I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY

RITA MARIE CAIN*

When Does Preemption Not Really Preempt? The Role of State Law after CAN-SPAM

Abstract: Congress has expressly preempted most state regulations of unsolicited commercial email, commonly known as spam. As of 2004, more than thirty states had passed various anti-spam regulations that were affected by the preemption provision in the federal CAN-SPAM Act. The scope of express preemption under the federal CAN-SPAM Act, however, has been the subject of several court decisions that have preserved claims under various state statutes. These cases raise questions about the efficacy and propriety of preemption under CAN-SPAM.

This article explains express preemption and the policy behind its use by Congress in the federal CAN-SPAM statute. The article examines the state claims that have survived in the face of that express preemption to determine if the current federal/state dynamic accomplishes the public policy CAN-SPAM intended to address. The article concludes with recommendations to revise CAN-SPAM to reinstate state protections or to include the best aspects of the preempted state laws in the federal law.

* Professor of Business Law, Bloch School of Business and Public Administration at the University of Missouri-Kansas City. Professor Cain gratefully acknowledges the financial support she received for this research from the Bloch School's Kemper Summer Research Grant Program. Professor Cain can be reached at cainr@umkc.edu.

I. INTRODUCTION: WHEN DOES PREEMPTION NOT REALLY PREEMPT? THE ROLE OF STATE LAW AFTER CAN-SPAM

The Commerce Clause in the United States Constitution enables Congress to protect the national economic interests of the United States.[1] States may regulate interstate business when commercial activity threatens the health or welfare of local citizens.[2] However, according to the Dormant or Negative Commerce Clause,[3] state regulations cannot impose an "undue burden" on interstate commerce.[4]

In the borderless cyber-economy, Congress recently circumvented the debate over the alleged undue burdens that arise from multi-state compliance. Congress resorted to express preemption regarding internet service taxes[5] and is considering this approach regarding spyware regulation.[6] Congress also expressly preempted most state regulations of unsolicited commercial email, commonly known as

---

[1] U.S. CONST. art. I, § 8, cl. 3 (granting Congress power "to . . . regulate Commerce . . . among the several States").

[2] *See, e.g.*, Huron Portland Cement Co. v. Detroit, 362 U.S. 440 (1960) (A local smoke ordinance against vessels was upheld).

[3] *See generally* Wikipedia, Dormant Commerce Clause, http://en.wikipedia.org/wiki/Dormant_Commerce_Clause (last visited Jan. 23, 2008). According to Justice Felix Frankfurter, "the Commerce Clause was not merely an authorization to Congress to enact laws for the protection and encouragement of commerce among the States, but by its own force created an area of trade free from interference by the States. In short, the Commerce Clause even without implementing legislation by Congress is a limitation upon the power of the States." Freeman v. Hewit, 329 U.S. 249, 252 (1946).

[4] "[I]n the name of the Dormant Commerce Clause, the Court has significantly limited the power of states to regulate across a wide range of subject areas, including train and truck safety, imports and exports of myriad goods and services, the conditions for the intake and outflow of solid and liquid waste, and insurance and corporatel [sic] law." Robert A. Schapiro, *Toward a Theory of Interactive Federalism,* 91 IOWA L. REV. 243, 263 (2005).

[5] 47 U.S.C. § 151 (2006).

[6] Currently there are two federal spyware bills pending in Congress. The SPY ACT would preempt all state spyware laws except "trespass, contract, or tort law" or "other State laws to the extent that those laws relate to acts of fraud." H.R. 29, 109th Cong. § 6 (2005). The SPY BLOCK Act would preempt all state spyware law except "State criminal, trespass, contract, tort, or anti-fraud law." S. 687, 109th Cong. § 10 (2005). *See also* Jordan M. Blanke, *Robust Notice and "Informed Consent:" The Keys to Successful Spyware Legislation,* 7 COLUM. SCI. & TECH. L. REV. 2 (2006).

spam.[7] As of 2004, more than thirty states had passed various anti-spam regulations that were affected by the preemption provision in the federal CAN-SPAM Act.[8] The scope of express preemption under CAN-SPAM, however, has been the subject of several court decisions preserving claims under various state statutes. These cases raise questions about the efficacy and propriety of preemption under CAN-SPAM.

First, this article briefly summarizes the problems associated with unwanted commercial email and the regulatory approaches to alleviating these problems.[9] Then, the article explains express preemption and the policy behind its use by Congress in the federal CAN-SPAM statute.[10] Next, the article examines state claims that have survived in the face of that express preemption to determine if the current federal/state dynamic actually accomplishes the public policy CAN-SPAM intended to address.[11] The article concludes with a recommendation to revise CAN-SPAM to reinstate state protections or to include the best aspects from the preempted state laws in the federal law.[12]

---

[7] Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, Pub. L. No. 108-87, 117 Stat. 2699 (2003) (codified at 15 U.S.C. §§ 7701–13; 18 U.S.C. §§ 1001, 1037; 28 U.S.C. § 994; and 47 U.S.C. § 227). The law is known by its acronym CAN-SPAM. Despite the reference to pornography in the title, the Act applies to all commercial email messaging.

[8] Jonathan Bick, *Congress Has Come to Control Spam, Not to Bury It,* LEGAL TIMES, Feb. 16, 2004. By their own provisions, the anti-spam statutes of Minnesota, Missouri and Tennessee automatically terminated upon the passage of CAN-SPAM. MINN. STAT. § 325F. 694 (2007); MO. REV. STAT. § 407.1132.3 (2007); TENN. CODE ANN. § 47-18-2501 (2006). North Dakota's law states that any provision of federal law dealing with false or misleading emails will supersede the North Dakota law. N.D. CENT. CODE § 51-27-09 (2007).

[9] *See infra* notes 13–30 and accompanying text.

[10] *See infra* notes 31–61 and accompanying text.

[11] *See infra* notes 62–103 and accompanying text.

[12] *See infra* notes 104–24 and accompanying text.

II. THE PROBLEM OF UNWANTED COMMERCIAL EMAIL

Legal, technical and news media have repeatedly documented the problem of unwanted commercial email.[13] This section will explain the major concerns that are relevant to the analysis below and will provide the most recent estimates of the costs of spam.

The term "spam" actually encompasses a variety of unwanted commercial emails, each with their own associated problems. First, email can be a delivery system for viruses, worms, and data mining programs, all of which may trigger extraordinary harms to computer systems or individual computers and lead to identity theft.[14] Most of the regulatory relief discussed below is not intended to combat the criminal intentions behind these messages. That said, however, the civil regulatory mechanisms discussed below can lighten the burden of non-criminal spam, thus freeing up attention and public resources to combat emails that facilitate computer crimes.

Email is also the latest tool for con artists. Just like snake oil salesmen of the past, con artists now use email to perpetuate age-old frauds to get money from the unwitting in exchange for unfulfilled promises of riches, exotic travel, prize money, virility, and more.[15] Further, messages peddling get-rich-quick schemes and fake charities, as well as those offering legitimate commercial products, often use false subject headings or transmission paths to avoid spam-blocking filters. In the discussion below, all of these messages are characterized as misleading, deceptive, or fraudulent. They are the express target of most spam enforcement today.

Finally, truthful commercial email delivers a legitimate commercial message and makes no attempt to hide its commercial purpose. These emails are the latest form of interactive marketing,

---

[13] For example, a Lexis search of "spam /s costs" in the Combined Law Review, CLE, Legal Journals and Periodicals fields yielded 34 articles from the previous year. The same search in the English-Language News file returned 552 articles.

[14] *See, e.g.,* Miering de Villiers, *Free Radicals in Cyberspace: Complex Liability Issues in Computer Warfare,* 4 NW. J. TECH. & INTELL. PROP. 13, 20 (2005) (explaining that email attachments accounted for 88% of virus attacks in 2003, up from only nine percent in 1996 when most viruses were transmitted by infected diskettes); *see also* Dana L. Bazelon, Yun Jung Choi & Jason F. Conaty, *Computer Crimes*, 43 AM. CRIM. L. REV. 259, 260–63 (2006).

[15] *See generally* Aaron Larson, *Spam Email Fraud*, EXPERTLAW, June 2004, *available at* http://www.expertlaw.com/library/consumer/spam_email_fraud.html; *see also FTC Names Its Dirty Dozen: 12 Scams Most Likely to Arrive Via Bulk Email,* FTC CONSUMER ALERT, July 1998, *available at* http://www.ftc.gov/opa/1998/07/dozen.shtm.

following in the tradition of door-to-door salesmen, bulk mail, telemarketing, and junk faxes. These email messages enjoy commercial speech protection under the First Amendment.[16] Nevertheless, they are subject to regulation because of the significant burdens associated with them.[17]

The burdens associated with spam can be divided into two categories: harms to Internet Service Providers ("ISPs") and their systems and harms to individual recipients. According to The Radicati Group, a technology and market research firm, roughly 183 billion spam messages were sent each day in 2006;[18] of those, 59 percent successfully landed in inboxes.[19] To maintain that less-than-sparkling 41 percent filtering rate, Sara Radicati estimates that $198 billion will be spent in 2007, up 10 times from the $20.5 billion her company estimated was spent combating spam in 2003.[20] That cost covers anti-spam filters, extra server space and network infrastructure, and information technology customer-service hours.[21]

The harm to individual users is harder to quantify but is just as real. When Congress adopted CAN-SPAM, it set out some of these concerns in its findings. Unwanted email costs recipients for the storage and time they spend accessing, reviewing, and discarding unwanted messages.[22] Large numbers of unwanted messages increase the risk that valuable messages will be lost or overlooked while the user attempts to manage all the messages.[23] As a result, the reliability and usefulness of email as a communications tool is reduced for the

---

[16] White Buffalo Ventures, LLC v. Univ. of Tex., 420 F.3d 366, 374–78 (5th Cir. 2005), *cert. denied,* 126 S. Ct. 1039 (2006).

[17] *See infra* notes 18–30 and accompanying text.

[18] Catherine Holahan, *Rising Stakes in the Spam Wars; Anti-spammers are Losing the Battle Against Unsolicited and Often Harmful E-mail,* BUS. WK. ONLINE, Sept. 19, 2006, http://www.businessweek.com/technology/content/sep2006/tc20060919_412904.htm.

[19] *Id*.

[20] *Id*.

[21] *Id.*

[22] 15 U.S.C. § 7701(a)(3) (2004).

[23] § 7701(a)(4).

recipient.[24] Additionally, "some commercial electronic mail contains material that many recipients may consider vulgar or pornographic."[25]

Finally, spam alters a long-held market expectation that the advertiser will directly bear the costs of advertising, while the market will only indirectly bear those costs through higher prices. In contrast, the recipient bears most of the direct costs of spam advertising.[26] Economists opine that advertising serves a "signaling function" to consumers that the advertised product is of a certain quality based on the expense the firm committed to advertising it.[27] Accordingly, consumers make judgments about the appropriate price of an item of that quality.[28] If the consumer, not the firm, is incurring most of the direct advertising expense, basic economic expectations about price and quality are upended.

When enacting CAN-SPAM, Congress found that email's "low cost and global reach make it extremely convenient and efficient, and offer unique opportunities for the development and growth of frictionless commerce."[29] Congress also found that the value of email is "threatened by the extremely rapid growth in the volume of unsolicited commercial electronic mail."[30] Obviously, the costs that spam to ISPs and individual recipients justify government regulation that attempts to limit these harms. The next question is whether federal or state law, or both, can best address these harms.

III. THE CAN-SPAM ACT VERSUS STATE LAW PROTECTIONS

The express preemption provisions in CAN-SPAM intend to create a single regulatory treatment of unsolicited commercial email.

---

[24] *Id*.

[25] § 7701(a)(5).

[26] *See generally* Daniel B. Kennedy, *Netiquette: Mind Your Manners or Get Burned*, CHI. DAILY L. BULL., at 6, Feb. 20, 1996.

[27] *See* Phillip Nelson, *Advertising as Information*, 82 J. POL. ECON. 729 (1974).

[28] *See, e.g*., Paul Milgrom & John Roberts, *Price and Advertising Signals of Product Quality*, 94 J. POL. ECON. 796 (1986).

[29] § 7701(a)(1).

[30] § 7701(a)(2).

> Many States have enacted legislation intended to regulate or reduce unsolicited commercial electronic mail, but these statutes impose different standards and requirements. As a result, they do not appear to have been successful in addressing the problems associated with unsolicited commercial electronic mail, in part because, since an electronic mail address does not specify a geographic location it can be extremely difficult to know with which of these disparate statutes they are required to comply.[31]

Whether preemption in CAN-SPAM has actually yielded a single, meaningful national standard for anti-spam regulation is questionable, because Congress did not entirely occupy the field of anti-spam regulation. The parameters of the federal versus state regulations are discussed next.

The federal CAN-SPAM Act does not prohibit sending unsolicited commercial emails. It focuses on disclosure and opting-out mechanisms. First, email solicitations or advertisements for products and services must be identified by means that are "clear and conspicuous."[32] In addition, commercial email senders are prohibited from using misleading or bogus subject lines and retransmissions of email ads for the purpose of concealing their origins.[33]

The CAN-SPAM Act expressly preempts state anti-spam laws with stricter provisions.[34] Most of the state anti-spam laws also prohibit false or misleading subject lines and origins.[35] A majority of preempted state laws, however, added a technical mandate[36]: they dictated that unsolicited commercial email must include a heading of "ADV" or "ADV ADULT" (for sexually explicit content) in the

---

[31] § 7701(a)(11).

[32] Unlike many now-preempted state laws, however, no uniform label, such as ADV, is required. Without such a uniform tag, blocking software is less effective at screening for these messages and consumers will have to delete them individually. 15 U.S.C. § 7704(a)(5) (2004).

[33] § 7704(a)(1)–(2).

[34] 15 U.S.C. § 7707(b) (2004).

[35] Lily Zhang, *The CAN-SPAM Act: An Insufficient Response to the Growing Spam Problem*, 20 BERKELEY TECH. L.J. 301, 315–17 (2005).

[36] *Id.*

subject line.[37] The advantage of such provisions is that spam filtering programs could more easily search for these common appellations to dispatch incoming messages to a junk mail folder or block them from the email server altogether.[38] Nevertheless, these state technical standards are preempted by CAN-SPAM. Instead, Congress opted for a more generic mandate that solicitation emails be identified by means that are "clear and conspicuous."[39]

Unfortunately, junk mail filters cannot be programmed to spot notices that are "clear and conspicuous" when the actual terms of the notices vary from sender to sender.[40] In other words, Congress asserted that the different standards found in states laws were ineffective at preventing spam. Yet Congress actually preempted these ADV heading mandates that were fairly uniform among the state laws and adopted a much looser "clear and conspicuous" standard that is not technically operational. Preemption of these state mandates seems to contradict the legislative intent behind CAN-SPAM to limit unwanted commercial email.[41]

According to CAN-SPAM, commercial solicitation email must give recipients the ability to send a reply message or other "Internet-based communication" in order to opt-out of additional emails from that sender.[42] This Internet-based mechanism for opting-out must remain viable for at least 30 days after the original message was sent.[43] A majority of the states' anti-spam laws included mandates for

---

[37] *Id.*

[38] Roger Allen Ford, *Preemption of State Spam Laws by the Federal CAN-SPAM Act*, 72 U. CHI. L. REV. 355, 364 (2005).

[39] *Id.*

[40] *Id.*; *see also* Adam Hamel, *Will the CAN-SPAM Act of 2003 Finally Put a Lid on Unsolicited Email?,* 39 NEW ENG. L. REV. 961, 995 (2005).

[41] "This battle in the spam war highlights the fundamental disagreement over the purpose and goal of CAN-SPAM. If the goal of the Act is to reduce the volume of spam at all costs, then the answer is clear: a uniform tag, like ADV, which can be used to filter out *all* unsolicited commercial messages will go a long way toward achieving that goal. If, however, the goal is not to eradicate spam completely, but rather to protect consumers from fraudulent e-mail offers, 'clear and conspicuous,' though non-uniform, 'identification' will allow e-mail users to quickly identify commercial messages without inhibiting the free flow of information over the Internet or stymieing the development of e-commerce." Hamel, *supra* note 40, at 996.

[42] 15 U.S.C. § 7704(a)(3)(A) (2004).

[43] § 7704(a)(3)(A)(ii).

allowing recipients to opt-out of future solicitations.[44] Of those states, only New Mexico included standards that would be deemed stricter than the federal CAN-SPAM mandates because New Mexico required that the opt-out information be located at the beginning of the email text.[45]

After receiving an opt-out request, CAN-SPAM allows the sender 10 business days to cease further email solicitations to that recipient.[46] The sender also is prohibited from selling or otherwise transferring email addresses of persons who have opted-out of future mailings.[47] In addition to a legitimate return email address, the commercial email solicitor must also provide its postal address.[48]

Unfortunately, opt-out provisions in CAN-SPAM are inadequate. Many computer security experts recommend that recipients *not* click on opt-out links because that action tells spammers the email address is active, thus signaling them to continue soliciting and to sell the address to other spammers. As a result, the cure becomes worse than the disease.[49] Accordingly, the opt-out regulation is completely ineffective if it is not backed-up with meaningful remedies when opt-out requests are routinely ignored.

Under CAN-SPAM, Congress empowered the Federal Trade Commission ("FTC") to enforce the law with civil penalties.[50] Congress also created a private cause of action for ISPs for violations that adversely affect their ability to provide their service.[51] In such

---

[44] *See generally* Spam Laws, http://www.spamlaws.com/state/summary.shtml (last visited Jan. 23, 2008).

[45] N.M. STAT. § 57-12-23(B)(2) (2006).

[46] § 7704(a)(4)(A)(i).

[47] § 7704(a)(4)(A)(iv).

[48] § 7704(a)(5)(A)(iii).

[49] "The opt out system, however, does not work because most spammers abuse the confidence of consumers that click on 'opt out' links in commercial e-mail. Spammers know that these consumers have read their e-mail, thus validating the consumers' address. Validated addresses get even more spam." Peter B. Maggs, *Abusive Advertising on the Internet (SPAM) under United States Law,* 54 AM. J. COMP. L. 385, 391 (2006).

[50] The FTC has pursued twenty civil actions under CAN-SPAM through 2005. *See* FTC, EFFECTIVENESS AND ENFORCEMENT OF THE CAN-SPAM ACT: A REPORT TO CONGRESS, app. 5 (2005), *available at* http://www.ftc.gov/reports/canspam05/051220canspamrpt.pdf.

[51] 15 U.S.C. § 7706(g)(1) (2004). ISP actions from the inception of CAN-SPAM through 2005 total 27. FTC, *supra* note 50, app. 6.

actions, courts may award injunctive relief, as well as actual or statutory damages. The statutory damages range from $25 to $1 million per email.[52] Attorney's fees are also available under CAN-SPAM.[53] Despite its findings about harm to individual recipients of spam,[54] Congress created no comparable private cause of action under CAN-SPAM for individual email recipients who are damaged by unwanted email solicitation. As such, individuals and businesses whose email access is burdened with spam have no recourse when their opt-out requests are ignored. Spammers remain undeterred until their violations reach a critical mass and trigger the FTC or an ISP to take action.

Most of the state anti-spam laws that were preempted by CAN-SPAM provided both ISPs and individual email recipients with private statutory claims. These state laws provided statutory damages that ranged from $10 per offending email message[55] to $500.[56] Some states provided greater remedies for ISPs than for individuals.[57] All states that provided private causes of action and statutory damages also provided attorneys fees and costs for prevailing plaintiffs.[58]

Presumably, these state law remedies made it financially feasible for email users to actually pursue anti-spam actions. Accordingly, these laws could have created an effective deterrent against spammers. CAN-SPAM came along quickly after many of these state laws went into effect. Therefore, there was never any meaningful opportunity to see if these remedies actually could make a difference in combating the spam problem before they were preempted by federal law.

---

[52] § 7706(g)(3).

[53] § 7706(g)(4).

[54] 15 U.S.C. § 7701(a)(3)–(5) (2004).

[55] *See, e.g.,* ARIZ. REV. STAT. ANN. § 44-1372.02.B (2007); ARK. CODE ANN. § 4-88-606(b)(1)(A) (2007); COLO. REV. STAT. § 6-2.5-104(2)(b) (2007). Illinois provides the lesser of $10 per email or $25,000 per day. 815 ILL. COMP. STAT. 511/10-(c) (2007).

[56] *See, e.g.,* CONN. GEN. STAT. § 52-570c(d) (2007); FLA. STAT. § 668.606(3)(b) (2007); IND. CODE § 24-5-22-10(d)(2) (2007). California provides a remedy of $1000 per email. CAL. BUS. & PROF. CODE § 17529.5(b)(1)(B)(ii) (2007). Idaho provides the greater of $100 per email or $1000. IDAHO CODE § 48-603E(4) (2007).

[57] *See, e.g.*, IOWA CODE § 714E.1(3)(a) & (b) (2007); ME. REV. STAT. § 1497.7 & 8 (2007); MD. CODE ANN. COM. LAW § 14-3003 (2007).

[58] *See generally* Spam Laws, *supra* note 44.

Historically, harms to individuals for loss or diminished use and enjoyment of their property have been protected by classic property-right torts under state law, such as trespass and nuisance.[59] These tort claims, however, require proof of actual damages. In the case of harm from unwanted email, the cost of storing, accessing, reviewing, discarding, and filtering messages can be extremely difficult to quantify even for ISPs on their systems, but especially for individual businesses and consumers. Further, traditional tort actions to protect property rights require plaintiffs to pay their own attorneys' fees. Attorneys have little incentive to take such cases on contingent fee arrangements when claims for actual damages are low and punitive damages are difficult to prove. Fronting the costs of any such litigation could be prohibitive for many individuals. Despite the inadequacy of these tort claims in providing meaningful consumer relief or any corresponding deterrent effect on spammers, Congress preserved "State laws that are not specific to electronic mail, including State trespass, contract, or tort law."[60]

Under CAN-SPAM, Congress expressly permits states to retain the power to regulate deceptive email advertising.[61] This is a traditional role of state law to protect citizens from fraud. This construct of leaving some state law protection intact while preempting other aspects of state authority under CAN-SPAM, however, may actually frustrate one stated goal of the federal law: to create a uniform standard for spam regulation. Email advertisers are still subject to state-by-state enforcement, so the goal of a uniform system for nationwide compliance has failed. At the same time, meaningful consumer relief provided by state statutory claims is frustrated by preemption. The resulting mix of federal and state law makes little sense from the perspective of either promoting national economic interests or protecting consumers.

Several state law claims have survived under court interpretations of the deceptive advertising provisions in CAN-SPAM. These decisions are discussed next.

---

[59] Regarding the use of tort law to tackle the problem of spam or other cyber harms, see Steven Kam, *Intel Corp. v. Hamidi: Trespass to Chattels and a Doctrine of Cyber-Nuisance*, 19 BERKELEY TECH. L.J. 427 (2004); *see also* Jeremiah Kelman, *E-Nuisance: Unsolicited Bulk Email at the Boundaries of Common Law Property Rights,* 78 S. CAL. L. REV. 363 (2004).

[60] 15 U.S.C. § 7707(b)(2)(A) (2004).

[61] § 7707(b)(1).

IV. STATE FRAUD CLAIMS SURVIVE PREEMPTION CHALLENGES UNDER CAN-SPAM[62]

Congress found that most unsolicited commercial email messages "are fraudulent or deceptive in one or more respects."[63] As noted above, CAN-SPAM and most state anti-spam laws prohibit emails with false or misleading subject lines, transmission paths, or email origins.[64] When recipients sue under these state laws, defendants have been unsuccessful in defeating the claims based on preemption under CAN-SPAM because the claims are based on the authority retained by the states to protect against deceptive advertising.

For example, in *Beyond Systems, Inc. v. Keynetics, Inc.*, a Maryland ISP sued under the Maryland Commercial Electronic Mail Act.[65] Beyond Systems, Inc. ("BSI") claimed it had received 6202 unsolicited commercial email messages from the defendants that were false or misleading regarding their origin or transmission path, or that contained false or misleading information in the subject line.[66] The Maryland statute authorizes Maryland recipients of commercial email to sue senders of messages that contain false or misleading information in the subject line or about the origin or transmission path of the

---

[62] In *White Buffalo Ventures*, the 5th Circuit held that an action by a state agency acting in its role as ISP was not preempted. This outcome is limited to cases when a state is acting as an email service provider and would have no applicability to claims by recipients suing under state anti-spam laws.

[63] 15 U.S.C. § 7701(a)(2) (2004).

[64] § 7701(a)(1)–(2).

[65] Beyond Sys., Inc. v. Keynetics, Inc., 422 F. Supp. 2d 523, 525 (D. Md. 2006).

[66] An earlier case brought under the Maryland statute dealt only with the issues of personal jurisdiction over an out-of-state spammer, as well as a claim that the statute violated the negative commerce power. Mary CLE, LLC v. First Choice Internet, Inc., 890 A.2d 818, 824–25 (Md. Ct. Spec. App. 2006). The Maryland court, as well as other courts have found the exercise of jurisdiction by a plaintiff's state to be proper based on spam contacts with the state. *See, e.g.,* Verizon Online Serv., Inc. v. Ralsky, 203 F. Supp. 2d 601 (E.D. Va. 2002); *see also* State v. Heckel, 24 P.3d 404 (Wash. 2001); *but see* Rhodes v. Unisys Corp., 2006 U.S. App. LEXIS 6143 (11th Cir. 2006) (holding that a *single* email from a CEO did not constitute sufficient contacts by him with the state to justify personal jurisdiction); Rice v. Karsch, 2005 U.S. App. LEXIS 24709 (6th Cir. 2005) (holding that personal jurisdiction over an attorney was improper since his email communications in the state were only in response to messages initiated by the plaintiff); Beyond Sys., Inc. v. Realtime Gaming Holding Co., LLC, 878 A.2d 567 (Md. App. 2004) (plaintiff was unable to establish an agency relationship to connect the defendant to the spammers).

message.[67] Under the Maryland law, an ISP may recover $1000 per email or actual damages (versus $25 per email under CAN-SPAM).[68] The *Beyond Systems, Inc.* Court rejected the defendants' assertion that the state claim was preempted under CAN-SPAM. CAN-SPAM "provides a carve-out" for state laws like the Maryland statute that target emails that are false or deceptive in any portion.[69] The Maryland statute is not impliedly inconsistent with CAN-SPAM either, according to the Court, because it furthers all of the goals of the federal law.[70]

Similarly, in *Gordon v. Impulse Marketing Group, Inc.*, a Washington resident sued a Nevada company under the Washington Commercial Electronic Mail Act[71] and the Washington Consumer Protection Act[72] for conspiring to initiate email transmissions with false or misleading information in the subject line.[73] The *Gordon* Court held that CAN-SPAM does not preempt state spam laws that regulate falsity or deception in commercial email messages.[74]

In this case, the plaintiff was a small business owner with an Internet website, not an ISP. Washington's statutory damages provide email users a remedy of $500 per offending email. No such claim is available to individual recipients like Gordon under CAN-SPAM.

The Washington district court did not consider if a private cause of action by an individual recipient would be impliedly preempted by the federal law that does not provide such a claim. Congress, however, would have been fully aware that such private claims existed in the state laws when it crafted the preemption provisions that preserved those state law claims against deceptive or misleading messages. The implied preemption analysis of the *Beyond Systems, Inc.* Court (in dicta, since that case dealt with the claim of an ISP) supports the

---

[67] MD. CODE ANN. COM. LAW § 14-3002(b) (West 2007).

[68] *Id.* at § 14-3003. End users who receive such messages can recover $500 per email under the Maryland law, but have no claims under CAN-SPAM.

[69] *Beyond Sys., Inc.*, 422 F. Supp. 2d at 537.

[70] *Id*. at 538.

[71] WASH. REV. CODE § 19.190.020(1) (2007).

[72] WASH. REV. CODE § 19.86 (2007).

[73] Gordon v. Impulse Mktg. Group, Inc., 375 F. Supp. 2d 1040, 1045 (E.D. Wash. 2005).

[74] *Id.* (citing 15 U.S.C. § 7707(b)(1)).

outcome for James Gordon: "providing a civil remedy to the individual recipient . . . is fully in harmony with CAN-SPAM's enforcement mechanisms."[75]

In *Asis Internet Services. v. Optin Global, Inc.*,[76] defendants did not assert that the anti-spam claim under the California Business and Professions Code was preempted by CAN-SPAM. Instead, they asserted that both the CAN-SPAM claim and the state cause of action were fraud claims that must be pled with particularity under Federal Rule of Civil Procedure 9(b).[77] (Defendants in *Gordon* unsuccessfully pursued the same defense when their preemption arguments failed.[78]) The *Asis* Court, citing *Gordon*, disagreed that the California statute (as well as CAN-SPAM) reflected classic elements of fraud.[79] The Court found that CAN-SPAM and the California Code prohibit false or misleading subject lines or originating email addresses.[80] The *Asis* Court concluded that these prohibitions lacked several of the elements of a traditional common law fraud claim: knowledge of the falsity, materiality, intent to defraud, or reliance on the falsity.[81]

These conclusions reveal the importance of state statutory claims to spam recipients. Although CAN-SPAM preserved state tort claims such as fraud,[82] the statutory anti-spam claims are much easier to prove than a traditional fraud claim. Again, the statutory claims provide damages and attorney's fees that make the claims financially feasible, whereas claims for actual fraud damages may not be.

Although the cases above reveal that a plaintiff need not prove a defendant's actual knowledge of the falsity in a message, many state

---

[75] *Beyond Sys., Inc.*, 422 F. Supp. 2d at 538.

[76] Asis Internet Servs. v. Optin Global, Inc., 2006 WL 1820902 at *2–3 (N.D. Cal. 2006).

[77] FED. R. CIV. P. 9(b).

[78] *Gordon*, 375 F. Supp. 2d at 1047–48.

[79] *Asis Internet Servs.*, 2006 WL 1820902 at *13.

[80] *Id.* at *11.

[81] *Id.* at *13. The court dismissed the state claim without prejudice, however, because plaintiff had not asserted that the offending commercial emails "advertised" as required by the California law.

[82] *See generally* Jeffrey D. Zentner, *State Regulation of Unsolicited Bulk Commercial E-mail and the Dormant Commerce Clause,* 8 VAND. J. ENT. & TECH. L. 477 (2006) (analyzing Virginia's anti-spam statute).

law claims require a plaintiff to prove the sender knew or should have known the recipient of its message was in the relevant state with the anti-spam statute. Proof of this intra-state "nexus" justifies regulation by the particular state over the out-of-state business. These nexus standards, however, trigger complaints that the state laws unduly burden interstate businesses that are subjected to multi-state regulation.[83] Email senders' actual knowledge about a recipient's physical location in a particular regulating state is unlikely since the email address does not provide the recipient's physical address.

In a seminal case decided before CAN-SPAM was enacted, the Washington Supreme Court rejected a Commerce Clause challenge to the Washington Commercial Electronic Mail Act.[84] The Washington Act prohibits transmitting emails with false or misleading subject lines, origins, or transmission paths to an email address that the sender "knows, or has reason to know, is held by a Washington resident."[85] The Act goes on to state that a "person knows that the intended recipient . . . is a Washington resident if that information is available, upon request, from the registrant of the Internet domain name contained in the recipient's electronic mail address."[86] Identical or similar "knowledge" approaches are used in the anti-spam statutes of Arizona,[87] Florida,[88] Indiana,[89] Kansas,[90] Michigan,[91] Rhode Island,[92] West Virginia,[93] and Wyoming.[94] These state law provisions address

---

[83] *See infra* notes 84–103 and accompanying text.

[84] *Heckel*, 24 P.3d at 411–12.

[85] WASH. REV. CODE ANN. § 19.190.020(1) (2007).

[86] § 19.190.020(2).

[87] ARIZ. REV. STAT. § 44-1372.01(E)(2) (2006).

[88] FLA. STAT. ANN. § 668.606(4) (West 2007).

[89] IND. CODE ANN. § 24-5-22-7(A) (West 2006).

[90] KAN. STAT. ANN. § 50-6,107(D) (2005).

[91] MICH. COMP. LAWS ANN. § 445.2503 (2007).

[92] R.I. GEN. LAWS § 6-47-2 (2001).

[93] W. VA. CODE ANN. § 46A-6G-2 (West 2006).

[94] WYO. STAT. ANN. § 40-12-402(a)(2007). The Wyoming provision goes on to state that it will be enforced if the sender knew or had reason to know the recipient was located in a state

one of Congress's findings for the CAN-SPAM Act. Although email senders do not know where a recipient is located merely by his or her email address, these states have concluded that simply looking at the email address to determine applicable state laws is inadequate. A check of the ISPs records to know where the recipient is located is expected and justifiable.

Naturally, checking with the ISP for a recipient's home address is wholly inconsistent with spammers' *modus operandi* of snagging active email addresses from cyberspace and using them for mass, untargeted messages.[95] But, the whole point of anti-spam legislation is to discourage, disrupt and penalize spammers for doing business as usual. Accordingly, the burden of legal compliance in these states seems completely justifiable in light of the purpose behind these statutes (and CAN-SPAM as well).[96]

In *Pike v. Bruce Church, Inc.*, the U.S. Supreme Court established a two-part test to determine if a state law imposes an undue burden on interstate commerce.[97] First, the state must assert a legitimate state interest for its regulation. Then the state statutory burden on interstate commerce is weighed against the local benefit derived from the state law.[98] In explaining the state's legitimate interest in regulating unsolicited email, *State v. Heckel* detailed the commonly-cited harms to ISPs and email users.[99]

Regarding the second prong of the *Pike* test, the *Heckel* Court concluded that the only burden placed on interstate commerce by the

---

or other jurisdiction with laws similar to Wyoming's. *Id*. State laws that regulate outside their own territory have been deemed *per se* invalid. *See* Healy v. Beer Inst., 491 U.S. 324, 336 (1989).

[95] *See, e.g.,* Matthew Barakat, *Dissecting the M.O. of a Convicted Spammer,* INFO. WEEK, Nov. 14, 2005, http://informationweek.com/story/showArticle.jhtml?articleID=52601698.

[96] Other states' mandates are triggered simply by virtue of the email being received by a state resident or received on or through a computer or computer network in the state. *See* ARK. CODE ANN. § 4-88-603(a) (2007); CAL. BUS. & PROF. CODE § 17529.1(b) (West 2007); COLO. REV. STAT. § 6-2.5-105 (2006); CONN. GEN. STAT ANN. § 52-59b(5); 815 ILL. COMP. STAT. ANN. 511/10(b) (West 2007); IOWA CODE § 714E.1.5 (2007); OHIO REV. CODE ANN. § 2307.64(A)(10) (West 2007); OKLA. STAT. ANN. tit. 15, § 776.3 (2007); VA. CODE ANN. § 8.01-328.1 (2007). Pennsylvania's act is only triggered when the offending message is sent from a computer in the state. 73 PA. STAT. ANN. § 2250.3(a) (West 2007).

[97] Pike v. Bruce Church, Inc., 397 U.S. 137, 142 (1970).

[98] *Id*. at 143.

[99] *See supra* notes 13–30 and accompanying text.

Washington anti-spam law was "the requirement of truthfulness, a requirement that does not burden commerce at all but actually facilitates it by eliminating fraud and deception."[100] The Court further noted that the truthfulness requirements of the Washington Act did not conflict with the requirements of any other state law (nor of CAN-SPAM now). In other words, *Heckel* makes it clear that it does not matter whether the email advertiser expressly knows where its messages are being received and what state law is in effect there. As long as the sender knows its practices are not fraudulent, misleading, or deceptive, it can be confident it is in compliance wherever its messages are received.

In upholding the Maryland anti-spam law in *Beyond Systems, Inc.*,[101] the Maryland federal district court relied heavily on the *Heckel* analysis. Additionally, the Court concluded that the express provision in CAN-SPAM that preserves the states' power to regulate false and misleading emails proves that Congress was satisfied that "supplementary state legislation would impose no undue burden on interstate commerce."[102]

Clearly, these recent cases confirm that states are still empowered to regulate false and misleading email under state anti-spam statutes. Private parties retain their rights to pursue all tort claims against spammers. Further, ISPs have a private cause of action for violations of state laws regardless of the truth or falsity of the spam.[103] But consumer and business recipients of *truthful* unwanted messages remain without recourse against these costly forms of commercial speech. This gap in anti-spam protection is discussed next.

---

[100] *Heckel*, 24 P.3d at 411 (citing Jack L. Goldsmith & Alan O. Sykes, *The Internet and the Dormant Commerce Clause*, 110 YALE L. J. 785, 819 (2001)). *See also* Jaynes v. Commonwealth, 634 S.E.2d 357, 368 (Va. Ct. App. 2006) (upholding the Virginia Computer Crimes Act under the Commerce Power).

[101] *Beyond Sys., Inc.*, 422 F. Supp. at 533–35.

[102] *Id*. at 535.

[103] In these private claims under state law, plaintiffs still have to justify why the courts of that state can assert personal jurisdiction over an out-of-state defendant. *See* sources cited *supra* note 66 and accompanying text. Some of the same "knowledge" standards for liability under the state anti-spam statutes will also address whether the defendant "purposely availed" itself of the in-state market, justifying personal jurisdiction by the local courts. *See e.g.*, IOWA CODE § 714E.1.4(5) (2007) (expressly stating that transmitting to or through a computer in the state constitutes an act in the state for personal jurisdiction).

V. THE GAPING HOLE IN ANTI-SPAM REGULATION: PROTECTION FOR RECIPIENTS AGAINST UNWANTED, TRUTHFUL MESSAGES

What has preemption under CAN-SPAM actually accomplished? As the cases above illustrate, claims to address the false and misleading aspects of unwanted email are alive and well under both federal and state law. Senders of these messages are called upon to defend claims in numerous states subject only to the limits of the courts' ability to get personal jurisdiction over them.[104]

Nothing in CAN-SPAM, however, seems to address the deluge of truthful but unwanted commercial messages. So-called "law-abiding businesses" can send truthful mass emails with the necessary federal disclosures and opt-out notices. If these allegedly law-abiding businesses fail to honor those opt-out messages, however, they will only be subject to claims when a critical mass of complaints from recipients reaches the FTC, state attorneys general, or ISPs. Recipients still have no meaningful legal recourse to address the deluge of unwanted messages, such as credit card and mortgage offers, in the same inbox as messages from family and friends.

If supplementary state regulation of false and misleading spam does not impose an undue burden on interstate commerce, then how does state-by-state compliance unduly burden the senders of truthful but unwanted emails? The burden of state-by-state compliance does not change with the truthfulness or falsity of the messages. According to *Heckel*, different compliance requirements from state to state do not render state statutes an undue burden on interstate commerce if the cost of complying with those different mandates does not clearly outweigh the local benefits from the laws.[105]

Congress expressly preempted state anti-spam constraints on truthful messaging "because, since an electronic mail address does not specify a geographic location, it can be extremely difficult for law-

---

[104] *See* sources cited *supra* note 66 and accompanying text.

[105] *Heckel*, 24 P.3d at 412. Presumably, this analysis would have applied to state mandates for emails to include specific subject headings such as ADV or ADV ADULT, but for express preemption of those mandates under CAN-SPAM. As was noted above, a majority of states with anti-spam laws had adopted this particular subject line mandate. The remaining states' anti-spam laws did not adopt a varying mix of different subject line mandates, but rather none at all. In light of the significant costs associated with spam, the addition of ADV or ADV ADULT to an email subject line pursuant to state law would be easily defensible under the *Pike* test. State-by-state compliance with this fairly uniform standard would have been simple, cost-effective, and could have greatly improved spam filtering with little burden on interstate commerce.

abiding businesses to know with which of these disparate statutes they are required to comply."[106] While Congress simply accepted the obvious fact that email addresses do not include geographic locations, many states found that simple inquiries would permit so-called law-abiding businesses to know the recipient's geographic location. A check of the ISP's records to find out the recipient's location is expected or at least justifiable in the face of the unacceptable burdens spam imposes on email communications.

Again, the current business model used by spammers does not conceive of checking with an ISP for a recipient's home address and then determining if the advertising program meets the recipient's home state laws. However, regulations should alter the spammers' current model of blanketing any and all active email addresses with untargeted messages.

For businesses that engage in deceptive email tactics, it does not matter whether they know the specific states they are peppering with their mass-email transmissions. It is likely that their massive transmissions are landing in every state and they are likely to be liable for these tactics in every state with an anti-spam law. CAN-SPAM expressly permits this state enforcement. Why shouldn't the same regulatory burden apply to senders of mass messages that are truthful? Senders of truthful spam impose the same burdens on email systems and users. They too shift the costs of their advertising onto the recipient. Their messages still require that systems and users invest in filtering processes that risk the loss of wanted, non-spam messages. In other words, these truthful messages pose the same threats to the convenience and efficiency of this important and popular communications vehicle. But, the senders of these truthful mass messages face none of the state regulatory constraints that plaintiffs are utilizing against the senders of deceptive messages. These senders of truthful messages should be imputed with the same constructive knowledge as their deceptive counterparts that their mass messages are received in every state and, thus, are actionable under every state law.

Congress expressed concern about the burden on legitimate commerce from state regulation of unwanted, truthful spam. The real concern, however, should be about the burdens that all untargeted email messages impose on Internet users, themselves participants in interstate commerce. Federal legislation needs to completely upend the practice of spamming by imposing significant burdens that make unwanted commercial email an unprofitable marketing method.

---

[106] 15 U.S.C. § 7701(a)(11) (2000).

Congress should reinstate all the private rights of action under state laws that were preempted by CAN-SPAM. Individual recipients could then pursue statutory damages from any sender of spam who ignores opt-out messages, not just senders whose messages violate the deception prohibitions. Alternatively, Congress should create a meaningful private cause of action for recipients in a revised CAN-SPAM Act. This article concludes with a discussion of this recommendation.

VI. A NEW CLAIM FOR RECIPIENTS AGAINST UNWANTED COMMERCIAL EMAIL

The intrusiveness of unwanted direct telephone advertising has been successfully addressed by state and federal legislation that provides telephone customers with a variety of options, including registration on the state or federal do-not-call lists.[107] Many states' do-not-call and do-not-fax laws include a private cause of action,[108] as does the original federal telemarketing law, the Telephone Consumer

---

[107] The FTC's do-not-call list only protects consumers and does not apply to unsolicited fax advertising. The FCC regulates both telemarketing and fax advertising under the TCPA, which is not limited to consumers and provides a private cause of action for recipients of prohibited advertising. *See generally* FCC, *Fax Advertising: What You Need to Know*, http://www.fcc.gov/cgb/consumerfacts/unwantedfaxes.html (last visited Jan. 23, 2008). Upon enacting CAN-SPAM, Congress ordered the FTC to consider a government-enforced do-not-email list, akin to the highly popular federal and state do-not-call lists for unwanted telemarketing. In June 2004, after a brief investigation, the FTC decided not to establish a national do-not-email registry. The Commission concluded that existence of such a list could do more harm than good in preventing unwanted email solicitation because it would yield a trove of viable email addresses for spammers to access. *See* FTC, NATIONAL DO NOT EMAIL REGISTRY: A REPORT TO CONGRESS (2004), *available at* http://www.ftc.gov/reports/dneregistry/report.pdf. One commentator, however, notes that the existence of such a registry would allow registrants to associate their email address with a physical location, thereby giving notice to the sender of the state's law that applies to communications with that address and the state courts that would be taking jurisdiction over a violation of those statutes. *See* Hamel, *supra* note 40, at 987.

[108] ARIZ. REV. STAT. ANN. § 44-1482 (2006); CAL. BUS. & PROF. CODE § 17538.43(b)(2) (West 2007); LA. REV. STAT. ANN. § 51:1747(B) (2003); MICH. COMP. LAWS ANN. § 445.1776 (West 2002); MINN. STAT. ANN. § 325E.395(3) (2004); N.Y. GEN. BUS. LAW § 396-aa(2) (McKinney 2007); N.D. CENT. CODE § 51-07-23 (1999); S.C. CODE ANN. § 15-75-50(B) (2005); TEX. BUS. & COM. CODE ANN. § 35.47(f) (Vernon 2002); UTAH CODE ANN. §13-25a-107 (2005). Some states characterize violations of their do-not-call or do-not-fax laws as deceptive or unfair trade practices and provide private causes of action under their general trade statutes. *See e.g.*, COLO. REV. STAT. §6-1-906 (2006); IDAHO CODE ANN. §48-1003 (2003); 73 PA. STAT. ANN. § 2250.7 (West 2007).

Protection Act of 1991 ("TCPA").[109] The only constraint on consumer protection with respect to truthful advertising messages has come from the commercial speech doctrine. Telemarketers' claims of free speech rights have been tried and rejected as a constraint on the telemarketing regulatory mechanisms.[110] CAN-SPAM has also survived early commercial speech challenges.[111]

Congress should reinstate all of the private rights of action under state law that were preempted by CAN-SPAM or should create a private cause of action for spam recipients akin to what was created in the TCPA.[112] All recipients of any and all unwanted commercial email should be armed with significant remedies in individual or class action claims when opt-out requests are ignored (or worse, used to target the email address that was used to opt-out with even more spam). Consumers should be educated on how to preserve and pursue their claims.

Under the TCPA, a person who has received more than one telephone call within any 12-month period from the same entity after that person has "opted-out" may sue in state court and receive up to $500 in damages for each violation. A similar private cause of action for unwanted email could be easy for individuals and businesses to pursue and win because the paper trail is readily accessible (unlike a

---

[109] A person who has received more than one telephone call within any 12-month period by or on behalf of the same entity in violation of the regulations prescribed under this subsection may, if otherwise permitted by the laws or rules of court of a State bring in an appropriate court of that State:

(A) an action based on a violation of the regulations prescribed under this subsection to enjoin such violation,
(B) an action to recover for actual monetary loss from such a violation, or to receive up to $500 in damages for each such violation, whichever is greater, or
(C) both such actions.

47 U.S.C. § 227(c)(5) (2000).

[110] *See, e.g.,* Mainstream Mktg. Servs. v. FTC, 358 F.3d 1228 (10th Cir. 2004), *cert. denied*, 543 U.S. 812 (2004) (upholding the constitutionality of the national do-not-call list); *see also* Missouri *ex rel.* v. American Blast Fax, Inc. 323 F.3d 649 (8th Cir. 2003), *cert. denied*, 540 U.S. 1104 (2004) and Destination Ventures, Ltd. v. FCC, 46 F.3d 54 (9th Cir. 1995) (both upholding the constitutionality of the TCPA, specifically its prohibitions on unsolicited fax advertising).

[111] *White Buffalo Ventures, LLC*, 420 F.3d at 374–78.

[112] *See* sources cited *supra* note 107 and accompanying text.

phone log that consumers had to maintain to prove a claim under the TCPA).

Currently, recipients of unwanted email are often told not to use the opt-out mechanisms because these replies simply confirm to the spammer that they have found a valid, in-use email address to continue to target and to sell to other spammers.[113] This common advice shows just how ineffective the CAN-SPAM protection and remedies are if consumers are actually advised not to exercise the rights the statute provides. Arguably, if opt-out replies actually became the basis for meaningful remedies, spammers might not be so cavalier in their decisions to flaunt them. If recipients invoked meaningful opt-out remedies in the same numbers that they signed up for state and federal do-not-call lists, spammers might finally feel some meaningful deterrence.

Recipients could be advised to include in their opt-out requests a statement about their intention to invoke this private right of action in their specific home state. This informs the spammer of the physical residence where the spam has been received and where the opt-out protection is being invoked. Then if the opt-out message is ignored by the spammer, this notice and exchange of messages between the spammer and the recipient should be sufficient to justify personal jurisdiction over the spammer in the recipient's state courts, as well as prove the state or CAN-SPAM statutory violation.[114]

Presumably, these actions would likely only be asserted against the most egregious spammers that refuse to honor consumer opt-out requests. Congress could copy the affirmative defense it adopted under the TCPA for organizations that show they had meaningful systems in place for complying with opt-out requests.[115] In fact, many of the state anti-spam private causes of action provided affirmative defenses for businesses that mistakenly send offending emails if they had a system in place to prevent such violations.[116] These defenses

---

[113] *See* Maggs, *supra* note 49 and accompanying text.

[114] *See* sources cited *supra* note 66 and accompanying text.

[115] "It shall be an affirmative defense in any action brought under this paragraph that the defendant has established and implemented, with due care, reasonable practices and procedures to effectively prevent telephone solicitations in violation of the regulations prescribed under this subsection." 47 U.S.C. § 227(c)(5) (2000).

[116] It is an affirmative defense to a violation of this subchapter if a person can demonstrate that the sender at the time of the alleged violation had:

suggest that when states enacted anti-spam laws, they looked to the TCPA as a template for a system of remedies Congress would find appropriate. Nevertheless, the states found those remedies preempted by a federal system that provided nothing comparable for non-ISP recipients of truthful, unwanted email. Congress should rectify that approach now.

Some commentators might argue that the company-specific do-not-call mandate under the TCPA had a poor record for consumer satisfaction.[117] That dissatisfaction led states, and eventually the federal government, to adopt government-enforced do-not-call lists.

The major drawback to the private cause of action under the TCPA is its lack of an attorney's fees provision. This makes pursuing claims under the statute problematic for consumers. When a consumer wins a small claims judgment under the $500 per message statutory provision, there is no disincentive for the defendant to initiate a trial *de novo* in federal district court. At that point, defendants can inundate *pro se* plaintiffs with intimidating motions and the threat of a jury trial.[118]

Most state anti-spam laws provide attorney's fees with their private causes of action.[119] Extending the CAN-SPAM attorney's fees provision to a new private claim for individual recipients would motivate counsel to represent these plaintiffs and would deter specious legal defenses.

---

(1) Maintained a list of consumers who have notified the person not to send any subsequent commercial electronic messages;
(2) Established and implemented with due care and reasonable practices and procedures to effectively prevent unsolicited commercial electronic mail messages in violation of this subchapter;
(3) Trained the sender's personnel in the requirements of this subchapter; and
(4) Maintained records demonstrating compliance with this subchapter.

ARK. CODE ANN. § 4-88-606(c) (2007). *See also* IND. CODE ANN. § 24-5-22-10(c) (2006); KAN. STAT. ANN. § 50-6,107(k) (2005); MINN. STAT. ANN. § 325M.07 (2004).

[117] FTC Telemarketing Sales Rule, Final Amended Rule, 68 Fed. Reg. 4580, 4629 (2003) (to be codified at 16 C.F.R. pt. 310).

[118] *See* Brief for Electronic Privacy Information Center and Private Citizen, Inc. at 3–4, as Amici Curiae Supporting Appellee, Carnett's Inc. v. Hammond, 596 S.E.2d 729 (Ga. App. 2004) (No. S04G1241), *available at* http://www.epic.org/privacy/telemarketing/hammond.pdf.

[119] *See generally* National Conference of State Legislatures, *State Laws Relating to Unsolicited Commercial or Bulk Email (SPAM)*, updated Jan. 24, 2006, http://www.ncsl.org/programs/lis/legislation/spamlaws02.htm.

The TCPA private cause of action has been successfully invoked to tackle the problem of unsolicited text message advertisements to mobile communications devices.[120] This suggests that the TCPA model is a useful one for protecting modern communications. The TCPA, however, has been held to *not* apply to spam.[121]

Further, lawyers have used class action litigation under the TCPA to make its private cause of action more feasible.[122] While class actions have been criticized for rewarding attorneys more than victims,[123] they provide strong incentives for lawyers to pursue private consumer protection claims that could create meaningful deterrents to spammers who violate CAN-SPAM and the state law provisions.[124] For this reason, a class action provision should also be expressly established in any new anti-spam claim for recipients. Again, if anti-spam legislation included meaningful remedies, spammers might finally be deterred in their flagrant violations of federal and state law.

---

[120] *See, e.g.,* Joffe v. Acacia Mortgage Corp., 121 P.3d 831, 835 (Ariz. App. 2005).

[121] Aronson v. Bright-Teeth Now, L.L.C., 824 A.2d 320, 323 (Pa Super. Ct. 2003). Plaintiff sued Bright-Teeth under the TCPA in state court after receiving six unsolicited emails. The TCPA prohibits "using a telephone facsimile machine, computer or other device to send an unsolicited advertisement to a telephone facsimile machine." *Id.* at 321 (quoting 47 U.S.C. § 227(b)(1)(C)). Aronson claimed that his personal computer fell within the definition of a "telephone facsimile machine." The Court held that the TCPA does not apply to spam. *See also* Bobby Kerlik, *Man Awarded $89,100 in Fight to Can Spam,* TRIB.-REV. (Pittsburg, Pa.), Oct. 11, 2006, *available at* http://www.pittsburghlive.com/x/pittsburghtrib/news/cityregion/s_474476.html (discussing Aronson's use of the Pennsylvania anti-spam law to tackle unwanted email).

[122] Accounting Outsourcing, L.L.C. v. Verizon Wireless Personal Comm'ns, L.P., 329 F. Supp. 2d 789, 802–3 (M.D. La. 2004). *See also* Hooters of Augusta, Inc. v. Nicholson, 537 S.E.2d 468, 469 (Ga. Ct. App. 2000).

[123] *See generally* Edward F. Sherman, *Complex Litigation: Plagued by Concerns Over Federalism, Jurisdiction and Fairness,* 37 AKRON L. REV. 589 (2004); *see also* Susan D. Susman, *Class Actions: Consumer Sword Turned Corporate Shield?,* 2003 U. CHI. LEGAL F. 1 (2003).

[124] *See* Sherman, *supra* note 123, at 592; *see also* Stephen Berry, *Ending Substance's Indenture to Procedure: The Imperative for Comprehensive Revision of the Class Damage Action*, 80 COLUM. L. REV. 299, 299–300 (1980) (small claimant class actions promote deterrence, but not compensation); David Rosenberg, *Adding a Second Opt-Out to Rule 23(b)(3) Class Actions: Cost Without Benefit,* 2003 U. CHI. LEGAL F. 19 (2003) (arguing that class actions in mass tort cases provide important economies of scale and ensure the best possible deterrence of defendants, but opt-outs reduce the effectiveness of the class action as a deterrent).

VII. CONCLUSION

When CAN-SPAM was originally passed, it was widely criticized for its anemic consumer protection.[125] So far, most enforcement under the law is targeted at false and deceptive messages.[126] The federal law has little or no effect on truthful unwanted messaging that email users find so frustrating and time-consuming. It is time for Congress to improve on this initial legislation.

In its findings supporting CAN-SPAM, Congress found that technological and legislative tools (including international responses) were necessary to fight spam. Many argue that the only real way to tackle spam is through technological solutions.[127] Similar arguments were made about blocking telemarketing calls with technology.[128] But states' do-not-call laws empowered individual consumers against that unwanted commercial speech. In other realms like product safety and personal security, society uses technology to prevent harms, but still permits individuals to sue those who commit harms regardless of technological advances. The advent of seatbelts, airbags and burglar alarms did not eliminate private claims for damages against bad drivers and thieves.

---

[125] *See* Zhang *supra* note 35, at 319–20; *see also* John W. Daniel, *Has Spam Been Fried? Why the CAN-SPAM Act of 2003 Can't: Regulation of Unsolicited Commercial Electronic Mail and the CAN-SPAM Act of 2003*, 94 KY. L.J. 363 (2005/2006); Thomas K. Ledbetter, *Stopping Unsolicited Commercial E-mail: Why the CAN-SPAM Act is Not the Solution to Stop Spam*, 34 SW. U. L. REV. 107 (2004).

[126] Twelve of the twenty FTC actions to enforce CAN-SPAM included claims of false or misleading transmission information under 15 U.S.C. § 7704(a)(1) or deceptive subject lines under 15 U.S.C. § 7704(a)(2). FTC, *supra* note 50.

[127] "No single law or method is going to stop spam. Because of the intangible and boundary-less nature of the Internet a technical solution and international solution is necessary." Grant A. Yang, *CAN-SPAM: A First Step to No-Spam,* 4 CHI.-KENT J. INTELL. PROP. 1, 2 (2004), *available at* http://jip.kentlaw.edu/archives.asp?vol=4&iss=1. "The inexorable rise in the volume of unsolicited commercial electronic messages and the inherent limitations of regulatory regimes make a technical solution to combating spam imperative." Taiwo Oriola, *Regulating Unsolicited Commercial Electronic Mail in the United States and the European Union: Challenges and Prospects,* 7 TUL. J. TECH. & INTELL. PROP. 113, 164 (2005).

[128] "[M]any new technologies provide alternatives to a complete ban, indicating that Congress has not chosen a solution that fairly balances consumers' interest in privacy with ADAD users' rights to free speech." Howard E. Berkenblit, *Can Those Telemarketing Machines Keep Calling Me?—The Telephone Consumer Protection Act after* Moser v. FCC, 36 B.C. L. REV. 85, 109 (1994). *See also*, Note*, The Impermeable Life: Unsolicited Communications in the Marketplace of Ideas*, 118 HARV. L. REV. 1314, 1336 (2005).

Nothing about spam suggests that it is such a uniquely vexing technological problem that statutory remedies crafted by the states need to be preempted, especially when Congress provides nothing comparable in CAN-SPAM. Congress never explained why the private litigation tool that was established by most state statutes was preempted for spam recipients. Congress allowed individual tort claims to remain in effect, but, for no obvious reason, wiped out the individual claims for statutory damages.

The traditional self-help role of individual litigation should be resurrected to tackle this modern communications problem. Businesses and individuals, when armed with meaningful legal rights, can have a real impact on stemming the tide of unwanted commercial email.