dedicating significant resources to fighting spam and policing relay use, MIT ran afoul of one such blacklist for simply having "bad email practices"[21]—and could easily allow ISPs to engage in selective enforcement, disproportionately blocking the websites and communications of competitors. Since ISPs are already natural monopolies, with customers in a given location typically having few, if any, alternatives, market forces would do little to restrain capricious blocking activity. Furthermore, ISPs that operate as part of much larger corporations have added potential for abuse by leveraging their blocking power in other markets; AT&T, for example, might use its position as an ISP to block the website and commercial messages of a competing cell phone carrier while allowing its own to go through. In this way, allowing ISPs to maintain blacklists enables them to magnify their already significant market power. Federal legislation against spam can obviate the need for private blacklists, stopping spam without generating anticompetitive forces.

III. Restraints on Email Address Acquisition: No Protection in Many Cases

The Computer Fraud and Abuse Act (CFAA)[22] as well as the common law of contract and trespass have been used to curtail spam indirectly by policing the illegitimate acquisition of email addresses.[23] However, these solutions are incomplete at best. Focusing on the acquisition of email addresses does nothing for individuals whose email addresses are already in the hands of spammers. Additionally, these restraints miss a wide variety of email address acquisition techniques. Lists of email addresses can still be bought, sold, or

vate policies overlaid onto a patchwork of state regulations, further hampering compliance.

[21] *See* Lawrence Lessig, *The Spam Wars*, THE INDUS. STANDARD (Dec. 31, 1998).

[22] 18 U.S.C. § 1030 (2012).

[23] *See, e.g.*, Register.com, Inc. v. Verio, Inc., 356 F.3d 393 (2d Cir. 2004) (determining that querying Register's servers to obtain their customers' email information for spamming purposes constituted a breach of contract on the part of Verio, as well as trespass to chattels); America Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444, 450 (E.D. Va. 1998) (determining that by using an AOL membership to harvest the email addresses of AOL users, LCGM was in violation of AOL's Terms of Service, and as a result both "exceeded authorized access" and "accessed without authorization" for the purposes of the CFAA).

posted for free by companies that acquired them. Users may unwittingly leave their contact information searchable on social media sites. Many email addresses can even be guessed.[24] Federal legislation addressing the act of spamming directly is needed to close these gaps, and provide recourse once an email address has been acquired.

IV. Conclusion: Crafting Better Federal Spam Regulation

A new federal statutory regime regulating spam is needed to replace CAN-SPAM. State regulations are prohibitively difficult to comply with, and lack proper enforcement mechanisms. Private regulation raises too many anticompetitive concerns. Restrictions on email address acquisition, while beneficial, are an inadequate solution on their own. New federal regulation that directly targets spamming activity, requires opting in rather than opting out, provides sufficient incentives for private parties to file complaints or bring suit, and dedicates resources for investigations would go far in reducing spam below its current level.

[24] Combinations of common first and last names with popular domains such as @gmail.com or @aol.com generate numerous positive results as of this writing (search conducted via web applets such as Linksy's Find-Email (http://linksy.me/find-email). There are even programs designed to help automate such guessing, such as the Gmail extension Rapportive (http://rapportive.com).