Vanderbilt Journal of Entertainment & Technology Law

Volume 14
Issue 1 *Issue 1 - Fall 2011*

Article 6

2011

Silence of the Spam: Improving the CAN-SPAM Act by Including an Expanded Private Cause of Action

David J. Rutenberg

Silence of the Spam: Improving the CAN-SPAM Act by Including an Expanded Private Cause of Action

ABSTRACT

In the last decade, email spam has become more than just an annoyance for email users. Unsolicited messages now comprise more than 95 percent of all email sent worldwide. This costs US businesses billions of dollars in lost productivity each year. The US Congress passed the CAN-SPAM Act of 2003 to regulate the spam industry. Unfortunately, data show that spam only increased since the Act's passage. Part of the reason for this failure is that the Act only authorizes the Federal Trade Commission, state attorneys general, and Internet Service Providers to bring action under its provisions. Each of these authorized entities either lacks the incentive or the resources to adequately enforce the Act, resulting in little to no reduction of spam. As a result, email recipients—not spammers—bear the cost of spam. This Note argues that the Act should incorporate an expanded private cause of action for email recipients, thereby increasing the enforcement level. This will deter spam prospectively by shifting the cost of unsolicited email from the recipient onto the sender.

TABLE OF CONTENTS

"We invite you to come see the 2020 and hear about the DECSystem-20 family." With that one line, composed in 1978 and sent to six hundred users of the pre-Internet ARPANET network, spam was born.[1] Gary Thurek, the author of this message and marketing manager of Digital Equipment Corporation, made more than $20 million for his computer company through this solicitation.[2] Almost immediately, other ARPANET users criticized Thurek for his unsolicited message.[3]

Despite this early start, modern spam[4] failed to take off until April 12, 1994, when two lawyers from Arizona, Laurence Canter and

1. Michael Specter, *Damn Spam*, NEW YORKER, Aug. 6, 2007, http://www.newyorker.com/reporting/2007/08/06/070806fa_fact_specter.

2. *Id.* ARPANET, short for the Advanced Research Projects Agency Network, was the precursor to the modern-day Internet and consisted mainly of government and university computers. At the time, users numbered only in the thousands, but their addresses were kept in a central contact list. Thurek, whose company was headquartered in Massachusetts, wanted to reach the West Coast technology sector to advertise events where DEC's computers would be demonstrated and sold for roughly $1 million each. The company sold more than twenty machines, thanks to the message. *Id.*

3. *Id.*

4. The term "spam," as applied to unsolicited commercial email, comes from a popular 1970 sketch created and performed by the British comedy troupe, Monty Python. In the sketch, a group of Vikings continually sings a song containing lyrics consisting solely of the word "spam," which drowns out all other conversation, much like how email spam can drown out legitimate email. Erika H. Kikuchi, Note, *Spam in a Box: Amending CAN-SPAM & Aiming Toward a Global Solution*, 10 B.U. J. SCI. & TECH. L. 263, 264 (2004); *see also Spam*, PYTHONLINE.COM (2009), http://pythonline.com/youtube_archive/spam.

his wife, Martha Siegel, sent a message to twenty million Internet users offering them immigration services.[5] Although the couple's spam provoked harsh reactions from network users and eventually resulted in termination of their Internet access by their Internet Service Provider (ISP), the couple claims to have earned $100,000 from the email.[6]

In less than two decades since the Canter-Siegel message, spam has grown to dominate email distribution, now comprising roughly 76 percent of all email sent worldwide.[7] This translates into ninety-three billion emails sent each day.[8] In the United States, spam accounted for 73.8 percent of all email traffic in October 2011.[9] Just ten years ago, according to Congressional findings, spam comprised only 7 percent of all email traffic.[10] This dramatic increase now represents more than mere annoyance to average email users. Spam is a huge burden on commercial entities, with an estimated annual cost to US businesses of $71 billion in lost productivity.[11] In 2007, the average business email user received twenty-one spam messages per day and spent 1.2 percent of his workday identifying and deleting such messages.[12] This cost will probably increase as the spam volume continues to rise both as a percentage of email sent and in real numbers.[13]

Spam's impact extends beyond everyday annoyances and lost worker productivity.[14] It has an increasingly detrimental impact on the environment, using thirty-three terawatt hours globally each year.[15] This is the amount of energy 2.4 million US homes would use annually.[16] Moreover, spam contributes seventeen million metric tons

---

5. Philip Elmer-DeWitt, *Battle for the Soul of the Internet*, TIME, Mar. 18, 2005, http://www.time.com/time/magazine/article/0,9171,981132,00.html.

6. *Id.*

7. COMMTOUCH, INTERNET THREATS TREND REPORT OCTOBER 2011 6 (2011), http://www.commtouch.com/download/2178.

8. *Id.*

9. SYMANTEC.CLOUD, OCTOBER 2011 INTELLIGENCE REPORT 7 (Oct. 2011), http://www.symanteccloud.com/mlireport/SYMCINT_2011_10_October_FINAL-en.pdf.

10. 15 U.S.C. § 7701(a)(2) (2006).

11. NUCLEUS RESEARCH, INC., Doc. No. H22, SPAM: THE REPEAT OFFENDER 5 (Apr. 2007), http://nucleusresearch.com/research/notes-and-reports/spam-the-repeat-offender (click "Download").

12. *Id.* at 1.

13. CISCO SYSTEMS, INC., CISCO 2010 MIDYEAR SECURITY REPORT 30 (2010), http://www.cisco.com/en/US/prod/collateral/vpndevc/security_annual_report_mid2010.pdf.

14. MCAFEE, INC., THE CARBON FOOTPRINT OF EMAIL SPAM REPORT (2009), http://resources.mcafee.com/content/NACarbonFootprintSpam (follow "Submit"; then follow "English Full 28-Page Report").

15. *Id.* at 3.

16. *See id.*

of the greenhouse gas, carbon dioxide, each year.[17] This accounts for 0.2 percent of global annual carbon dioxide emissions or the equivalent of emissions from 1.5 million US homes.[18]

The private sector responded to the rising tide of spam through a range of methods and proposals intended to reduce it—most of which have failed or are otherwise untenable.[19] Approaches include email postage where customers interested in the service pay a nominal fee, usually less than one cent, to ensure that the message reaches the recipient's inbox.[20] While these costs are negligible for those sending legitimate email, spammers sending millions of emails would find the costs prohibitive.[21] However, this method does not actually stop junk mail; rather, it ensures that users receive legitimate email.[22]

One common technology-based approach to spam reduction is a spam filter, which can identify spam before it reaches the intended recipients' inboxes.[23] Spam generally must pass through multiple spam filters from the moment it is sent until the time it is received.[24] Some filters block messages from known spammers, while other filters can scan individual emails' content to determine if it is spam.[25] However, spammers continually update their methods to fool both electronic spam filters and end users to ensure that the email not only reaches the inbox, but also that the user views the message.[26] Often, this entails using false or misleading information in the subject headers, sender information, and body to deceive electronic filters and human recipients.[27]

Despite these and other tactics, electronic filtering software successfully blocks roughly 95 percent of all spam.[28] Considering that

---

17. *Id.* Sources for energy use and carbon dioxide production include: harvesting addresses, creating spam campaigns, sending and transmitting spam, receiving spam, storing the messages, viewing and deleting spam, filtering spam, and searching for legitimate software miscategorized by spam filters. *Id.*

18. *Id.*

19. *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, 171-74 (2008) (providing an overview of proposed non-legal solutions to the spam problem).

20. *Id.* at 171; MacGregor Campbell, *Pay-Per-Email Plan to Beat Spam and Help Charity*, ABC NEWS (Aug. 13, 2009), http://abcnews.go.com/Technology/story?id=8318609.

21. Soma et al., *supra* note 19, at 171.

22. *Id.*

23. Adam Hamel, Note, *Will the CAN-SPAM Act of 2003 Finally Put a Lid on Unsolicited E-mail?*, 39 NEW ENG. L. REV. 961, 971-74 (2005).

24. *Id.*

25. *Id.* at 973.

26. *Id.*

27. DIV. OF MKTG. PRACTICES, U.S. FED. TRADE COMM'N, FALSE CLAIMS IN SPAM 2-12 (Apr. 30, 2003), *available at* http://www.ftc.gov/reports/spam/030429spamreport.pdf.

28. Specter, *supra* note 1.

spammers usually get fifteen positive replies for every million spam messages sent, electronic filtering software merely forces spammers to increase the number of emails sent.[29] This is a negligible cost for the sender.[30] This only increases the power burden on servers and other equipment and forces companies to sink more resources into spam protection.[31] The burden is further increased on the final spam filter—the spam recipient—who uses sixteen seconds on average to determine if a given message is spam.[32] Lastly, concerns linger about "false positives," email that filtering software incorrectly identifies as spam.[33] This contributes to additional lost time and lowered productivity resulting from the search for legitimate emails that, unbeknown to the intended recipient, the server did not deliver.[34]

Recognizing that private sector remedies alone failed to stem spam's rising volume, Congress passed the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 ("CAN-SPAM Act" or "the Act").[35] The Act failed to reduce spam.[36] This Note will argue that in order to better curb the continued propagation and expansion of unsolicited commercial email (UCE), Congress should amend the CAN-SPAM Act to allow for a private cause of action by individual computer users who receive spam. While the Act could benefit from a myriad of improvements to reduce spam, this Note will consider only the addition of a private cause of action.

Part I of this Note will provide an overview of CAN-SPAM's regulatory framework. Part II will discuss why CAN-SPAM's enforcement provisions failed to curtail spam's growth and why common tort law does not provide an adequate cause of private action within the spamming context. Part III will propose an expanded cause of private action for individual email users as a means to shift costs—or potential costs—off of the recipient and onto the spammer. Part IV will conclude by acknowledging that, while an expanded right of private action is not a silver-bullet solution, it provides a reasonable first step to combatting spam through established legal mechanisms.

---

29. *Id.*

30. *Id.*

31. MCAFEE, *supra* note 14; NUCLEUS RESEARCH, *supra* note 11.

32. NUCLEUS RESEARCH, *supra* note 11, at 2.

33. Saul Hansell, *The High, Really High or Incredibly High Cost of Spam*, N.Y. TIMES, July 29, 2003, *available at* http://www.lexisone.com/balancing/articles/n080003d.html.

34. *Id.*

35. 15 U.S.C. §§ 7701-7713 (2006).

36. Kikuchi, *supra* note 4; Soma et al., *supra* note 19.

I. OVERVIEW OF THE CAN-SPAM ACT: REGULATION, NOT PROHIBITION

The CAN-SPAM Act recognizes that mass email can play a significant role in the domestic and global economy.[37] In response, the Act regulates "commercial electronic mail" messages rather than banning them entirely.[38] Specifically, CAN-SPAM seeks to regulate email through certain requirements related to content and transmission and how the sender obtained recipients' email addresses.[39]

A. Regulation through Criminal Liability and Statutory Penalties

The Act enables the US Sentencing Commission to review or amend penalties and sentencing guidelines when spammers evade filters or obtain email addresses through "improper means."[40] The Act contains a number of provisions regulating UCE content.[41] For instance, email cannot contain false, misleading, or deceptive information in the "header" or "subject" lines.[42] Any commercial email must contain a functioning return email address or other electronic mode of contact.[43] Moreover, commercial email senders must include a valid physical return address within their emails.[44] Each commercial email must contain a "clear and conspicuous" identifier, indicating that the message is an advertisement or solicitation.[45] Commercial email that contains sexually oriented material must include a warning in the subject heading that is viewable before opening the email.[46] Moreover, the email must contain notice of the opportunity to opt out of future mailings.[47] The Act prohibits sending

---

37. 15 U.S.C. § 7701(a)(1) ("[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.").

38. *Id.* § 7702(2)(a) (defining "commercial electronic mail message" as "any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service (including content on an Internet website operated for a commercial purpose)").

39. *Id.* § 7701.

40. *Id.* § 7703; 18 U.S.C. § 1037 (2006) (providing penalties for email fraud).

41. 15 U.S.C. § 7701(a).

42. *Id.* § 7704(a)(1)-(2); *see also* 149 CONG. REC. S15,946 (daily ed. Nov. 25, 2003) (statement of Sen. Leahy) (noting that the Act bars individuals from forging "header information," by falsifying information about the origin of the email message and its route between the sender and the recipient).

43. 15 U.S.C. § 7704(a)(3).

44. *Id.* § 7704(a)(5).

45. *Id.*

46. *Id.* § 7704(d).

47. *Id.* § 7704(a)(5).

additional commercial email messages to recipients who already opted out of receiving additional mailings.[48]

In addition to its content provisions, the CAN-SPAM Act regulates the methods spammers use to obtain recipient email addresses and to create recipient lists.[49] The Act criminalizes unauthorized access to computers for the purpose of obtaining email addresses or using others' computers to send email.[50] Senders may not randomly generate email addresses in an attempt to create valid recipient addresses.[51] They are further prohibited from using an automated means to create a multitude of email accounts from which to send spam.[52] Lastly, the Act outlaws relay of commercial email through a computer or computer network that the sender is unauthorized to use.[53]

The Act permits criminal fines and imprisonment for up to five years for violators of its provisions.[54] Given the difficulty of locating individual spammers, the Act primarily aims at general deterrence thereby preventing spam from being sent at all.[55]

B. Enforcement of CAN-SPAM Provisions: Actions by Federal Agencies, States, and ISPs Only

The CAN-SPAM Act provides that the Federal Trade Commission (FTC) is the primary enforcement authority for most of the Act's regulatory provisions.[56] The Act also reserves authority for certain other federal agencies when the particular spam is related to

---

48. *Id.* § 7704(a)(4).

49. *Id.* § 7704(b).

50. *Id.* § 7703(b)(1)(A)(i).

51. *Id.*

52. *Id.* § 7704(b)(2); *see also* 149 CONG. REC. S15,946-47 (daily ed. Nov. 25, 2003) (statement of Sen. Leahy) (noting that this provision criminalizes "account churning," a technique by which spammers register large quantities of email accounts using false information in order to evade detection by ISP software filters).

53. 15 U.S.C. § 7704(b)(3); *see also* 149 CONG. REC. S15,947 (daily ed. Nov. 25, 2003) (statement of Sen. Leahy) (explaining that spammers often hijack IP addresses to "falsely assert that they have the right to use a block of IP addresses, and obtain an Internet connection for those addresses" to hide behind them).

54. 15 U.S.C. § 7704(d)(5); 18 U.S.C. § 1037(b) (2006).

55. *See* 149 CONG. REC. S13,023 (daily ed. Oct. 22, 2003) (statement of Sen. Wyden) ("[W]e give a role to the State attorneys general, the Internet service providers – when this bill is signed into law, to bring a handful of actions very quickly to establish that for the first time there is a real deterrent, there will be real consequences when those big-time spammers try to exploit our citizens.").

56. 15 U.S.C. § 7706(a). The Act directs the FTC to treat a violation of its statutory provisions as if it were an "unfair or deceptive act or practice proscribed" defined under 15 U.S.C. § 57a(a)(1)(B), which provides authority to the FTC to promulgate and enforce rules for acts that affect commerce. *Id.*

the work of those agencies.[57] Additionally, the Act gives the Department of Justice (DOJ) authority to enforce the Act's criminal provisions.[58]

In addition to granting broad authority to the FTC, the Act also grants limited authority to the states through state attorneys general.[59] States may bring civil actions in cases where spammers send email messages that contain false or misleading information or include sexually explicit content without the requisite warnings.[60] The Act also enables states to enforce the opt-out provisions and the requirement to include a return email address.[61] States may sue on behalf of their citizens for injunctive relief.[62] Additionally, states may sue for monetary damages on behalf of their residents.[63] The Act provides a penalty of $250 per violation, which is defined as "each separately addressed unlawful message received by or addressed to such residents."[64] However, the Act limits the total amount that may be collected to $2 million.[65] In cases where the states bring legal action against accused spammers, the FTC retains the right to intervene.[66]

While the Act authorizes multiple government entities to enforce its provisions, the only private parties that may file suit are ISPs adversely affected by certain CAN-SPAM violations.[67] Similar to the limited causes of action granted to states, the Act allows ISPs to sue based only on a subset of the provisions on which FTC may bring action.[68] Specifically, the Act allows ISPs to sue if they can show that spammers sent email with false header information or "from" lines, used misleading subject headings, or included sexual content without the required warnings.[69] The Act also provides ISPs a cause of action if spammers fail to include an opt-out mechanism or continue to send

57. *Id.* § 7706(b). Other federal agencies that the Act grants authority to include the Office of the Comptroller of the Currency, the Federal Reserve Board, the Federal Deposit Insurance Corporation, the National Credit Union Administration, and the Securities and Exchange Commission, among others. *Id.*

58. *Id.* § 7703(c)(2).

59. *Id.* § 7706(f)(1).

60. *Id.* § 7706(f)(1) (referencing §§ 7704(a)(1)-(2), 7704(d)).

61. *Id.* § 7706(f)(1) (referencing § 7704(a)(3)-(5)).

62. *Id.* § 7706(f)(1)(A).

63. *Id.* § 7706(f)(1)(B).

64. *Id.* § 7706(f)(3)(A).

65. *Id.* § 7706(f)(3)(B).

66. *Id.* § 7706(f)(5).

67. *Id.* § 7706(g).

68. *Id.* § 7706(g)(1).

69. *Id.*

spam after consumers exercise the opt-out function.[70] Depending on the particular violation, the Act provides for penalties ranging between twenty-five and one hundred dollars per violation up to a limit of $1 million.[71] The CAN-SPAM Act does not provide a cause of action to private non-ISP Internet users like individuals or corporations.[72]

C. The Do-Not-E-Mail Registry and its Subsequent Rejection

Congress ordered the FTC to produce a feasibility report on the Do-Not-E-mail Registry and authorized the agency to implement such a registry if practicable.[73] Congress's interest in the Do-Not-E-mail Registry was in response to the recently implemented Do-Not-Call Registry.[74] The Do-Not-Call Registry provides individuals who place their phone numbers on the list a private cause of action granting them at least $500 for each call received from uninvited solicitous callers.[75]

The Do-Not-E-mail Registry would have given businesses and individuals the ability to register entire domain names to prevent receiving spam.[76] This Registry may also have served as a vehicle for a private cause of action for individual spam recipients, not unlike the Do-Not-Call Registry.[77] While the CAN-SPAM Act does not contain many specific provisions regarding the Do-Not-E-mail Registry's precise form, it provides considerable discretion to the FTC to develop an implementation plan.[78]

However, the FTC declined to implement a Do-Not-E-mail Registry, pointing to the email system's technical limitations and privacy concerns associated with creating a centralized list of email

---

70. *Id.*

71. *Id.* § 7706(g)(8).

72. *See* 149 CONG. REC. H12,193 (daily ed. Nov. 21, 2003) (statement of Rep. Sensenbrenner) ("[T]here is specific language in the bill limiting this authority to law enforcement officials or agencies of the State, and it is not the intent of Congress to allow outsourcing of this truly State function to the plaintiff's bar.").

73. 15 U.S.C. § 7708.

74. *See* 149 CONG. REC. S13,041 (daily ed. Oct. 22, 2003) (statement of Sen. Pryor) (noting the similarity between unwanted phone calls and spam and the potential for a Do-Not-Spam Registry).

75. 47 U.S.C. § 227(b)(3) (2006).

76. U.S. FED. TRADE COMM'N, NATIONAL DO NOT EMAIL REGISTRY: A REPORT TO CONGRESS 14-15 (June 2004) [hereinafter FTC NATIONAL DO NOT EMAIL REGISTRY], *available at* http://www.ftc.gov/reports/dneregistry/report.pdf.

77. *See* 149 CONG. REC. S13,025 (daily ed. Oct. 22, 2003) (statement of Sen. Schumer) (likening the cause of action in a potential Do-Not-E-mail registry to that of the Do-Not-Call registry).

78. 15 U.S.C. § 7708(b).

addresses.[79] Specifically, the FTC found that, unlike with phone callers, email senders could easily alter the header information associated with the origin of the email.[80] This makes it nearly impossible to locate the sender of potential spam for purposes of prosecution.[81] Moreover, spammers value a centralized list of valid email addresses because, unlike phone numbers, tracking down or generating valid email addresses is incredibly difficult.[82] Cognizant of spammers' desire to obtain such a list, the FTC expressed concerns about its ability to fully protect the list and ultimately concluded that a Do-Not-Spam Registry was impracticable without improved protection mechanisms.[83]

D. Preemption of State Spam Laws

The CAN-SPAM Act explicitly preempts state spam statutes, bringing national spam regulation exclusively under the Act's regulatory and enforcement framework.[84] Federal preemption of state spam laws reflects Congress's concern that a patchwork of state laws neither provides an effective regime to regulate and curb spam nor appropriately recognizes that spam is an interstate issue that requires a single regulatory framework.[85] The Act does not, however, preempt other state laws not specific to email that may otherwise be enforced against spam, including "[s]tate trespass, contract, or tort law."[86] Additionally, CAN-SPAM does not preempt state laws that relate to computer fraud and other types of computer crime.[87]

---

79. FTC NATIONAL DO NOT EMAIL REGISTRY, *supra* note 76, at 15-18.

80. *Id.* at 12-13.

81. *Id.*

82. *Id.* at 16-17. The Report notes that spammers may try to generate email addresses by using "dictionary attacks" that generate random alphanumeric email addresses similarly to an automatic dialer. *Id.* at 17. However, dictionary attacks tend to be less successful than an automatic dialer because of the number of possible alphanumeric combinations that make up an email addresses compared to the set number of possible phone numbers in existence. *Id.* As a result, a large number of valid email addresses would be extremely valuable to spammers. *Id.*

83. *Id.* at 18.

84. 15 U.S.C. § 7707(b)(1) (2006) ("This Act 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 . . . .").

85. *Id.* §§ 7701(a)(11), 7701(b)(1); *see also* 149 CONG. REC. S13,023 (daily ed. Oct. 22, 2003) (statement of Sen. Wyden) ("But I believe a State-by-State approach cannot work in this area. The numerous State laws to date certainly have not put in place a coordinated effort against spam . . . . What is needed is a uniform, nationwide spam standard to put the spammers on notice and to empower the consumers to have an enforcement regime consistent with their reasonable expectations.").

86. 15 U.S.C. § 7707(b).

87. *Id.* § 7707(b)(2)(B) (providing that the Act does not preempt "other State laws to the extent that those laws relate to acts of fraud or computer crime").

II. CAN-SPAM'S ENFORCEMENT FAILURE: A QUESTION OF ECONOMICS AND INCENTIVES

While there are numerous possible explanations for why spam continues to grow, part of the problem stems from the Act's failure to adequately address the particular costs and incentives of all the players in the spam industry.[88] This failure to recognize the economics of the spam industry short-circuited Congress's goal in deterring potential spammers from sending spam in the first place.[89] During floor debate highlighting the proposed CAN-SPAM bill, Senator Ron Wyden presciently noted: "It is clear this Congress must act, but we should make no mistake—unless we can effectively enforce the laws we write, those laws will have little meaning or deterrent effect on any would-be purveyor of spam."[90] This Part discusses the economics of the spam industry as a basis for why CAN-SPAM's three primary enforcement mechanisms—as well as tort and state law not preempted by CAN-SPAM—failed to sufficiently shift the cost incentives enough to deter spammers from continuing and increasing the number of spam messages sent since the Act's passage nearly a decade ago.[91]

A. The Economics of the Spam Industry: Low Costs Plus Limited Attention Spans Equals More Spam

The key difference between email spam on the one hand and telemarketing and traditional junk mail on the other is that the marginal cost of sending one email is negligible to the spammer, whereas telephone and traditional mail involves significant investment of time and money per message.[92] Additionally, the little cost associated with sending one more email message falls harder on the recipient than on the spammer.[93] This is called the "recipient pays" economic paradigm.[94] A recipient pays paradigm differs from a "sender pays" paradigm in that the recipient of the unwanted message

88. Alex C. Kigerl, *CAN SPAM Act: An Empirical Analysis*, 3 INT'L J. CYBER CRIMINOLOGY 566, 576 (2009).

89. *See supra* note 55 (explaining Congressional intent to deter spam through included statutory mechanisms).

90. 149 CONG. REC. S13,023 (daily ed. Oct. 22, 2003) (statement of Sen. Wyden).

91. *Supra* text accompanying notes 7-13.

92. *See* Robert K. Plice et al., *Spam and Beyond: An Information-Economic Analysis of Unwanted Commercial Messages*, 18 J. ORGANIZATIONAL COMPUTING & ELECTRONIC COM. 278, 279 (2008).

93. *See, e.g.*, Eric Allman, *The Economics of Spam*, QUEUE 78 (Jan. 29, 2004), *available at* http://portal.acm.org/ft_gateway.cfm?id=966799&type=pdf.

94. *Id.*

shoulders the economic burden of the last marginal email sent rather than the emailer.[95] This contrasts to other forms of media, which require larger investments of time and money—through the use of stamps, long-distance charges, etc.—to send each additional letter or make each additional phone call.[96]

This economic paradigm incentivizes spammers to send increasingly more emails to recipients in the hopes of maximizing spam profits, which are based on the quantity—not quality—of emails sent.[97] The recipient pays principle leads to poorly targeted emails often having little connection to the recipients' actual interests because it is cheaper to send a larger quantity of email than to conduct market research or otherwise tailor individual messages.[98] This *de minimis* marginal cost, paired with little concern for overall public image, incentivizes spammers to send as many individual email messages as possible in order to receive sufficient quantities of responses to turn a profit.[99]

Meanwhile, spam recipients pay a disproportionate amount of time and attention for each marginal email received as compared to spammers.[100] Economists view attention span as a finite resource, which, if overused by spammers, will result in a depletion of attention available for each additional spam message.[101] Since the first step in gaining profit from spam requires that the recipient pay attention to

---

95. Plice et al., *supra* note 92, at 279; *see also* Brett A.S. Martin et al., *Email Advertising: Exploratory Insights from Finland*, 43 J. ADVERTISING RES. 293, 293 (2003) (noting that email costs senders $5 to $7 per thousand emails sent while traditional mail costs $500 to $700 per thousand units sent); *infra* note 140 and accompanying text.

96. Martin et al., *supra* note 95.

97. Kigerl, *supra* note 88, at 576.

98. Plice et al., *supra* note 92, at 279.

99. Timothy J. Muris, Chairman, Fed. Trade Comm'n, Remarks at the Aspen Summit: Cyberspace and the American Dream (Aug. 19, 2003), http://www.ftc.gov/speeches/muris/030819aspen.shtm ("This shifting of costs encourages inefficiency because the total cost to send tens of millions of emails, if borne by the spammer, would presumably outweigh the proceeds that most spam generates. Yet at our Spam Forum, a bulk emailer testified that he could profit even if his response rate was less than 0.0001%."); *see also* Oleg V. Pavlov et al., *Mitigating the Tragedy of the Digital Commons: The Problem of Unsolicited Commercial Email*, 16 COMM. ASS'N FOR INFO. SYS. 73, 81 (2005).

100. *See supra* notes 11-12 and accompanying text.

101. *Id.*; *see also* Garrett Hardin, *The Tragedy of the Commons*, 162 SCIENCE 1243 (1968). Hardin developed the idea of "the tragedy of the commons," which is a situation where multiple individuals, acting in their own best interests, utilize a free and open common-pool resource in such a way that the resource eventually becomes depleted through their collective action because the marginal cost of utilizing one more unit of that resource is negligible to each individual. Hardin, *supra*. The quintessential illustration of the tragedy of the commons is a grazing field that eventually becomes depleted because individual ranchers continually add their cows to the field at no marginal cost and are therefore not incentivized as individuals to limit the number of cows sent to graze. *Id.* Eventually, the field has no grass to offer, putting the ranchers—and their cows—out of luck. *Id.*

the email, spammers send increasingly higher volumes of email in order to garner a larger share of recipients' attention relative to competing spammers.[102] Unfortunately, spam-filtering technology, while preventing the receipt of the vast majority of spam,[103] further incentivizes spammers to send more email.[104] The few messages that get through will receive more attention from recipients, leading to higher response rates and profits per email that circumvents the automatic filters.[105]

Each facet of the spam industry—initial volume sent, limited time and attention, and even spam control technologies—centers around the *de minimis* marginal cost of each email sent and perversely incentivizes spammers to send increasingly more email.[106] For legislation intended to curb spam to be effective, it must shift more of the financial burden onto spammers by raising the cost of each marginal email sent.[107] Since spammers are effective only if they send a sufficient quantity of email messages, generally millions, adding even a small cost—or potential cost—to each email could dramatically impact spammers by flipping the incentives associated with sending each additional email.[108]

That spam increased since the enactment of the CAN-SPAM Act suggests that its enforcement provisions did not have the deterrent effect on spammers that Senator Ron Wyden and Congress had envisioned.[109] Only 14.3 percent of spam complied with all three major criteria of the Act during the first full year after its passage, with compliance dropping to 5.7 percent by 2006.[110] This suggests that spammers recognize the risks of prosecution for non-compliance with CAN-SPAM are not sufficiently high to shift the costs onto them and to disincentivize spamming.[111]

The FTC, state attorneys general, and ISPs will bring enforcement actions only when they receive a critical mass of

---

102. Plice et al., *supra* note 92, at 279.

103. *See supra* text accompanying note 28.

104. Pavlov et al., *supra* note 99, at 81.

105. *Id.*

106. Kigerl, *supra* note 88, at 576.

107. *Id.*

108. *Id.*

109. *Id.*

110. Galen A. Grimes, *Compliance with the CAN-SPAM Act of 2003: Studying the Application of the CAN-SPAM Act and its Effect on Controlling Unsolicited Email Messages*, 50 COMM. ACM 56, 59 (Feb. 2007). The study defined compliance as: (1) not using a deceptive or misleading subject line, (2) including the physical address or advertiser, (3) including a functional opt-out provision within each email, and (4) identifying a sexually explicit message as such. *Id.* at 60-61.

111. Kigerl, *supra* note 88, at 578.

complaints about noncompliant email from individual spam recipients.[112] The Act's weak enforcement provisions are the result of aggressive lobbying by Internet marketing and retail associations concerned about the stricter laws that many states were developing and implementing at the time that CAN-SPAM was passed.[113] The current enforcement provisions, in order to successfully deter spam, require strengthening so that prosecution and punishment become more of a reality. The provisions must force spammers to recalculate the cost of sending spam in order to internalize the risk of defending against lawsuits for violation of the Act.[114]

This section will discuss why the three primary enforcement agents of the CAN-SPAM Act—the FTC, state attorneys general, and ISPs—have failed to effectively curb the expansion of spam since the Act's passage.[115] Since the Act reserves private causes of action that sound in common law and state fraud regulation,[116] this section will also consider why these causes of action may not adequately shift the cost of sending email onto the senders of spam.

B. FTC Enforcement: Little Enforcement Against a Rising Tide of Spam

Federal enforcement of the CAN-SPAM Act, though consistent, failed to make any real dent in the growing spam problem.[117] In the first two years after Congress enacted CAN-SPAM, the federal government brought only twenty cases.[118] Between 2005 and 2007,

---

112. Rita M. Cain, *When Does Preemption Not Really Preempt? The Role of State Law After CAN-SPAM*, 3 ISJLP 751, 768 (2008).

113. *See* Stefanie Olsen, *Ad Groups Lobby for Antispam Law*, CNET (Nov. 13, 2003), http://news.cnet.com/Ad-groups-lobby-for-antispam-law/2100-1024_3-5107059.html (explaining CAN-SPAM preempted California's stringent "opt-in" law); 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 (noting that industry lobbyists preferred the Senate's legislation that eventually became CAN-SPAM to other, stricter standards considered in the House).

114. Kigerl *supra* note 88, at 578.

115. *See infra* Part II.B.

116. *See supra* note 86.

117. Tom Spring, *Spam Slayer: FTC's CAN-SPAM Report Card*, PCWORLD (Dec. 20, 2005, 8:00 AM), http://www.pcworld.com/article/123982/spam_slayer_ftcs_canspam_report_card.html.

118. *See* DIV. OF MKTG. PRACTICES, U.S. FED. TRADE COMM'N, SPAM SUMMIT: THE NEXT GENERATION OF THREATS AND SOLUTIONS 6 (Nov. 2007) [hereinafter 2007 FTC REPORT], *available at* http://www.ftc.gov/os/2007/12/071220spamsummitreport.pdf (noting that "nearly 30 law enforcement actions focusing on the core protections" of the CAN-SPAM Act have been brought); U.S. FED. TRADE COMM'N, EFFECTIVENESS AND ENFORCEMENT OF THE CAN-SPAM ACT: A REPORT TO CONGRESS app. 5 (Dec. 2005) [hereinafter 2005 FTC REPORT], *available at*

the FTC and DOJ brought fewer than ten total additional cases.[119] This means that in that two-year period, the federal government brought, on average, fewer than five additional cases per year.[120] Light enforcement coincided with a period of an increasing spam volume, underscoring the inability of just one primary enforcement agency, the FTC, to adequately confront the spam problem.[121] At the time of the 2007 FTC Report, the largest single civil penalty was for $900,000.[122] However, the average imposed civil (or criminal) penalty for violations of the CAN-SPAM law remains unclear. In any case, the chance that any individual spammer will face an enforcement action is extremely unlikely given the number of spammers and the low level of enforcement.[123]

C. State-brought Suits: Limited Enforcement with Limited Budgets

In addition to federal action, the Act authorizes state attorneys general to bring suits against noncompliant spammers.[124] Although empowering states with a cause of action introduces fifty additional potential plaintiffs to bring such suits, state attorneys general offices failed to make CAN-SPAM enforcement a priority.[125] In the first two years after Congress passed the CAN-SPAM Act, state attorneys general brought a total of six cases to enforce the Act's provisions.[126] One of these cases was filed jointly with the FTC, which is included in the initial twenty cases brought by the FTC as mentioned above, meaning that states alone filed only five additional cases.[127]

The current state budget deficits suggest that state attorneys general will not be able to increase the already low number of

---

http://www.ftc.gov/reports/canspam05/051220canspamrpt.pdf (noting that the FTC brought twenty cases at the time the Report was released).

119. 2007 FTC REPORT, *supra* note 118, at 6.

120. *Id.*

121. *See supra* notes 7-13 and accompanying text.

122. 2007 FTC REPORT, *supra* note 118, at 7; *see also* Consent Decree and Order for Civil Penalties and Injunctive and Other Relief at 7, United States v. Jumpstart Techs., LLC, No. C-06-2079 (MHP) (N.D Cal. Mar. 22, 2006) (providing for a $900,000 civil penalty).

123. *See* 2007 FTC REPORT, *supra* note 118, at 7.

124. 15 U.S.C. § 7706(f)(1) (2006).

125. 2005 FTC REPORT, *supra* note 118, at app. 7.

126. *Id.* Three cases were filed in federal court, while an additional three were filed in state courts. *Id.* The states filing cases include California, Florida, Massachusetts (2), Washington, and Texas. *Id.*

127. 2005 FTC REPORT, *supra* note 118, at app. 7 (states filing cases include California, Florida, Massachusetts, Texas and Washington); *see also* FTC v. Optin Global, Inc., No. C05-1502 SC, 2005 WL 1027108 (N.D. Cal. Apr. 13, 2005) (exemplifying a joint federal and state prosecution of CAN-SPAM Act violations).

CAN-SPAM actions.[128] Nationwide state budget shortfalls for fiscal years 2009 to 2011 totaled over $430 billion.[129] States confronted these deficits partly through spending cuts to various government services and agencies.[130] Nonetheless, states will continue to see budget shortfalls into the foreseeable future, with forty states already projecting a combined $113 billion deficit through fiscal year 2012.[131] If revenue continues to decline, states will continue to cut spending and services as past budget shortfalls deplete reserve funds.[132] Exacerbating matters, state budgets tend to recover slowly from recessions, indicating further budget cuts to the offices of state attorneys general in the future.[133] Some states already identified budgetary cuts in their offices of the attorney general, which will further reduce the human and capital resources available for litigating CAN-SPAM cases.[134]

The states' current minimal enforcement of CAN-SPAM, along with the dismal outlook of state funds, suggests that states will not pick up the slack in enforcement in the foreseeable future. As a result, CAN-SPAM's anticipated deterrent effect will not be enough because the chances of litigation and its attendant civil and criminal penalties are too low to prompt spammers to factor these risks into their costs.

D. Internet Service Provider Private Suits: Incentivized Not to Bring Suit

Despite the commonly accepted proposition that ISPs are the ideal private plaintiffs to file CAN-SPAM suits because spam burdens

128. Elizabeth McNichol, Phil Oliff & Nicholas Johnson, *States Continue to Feel Recession's Impact*, CTR. ON BUDGET & POLICY PRIORITIES 6 (June 17, 2011), http://www.cbpp.org/files/9-8-08sfp.pdf.

129. *Id.* at 2.

130. *Id.*

131. *Id.* at 6. This total will most likely grow as it does not include the budgets of all fifty states.

132. *Id.* at 7.

133. NAT'L CONF. OF STATE LEGISLATURES, STATE BUDGET UPDATE: NOVEMBER 2010 1 (Dec. 7, 2010), http://www.ncsl.org/documents/fiscal/november2010sbu_free.pdf.

134. *See, e.g.*, STATE OF WASH. OFFICE OF ATT'Y GEN., TEN PERCENT GFS REDUCTION, 100-BT-2011-13 (2010), *available at* http://www.ofm.wa.gov/reductions/2011-13/100.pdf (listing reductions across state Office of Attorney General). Some states, like Pennsylvania, currently exempt offices of the state attorney general from funding cuts. *State Budget Issues, 2010-2011*, SUNSHINE REV., http://sunshinereview.org/index.php/State_budget_issues,_2010-2011 (last visited Jan. 2, 2011).

their networks, ISPs have mixed incentives to bring such actions.[135] The marginal financial cost of transmitting spam for ISPs is as low, or lower, than it is for spammers to send email.[136] As a result, the cost of carrying spam to ISPs, both in economic terms and in terms of server network stress, tends to be overstated.[137] Courts have begun to recognize that paucity of evidence supporting the contention that spam strains network capacity.[138] This renders moot the argument that ISPs have the primary private motive to sue spammers, thereby calling into question whether the Act properly incentivizes ISPs to bring enough suits to deter spam.[139]

The Fifth Circuit declared in *White Buffalo Ventures, LLC v. University of Texas at Austin* that server efficiency and load "is among the most chronically over-used and under-substantiated interests asserted by parties."[140] The opinion continues: "declaring server integrity to be a substantial interest without evidentiary substantiation might have unforeseen and undesirable ramifications in other online contexts."[141] Even if there is an additional cost to ISPs resulting from the filtering and increased server load associated with spam, evidence suggests that ISPs just pass that cost—as much as two dollars per month per user—directly to the consumer.[142]

In addition to being a financially neutral "problem" for ISPs, providers may actually profit from having spam on their servers. The clearest example of this profiting is when the Internet user pays for access by-the-minute or has a cap on the amount of data that may be used for a given period of time.[143] Many rural or poorer Internet users do not have the unlimited broadband access that urban or wealthier Internet users have.[144] As a result, the time that users spend online sorting through unwanted spam, when aggregated over many Internet

---

135. 149 CONG. REC. S13,020 (daily ed. Oct. 22, 2003) (statement of Sen. McCain) ("Internet service providers are the businesses caught in the middle, forced every day to draw distinctions between what they perceive as legitimate email and what is spam.").

136. Soma et al., *supra* note 19, at 192.

137. *Id.*; *see also* Saul Hansell, *Totaling Up the Bill for Spam*, N.Y. TIMES, July 28, 2003, http://www.nytimes.com/2003/07/28/business/totaling-up-the-bill-for-spam.html (noting that one ISP has actually reduced network usage through its spam management system).

138. *See e.g.*, White Buffalo Ventures v. Univ. of Tex. at Austin, 420 F.3d 366, 377 n.24 (5th Cir. 2005) (noting that courts are beginning to require better evidence that spam and unauthorized access physically damages computer networks).

139. *Id.*

140. *Id.* at 375.

141. *Id.* at 377.

142. Derek E. Bambauer, *Solving the Inbox Paradox: An Information-Based Policy Approach to Unsolicited E-mail Advertising*, 10 VA. J.L. & TECH. 5, 23 (2005).

143. S. REP. NO. 108-102, at 7 (2003).

144. *Id.*

users, can translate into profits for ISPs, further reducing their incentive to go after spammers.[145]

While pay-by-the-minute home Internet access will eventually give way to unlimited broadband, wireless Internet providers—which represent a growing segment of ISPs—are moving away from unlimited mobile access and toward monthly data caps.[146] Unlike the traditional unlimited access available on some mobile Internet devices, plans with data caps charge additional fees when users exceed the preset limit.[147] Screening unwanted spam will cause some Internet users to exceed these data limits, providing additional spam-based revenue to ISPs.[148]

Furthermore, many ISPs, such as America Online and Microsoft, also host web-based email services that charge advertisers for allotted online space where they may post banners and other advertisements.[149] The more time users spend on these websites, the more ISP-based email providers can charge advertisers for that online space as users click around.[150] Counterintuitively, the time Internet users spend manually filtering spam on email websites can generate more money for ISPs.[151] Lastly, some ISPs have leveraged the spam problem directly by packaging additional spam-related software like filtering and ad-blocking services to consumers in order to engage in advertising and market differentiation.[152]

The enforcement provisions in the CAN-SPAM Act assume that ISPs' incentives for blocking spam align with those of their customers.[153] The problem is that ISPs do not necessarily have proper incentives to sue spammers on behalf of their customers because spam may be economically neutral or even lucrative for ISPs. Online security systems tend to fail when the party charged with implementing those systems is not the party that will suffer from such

---

145. *Id.*

146. Julia Boorstin, *AT&T's New Tiered Pricing: Why & Why Now?*, CNBC (June 2, 2010), http://www.cnbc.com/id/37471802/AT_T_s_New_Tiered_Pricing_Why_Why_Now.

147. *Id.*

148. *See* Bambauer, *supra* note 142 and accompanying text.

149. Igor Helman, Note, *SPAM-A-Lot: The States' Crusade Against Unsolicited E-mail in Light of the CAN-SPAM Act and the Overbreadth Doctrine*, 50 B.C. L. REV. 1525, 1555 (2009).

150. *Id.*

151. *Id.*

152. Hansell, *supra* note 137.

153. 149 CONG. REC. S13,023 (daily ed. Oct. 22, 2003) (statement of Sen. Wyden) ("[W]e give a role to . . . the Internet service providers . . . to bring a handful of actions very quickly to establish that for the first time there is a real deterrent, there will be real consequences when those big-time spammers try to exploit our citizens.").

failure, as is the case with ISPs.[154] As a result, empowering a private third party, like an ISP, to protect its customers from spam may not be the best means to protect consumers as Congress intended.[155] An ISP's own financial stake in maintaining spam nullifies its incentive to bring suit as often as possible. Similar to the problems associated with the FTC and the states, it is likely that the risk of litigation will be insufficient to increase spammers' projected costs of each email.

E. Tort and State Fraud Law: Too Murky to Clearly Deter

While the CAN-SPAM Act provides no private cause of action for individuals, and simultaneously preempts state spam laws, it allows individuals to sue under various common law tort theories and preserves state laws focusing more generally on fraud and cybercrime.[156] However, tort law application in spam cases remains unreliable and risky for plaintiffs.[157] Moreover, courts are unpredictable in determining whether CAN-SPAM exempts particular state statutes from its express preemption provision.[158]

The seminal tort case brought against a spammer is *Intel Corporation v. Hamidi*.[159] In *Hamidi*, Intel, a computer processor manufacturer, brought a common law trespass to chattels claim against Kourosh Kenneth Hamidi, a former Intel employee who repeatedly sent uninvited scathing email messages through Intel's mail servers to numerous Intel employees.[160] Relying heavily on the *Restatement (Second) of Torts*, the court held that Intel must show tangible damage to its servers or email system in order to bring a successful claim—something that Intel could not do since unauthorized use of the systems do not physically harm them.[161]

While the *Hamidi* decision spawned much commentary and debate, it is important here for two reasons. First, *Hamidi*

---

154. Ross Anderson & Tyler Moore, *The Economics of Information Security*, 314 SCIENCE 610, 610 (Oct. 27, 2006).

155. *Id.*

156. *See supra* notes 84, 87.

157. Richard A. Epstein, Intel v. Hamidi: *The Role of Self-Help in Cyberspace?*, 1 J.L. ECON. & POL'Y 147, 147 (2005).

158. *Compare* Beyond Sys., Inc. v. Keynetics, Inc, 422 F. Supp. 2d 523 (D. Md. 2006) (holding that CAN-SPAM does not preempt Maryland Commercial Electronic Mail Act), *with* Omega World Travel, Inc. v. Mummagraphics, Inc., 469 F.3d 348 (4th Cir. 2006) (holding CAN-SPAM preempts an Oklahoma statute regulating commercial email).

159. Intel Corp. v. Hamidi, 71 P.3d 296 (Cal. 2003). For a more expansive discussion of *Hamidi*, see Epstein, *supra* note 157; see also Steven Kam, Note, Intel Corp v. Hamidi: *Trespass to Chattels and a Doctrine of Cyber-Nuisance*, 19 BERKELEY TECH. L.J. 427 (2004).

160. *Hamidi*, 71 P.3d at 299-300.

161. *Id.*

underscores the difficulty that courts face in adapting centuries-old common law to modern technology cases in general and with spam in particular.[162] These types of "legal gymnastics" create confusion among potential plaintiffs and reduce the chances that they will bring common law tort actions for issues like spam.[163] Secondly, and as a corollary to the first point, *Hamidi*'s holding that requires proof of damage to the computer systems sets a high bar for a successful plaintiff.[164] Considering the difficulty in quantifying the cost of spam to large ISPs with their vast financial resources,[165] proving physical damage for individual businesses and consumers can be prohibitive.[166]

These two facts, combined with the American Rule that requires each party in a lawsuit to pay his own attorney fees,[167] suggest that plaintiffs will not risk a common law suit to bring spammers into court when the probability of winning is so low.[168] Congress recognizes the importance of providing attorney fees in CAN-SPAM by giving courts the option to assess attorney fees to any party courts see fit—an option unavailable under tort law.[169] Doctrinal confusion and high financial risk dissuades potential plaintiffs from filing actions,[170] short-circuiting the deterrence impacts of tort and state law. There must be a higher degree of certainty that the plaintiff will first file a case and then win in order to raise the perceived costs of sending spam.

Similar to the problems associated with applying tort law to unwanted spam, state statutory regimes designed to regulate email fraud remain inconsistently preempted.[171] Thus, a plaintiff must first show that CAN-SPAM does not preempt the particular state cause of action and only then may proceed to argue the substance of the case. Many state anti-fraud laws, if not preempted by CAN-SPAM, require the plaintiff to prove that the sender knew or should have known that the recipient lived in the state with the anti-fraud statute.[172] Since

---

162. Adam Mossoff, *Spam—Oy, What a Nuisance!*, 19 BERKELEY TECH. L.J. 625, 641-44 (2004) (criticizing court's use of nuisance-type substantial interference with use of property for a claim rooted in trespass theory, which does not traditionally require such a showing).

163. Dan L. Burk, *The Trouble with Trespass*, 4 J. SMALL & EMERGING BUS. L. 27, 40 (2000).

164. *See* Cain, *supra* note 112, at 761 (noting the difficulty in quantifying physical damage from spam).

165. *See supra*, Part II.C.

166. Cain, *supra* note 112, at 761.

167. Alyseka Pipeline Serv. Co. v. Wilderness Soc'y, 421 U.S. 240, 247 (1975).

168. Cain, *supra* note 112, at 761.

169. 15 U.S.C. § 7706(g)(4) (2006).

170. Mossoff, *supra* note 162, at 641.

171. *Supra* note 158.

172. Cain, *supra* note 112, at 764-65.

email addresses provide no indication of where recipients live, proving actual knowledge is borderline impossible in the vast majority of cases.[173]

As a result, potential plaintiffs find themselves left in a difficult position. On the one hand, courts may (or may not) find particular state spam statutes preempted, thereby removing the private cause of action. On the other hand, those state statutes that CAN-SPAM does not preempt often require evidentiary showings that may be nearly impossible to prove. These challenges further underscore the need for a CAN-SPAM private cause of action for individuals to seek damages against spammers, because the Act preempts any statute that could meaningfully deter spammers by increasing the probability that spammers would be brought to court and held liable.

III. PRIVATE ACTION TO DETER SPAM: ANY ACTION IS GOOD ACTION

The private cause of action, in any of its many forms, primarily works to increase the deterrence value of statutory enforcement provisions by enabling larger classes of plaintiffs to bring actions against violators.[174] Even a weak private enforcement provision spreads the enforcement authority so broadly that the enlarged number and diversity of enforcers invites more prosecutorial innovation and flexibility than a "monopolistic government enforcer would produce" on its own.[175] Authorizing more potential plaintiffs to bring suit increases the likelihood that a particular spam offender will find himself as a defendant in either a civil or criminal case, thereby shifting additional risk and potential cost onto that violator.[176]

Bringing additional private actors into the larger CAN-SPAM enforcement scheme may help remedy the particular challenges and shortcomings associated with the Act's current enforcement structure.[177] Supplementing government action with private enforcement mechanisms serves to alleviate the financial burden on limited or dwindling state and federal government resources.[178]

---

173. *Id.* at 765.

174. Edward A. Fallone, *Section 10(B) and the Vagaries of Federal Common Law: The Merits of Codifying the Private Cause of Action under a Structuralist Approach*, 1997 U. ILL. L. REV. 71, 118.

175. William B. Rubenstein, *On What a "Private Attorney General" is—and Why it Matters*, 57 VAND. L. REV. 2129, 2152 (2004).

176. *See supra* note 173 and accompanying text.

177. *Supra* Part II.

178. *See, e.g.*, Gregory Huffman, *UPL, MDP, MJP: How Irresistible are These Changes?*, 65 TEX. B. J. 428, 430 (2002) (discussing Texas's adoption of a private cause of action as a

Federal agencies recognize the value of private suits in supplementing government action, thereby reducing the financial burden associated with enforcing frequently violated statutory regulations like those implementing the CAN-SPAM Act.[179] Moreover, a wider cause of private action provides a relief valve for enforcement authorities when those entities authorized to bring legal action are unwilling or unable to prosecute or pursue such actions, as is the case with ISPs and the states.[180] In fact, Congress considered, but ultimately rejected, a "bounty" system where the FTC would pay private citizens to pursue spammers on its behalf.[181]

States seeking to limit spam prior to the adoption of CAN-SPAM recognized the power of a private cause of action.[182] For example, the California approach authorizes each recipient, defined as "the addressee of an unsolicited commercial email advertisement," to bring a civil action to recover either actual damages or liquidated damages of one thousand dollars for each unsolicited commercial email up to one million dollars.[183] State provisions like these, designed to deter users from sending spam, led marketing groups to lobby for CAN-SPAM's adoption and its weak enforcement provisions.[184] This section will consider the potential impact of various forms of private action on deterring spammers from sending spam by examining areas of regulatory enforcement that provide for more expanded private action than does CAN-SPAM.[185]

---

replacement for the State's earlier system of exclusive government enforcement for unauthorized practice of law, which had been ineffective due to budgetary constraints).

179. *See, e.g.*, OFFICE OF ENFORCEMENT, U.S. ENVTL. PROT. AGENCY, ENFORCEMENT IN THE 1990'S PROJECT: RECOMMENDATION OF THE ANALYTICAL WORKGROUPS, No. 22E-2000, 5-47-5-48 (1990) ("[T]he availability of citizen suit remedies has served to leverage our scarce enforcement resources. . . . Moreover, to the extent that the regulated community views citizens enforcement as unpredictable, an even greater deterrent effect is achieved by the reality of active, broadly spread citizen suit enforcement as regulates seek to achieve compliance to avoid not only federal and state prosecution but also to avoid independent citizen enforcement actions.").

180. Christopher G. Granaghan, Note, *Off the Mark: Fixing the False Marking Statute*, 89 TEX. L. REV. 477, 489 (2010).

181. *See* 149 CONG. REC. S13,041 (daily ed. Oct. 22, 2003) (statement of Sen. Corzine) ("Creating incentives for private individuals to help track down spammers is likely to substantially strengthen the enforcement of anti-spam laws. It promises to create an army of computer geeks who seek out spammers for their and the public's benefit.").

182. *See, e.g.*, CAL. BUS. & PROF. CODE § 17529.5 (2003) (allowing any "recipient of an unsolicited commercial email advertisement" a cause of action) (preempted by CAN-SPAM Act).

183. *Id.*

184. Olsen, *supra* note 113 (noting that marketing groups were concerned about some states' stiff legal provisions and therefore preferred Congress's relatively permissive spam bill).

185. Measuring deterrence is fundamentally difficult because it requires predicting an illegal action and identifying a causal link between a present deterrence approach's impact on reducing the probability of that illegal action. Christina O. Broderick, Note, *Qui Tam Provisions*

A. The Private Attorney General: Private Standing when the Government Sits Down

Although the phrase "private attorney general" first made its way to the US Supreme Court in 1943,[186] its usage remains nebulous and imprecise.[187] Nonetheless, for the purposes here, the clearest definition is "a private citizen working on behalf of public good within the legal forum."[188] This definition coincides with the purposes of the CAN-SPAM Act, as the compensation available when filing a civil suit, the "private" part of the phrase, works to incentivize actors to work for public deterrence of statutory violations, the "attorney general" part of the phrase.[189] This public function by private actors supplements the public enforcement that has so far failed to deter violations adequately on its own.[190]

Qui tam actions provide the best-known example of the role of a private attorney general.[191] In a *qui tam* action, a private attorney appoints himself to enforce those provisions for which *qui tam* actions are authorized.[192] After the private attorney brings a case, he must inform the Attorney General's office, which has the option to replace the private attorney and take over the case.[193] However, if the Attorney General chooses not to intervene, the private attorney may continue the *qui tam* action, incentivized by the fees and additional proceeds he may keep through bringing a successful case.[194] Currently, three statutes in the United States Code include *qui tam* provisions.[195] These include the False Claims Act (FCA), the false marking statute, and a statute intended to protect American Indian

---

and the Public Interest: An Empirical Analysis, 107 COLUM. L. REV. 949, 980 (2007).This results in a very high level of uncertainty. *Id.*

186. FCC v. NBC, 319 U.S. 239, 265 n.1 (Douglas, J., dissenting).

187. Rubenstein, *supra* note 175, at 2130.

188. *Id.* at 2134.

189. *Id.* at 2140.

190. Susan D. Hoppock, Current Development 2006-2007, *Enforcing Unauthorized Practice of Law Prohibitions: The Emergence of the Private Cause of Action and its Impact on Effective Enforcement*, 20 GEO. J. LEGAL ETHICS 719, 734 (2007); Granaghan, *supra* note 180, at 489.

191. The *qui tam* action may be best known because it has proven to be divisive among scholars as to its constitutionality and its arguably perverse incentives. Loretta Calvert, *The Qui Tam Provision of the False Claims Act: Congressional Missile or a Net Full of Holes?*, 1998 ANN. SURV. AM. L. 435. *Qui tam* is short for *qui tam pro domino rege quam pro se ipso in hac parte sequitur*, which means "who as well for the king as for himself sues in this matter." Granaghan, *supra* note 180, at 488.

192. Rubenstein, *supra* note 175, at 2145.

193. *Id.* at 2144.

194. *Id.*

195. Granaghan, *supra* note 180, at 499.

tribes.[196] States are increasingly reliant on *qui tam* actions to alleviate burdens imposed by regulatory enforcement.[197]

The FCA allows the Attorney General or private attorneys, known as relators, through a *qui tam* action, to file actions against federal contractors believed to be committing fraud against the government.[198] Congress included a *qui tam* provision in the FCA because detecting fraud requires specialized knowledge, and the expanding federal contractor sector impeded the government from adequately monitoring every government contract.[199] Congress recognized the government's limits in expertise and resources in finding and prosecuting spammers.[200]

Between 1986, when Congress added the *qui tam* provision to the FCA, and 2004, relators filed 4,704 *qui tam* lawsuits, through which they recovered 8.4 billion dollars for the government.[201] During this time, the average recovery for *qui tam* actions under the FCA was 1.7 million dollars, while the average government-initiated action settled for 1.4 million dollars.[202]

Similar to federal contractor fraud against the government, two of the most serious challenges facing spam enforcement are the difficulty and expense of tracking down individual spammers.[203] However, such a *qui tam* provision could incentivize a wider group of people with specialized knowledge about spamming technology and the spamming business to take action against spammers.[204] In this way, the federal government and the states benefit because they do not need to rely as heavily on their own funds to ensure the level of enforcement necessary to successfully deter spammers from sending email.[205] States have already adopted *qui tam* provisions to help

196. *Id.*

197. Broderick, *supra* note 185, at 956.

198. 31 U.S.C. §§ 3729-3733 (2006). The *qui tam* provision allows relators to recover up to 25 percent of the damages as well as reasonable attorney fees. *Id.*

199. Broderick, *supra* note 185, at 960-61.

200. *See* 149 CONG. REC. S13,041 (daily ed. Oct. 22, 2003) (statement of Sen. Corzine) ("The fundamental problem in dealing with spam is enforcement. It is one thing to propose rules governing emails. But it is often hard for Government officials to track down those who violate those standards. Spammers typically use multiple email addresses or disguised routing information to avoid being identified. As a result, finding spammers can take not just real expertise, but persistence, time, energy and commitment.").

201. Broderick, *supra* note 185, at 955.

202. *Id.* at 979.

203. FTC NATIONAL DO NOT EMAIL REGISTRY, *supra* note 76.

204. *Qui tam* provisions rely on the "common informer" principle, where relators with particularized knowledge either of the specific statutory violation or the issue will fill the enforcement gaps left by limited government resources. Broderick, *supra* note 185, at 960-61.

205. *See supra* Part II.B.

relieve the burdens imposed by investigating and prosecuting fraud.[206] Internet users will benefit through a larger critical mass of cases brought on their behalf—something the states have not done.[207]

B. Citizen Suits: Removing the Middle Man

Citizen suits are in some ways better suited to the spam problem because *qui tam* actions are generally used only to recover compensatory damages on behalf of the government, and not as widely used to enforce the types of civil and criminal sanctions found in the CAN-SPAM Act.[208] Unlike *qui tam* actions, citizen-suit provisions grant standing to bring suit against violators, like spammers, to anyone who can show damages.[209] Moreover, citizen suits are intended to deter bad acting prospectively, not punish reactively,[210] which aligns with the purposes of the CAN-SPAM Act.

Environmental protection remains the pioneering legal area in which citizen suits are used to supplement government action.[211] For the most part, these suits have succeeded in helping the Environmental Protection Agency (EPA) and the DOJ enforce environmental statutes.[212] Specifically, the citizen-suit fee recovery system incentivizes private action among a large group of people because plaintiffs recover costs and penalties if they prevail in litigation.[213] Citizen-suit actions work to fill in the regulatory enforcement gaps left by broad regulatory schemes, such as those related to the environment and to spam.[214] Such schemes—those

206. For example, Tennessee had a Medicaid *qui tam* provision that successfully exposed "significant amounts" of fraud. Broderick, *supra* note 185, at 996. In fact, the Tennessee Attorney General has never had to bring a state-initiated action because of the *qui tam* provisions. *Id.* Similarly, Texas recovered all of its Medicaid False Claims Act's $15.8 million through *qui tam* actions. *Id.*

207. *See id.* at 961.

208. Rubenstein, *supra* note 175, at 2145.

209. *See, e.g.*, Clean Water Act, 33 U.S.C. § 1365(a) (2006) ("Except as provided in subsection (b) of this section and section 309(g)(6), any citizen may commence a civil action on his own behalf—(1) against any person (including (i) the United States, and (ii) any other governmental instrumentality or agency . . . .)").

210. Hoppock, *supra* 190, at 730.

211. The Clean Air Act of 1970, 42 U.S.C. § 7604, was the first environmental statute to include a citizen suit provision. Robert V. Percival & Joanna B. Goger, *Escaping the Common Law's Shadow: Standing in the Light of* Laidlaw, 12 DUKE ENVTL. L. & POL'Y F. 119, 130 (2001).

212. Jeanette L. Austin, Comment, *The Rise of Citizen-Suit Enforcement in Environmental Law: Reconciling Private and Public Attorneys General*, 81 NW. U. L. REV. 220, 221 (1987).

213. Barry Boyer & Errol Meidinger, *Privatizing Regulatory Enforcement: A Preliminary Assessment of Citizen Suits Under Federal Environmental Laws*, 34 BUFF. L. REV. 833, 838 (1985).

214. *Id.*

which may involve an unmanageable number of violators—basically necessitate provisions for citizen suits to supplement government action.[215] That is, citizen-suit provisions reflect the recognition that some regulated communities are so vast that government enforcement alone cannot adequately deter statutory violations—a problem apparent with spam.

The primary challenge associated with environmental citizen suits is that plaintiffs often have difficulty showing injury, and therefore lack standing to bring the suit.[216] If Congress were to add a private cause of action, a plaintiff would prove standing simply by showing that he received spam that violated the CAN-SPAM Act. This is distinguishable from the many environmental cases in which the court held that the citizen plaintiff failed to show a particularized injury, given the often-attenuated link between environmental statutory violations and personal harm.[217] Since the harm in spam cases is already defined in the statute as the receipt of certain forms of email, the harm is less abstract than the environmental harm or particularized injury in the environmental statutes. Moreover, the wider adoption of citizen-suit provisions, when compared with *qui tam* provisions, would provide a greater body of decisions from which Congress can draw to adequately craft effective legislation.[218] To avoid such issues of standing, Congress could mirror much of the language used to authorize ISP private causes of action.[219]

One rejoinder to this argument is that the civil penalties imposed by the Act are not substantial enough per individual email, especially if there is not a critical mass of people who would rather seek a relatively small penalty through expensive litigation than just delete the email.[220] Unlike ISPs, which could bring suit for all the

---

215. Michael S. Greve, *The Private Enforcement of Environmental Law*, 65 TUL. L. REV. 339, 374-75 (1990).

216. For a discussion of standing see Massachusetts v. EPA, 549 U.S. 497 (2007).

217. *See, e.g.*, Lujan v. Defenders of Wildlife, 504 U.S. 555 (1992); Lujan v. Nat'l Wildlife Fed'n, 497 U.S. 871 (1990).

218. *See, e.g.*, Gwaltney of Smithfield v. Chesapeake Bay Found., 484 U.S. 49, 57-58 (1987), *superseded by statute* (holding that language of Clean Water Act's citizen suit provision did not grant standing for wholly past violations and suggesting that Congress clarify the language). Congress took the Court's advice in the 1990 amendments to the Act. Clean Air Act of 1970, Pub. L. No. 101-549, 104 Stat 2399 ("PAST VIOLATIONS.—Section 304(a) of the Clean Air Act is amended by inserting immediately before 'to be in violation' in paragraphs (1) and (3) 'to have violated (if there is evidence that the alleged violation has been repeated) . . . .'").

219. 15 U.S.C. § 7706(g) (2006).

220. *Id.* § 7706(f)(3)(A) (providing for a $250 penalty per CAN-SPAM violation); *see also* Samuel M. Hill, *Small Claimant Class Actions: Deterrence and Due Process Examined*, 19 AM. J. TRIAL ADVOC. 147, 152 ("An additional contention is that if the small claimant class action is unavailable defendants will be free to violate the law as long as the negative effects are diffused

individual emails that a particular spammer sends through its servers, an individual bringing such action would have standing to bring suit only for that one email received. The current civil penalty is too low to deter plaintiffs from bringing such action. This would require massive amounts of plaintiffs to file in order to deter spammers. Such a critical mass of plaintiffs could put a strain on the courts due to the amount of potential new litigation.

Given the number of emails sent by spammers, however, class action suits organized and brought by lawyers incentivized by the prospect of hefty attorney fees could act as a large deterrent to spammers. This is especially true if the civil penalty prescribed by statute is multiplied by the number of individuals in the class.[221] Considering the number of recipients associated with just one mailing and the fact that all recipients receive the same email violating the same statute, such a class could easily fulfill the numerosity, commonality, and typicality elements required for class certification under the Rule 23 of the Federal Rules of Civil Procedure.[222] In this way, there would be an increased number of plaintiffs seeking to pursue spammers. Thus, the higher cost of legal defense, statutory fees, and even criminal incarceration would force some spammers to exit the industry or at the very least reduce the number of emails sent, since each email would mean one additional potential plaintiff.

C. The Limits of Domestic Action

A direct criticism of the proposed expansion of the private cause of action is that private action alone does not recognize the problem's scope. The Act's goal is to ensure that Internet users do not waste time and money sorting through and deleting the multitude of unwanted email they receive daily.[223] Simply put, no matter what domestic regulation Congress may adopt to confront spam—private cause of action or otherwise—unwanted email will still reach users' inboxes if domestic regulation is the only tool to combat spam.

Spam is an international problem that does not respect national borders.[224] Even though the United States is by far the

---

among many victims, and the small size of the individual claims will virtually guarantee that no legal action will be forthcoming.").

221. Hill, *supra* note 220, at 152.

222. *See* FED. R. CIV. P. 23; *see also* Wal-Mart Stores, Inc. v. Dukes, 131 S. Ct. 2541, 2551 (2011) (noting that commonality "must be of such a nature that it is capable of classwide resolution—which means that determination of its truth or falsity will resolve an issue that is central to the validity of each one of the claims in one stroke").

223. 15 U.S.C. § 7701(a)(4).

224. SYMANTEC, STATE OF SPAM & PHISHING: A MONTHLY REPORT 7 (Oct. 2011), http://www.symanteccloud.com/mlireport/SYMCINT_2011_10_October_FINAL-en.pdf.

number one source of spam worldwide, about three-quarters of spam originates outside of this country.[225] While there have been international efforts for cooperation on spam regulation, no international legal norms or binding agreements yet exist to effectively prevent the receipt of spam.[226] As a result, true spam control will require an international effort that includes both the public and private sectors of the global community, which is beyond CAN-SPAM's scope. Without such international controls, there is a possibility that spam operations will simply move to other countries with weaker regulations than an improved CAN-SPAM Act.[227]

IV. CONCLUSION: PRIVATE ACTION IS JUST ONE ARROW IN THE QUIVER

The CAN-SPAM Act, in its current form, has done very little to shift the cost of each marginal email onto the spammer.[228] Spam only increased since Congress passed the Act.[229] That much spam originates outside of US borders does not imply that domestic regulation should remain in its weakened form. The United States accounts for roughly one third of all spam worldwide.[230] Effective domestic action is better than no action in the absence of an international agreement, even if it is not a perfect solution. So long as the CAN-SPAM Act remains the near-exclusive enforcement authority for unsolicited spam, a private cause of action would promote its goals by deterring a critical mass of spammers from sending their unwanted messages—something the current CAN-SPAM Act simply does not do.

*David J. Rutenberg**

---

225. *Id.* The United States accounts for 34 percent of spam, while India, the second largest source of spam, generates 5.8 percent. *Id.*

226. *See, e.g.*, Convention on Cybercrime, Nov. 23, 2001, E.T.S. No. 185 (Council of Eur.), http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm; SECRETARIAT, ASIA-PACIFIC ECON. COOPERATION, APEC No. 205-SO-01.2, APEC PRIVACY FRAMEWORK (2005); *The London Action Plan on International Spam Enforcement Cooperation: Plan in Detail*, INT'L SPAM ENFORCEMENT NETWORK (2007), http://www.londonactionplan.org/?q=node/1.

227. Robert Stavins, *A Meaningful U.S. Cap and Trade System to Address Climate Change*, 32 HARV. ENVTL. L. REV. 293, 357 (2008) (discussing the concept of leakage in a global climate change context where domestic emitters of greenhouse gasses move offshore to other countries with weaker regulations).

228. *See supra* Part II.

229. *See supra* text accompanying note 36.

230. SYMANTEC, *supra* note 224.

* J.D. Candidate, Vanderbilt University Law School, 2012; M.P.P., Georgetown University, 2008; B.A., History, University of Pennsylvania, 2005. The author wishes to thank Katie Brown, Lauren Gregory, Ilana Kattan, Megan LaDriere, and Sophia Behnia for their thoughtful input regarding this Note. The author further wishes to thank the rest of the VANDERBILT JOURNAL OF ENTERTAINMENT AND TECHNOLOGY LAW Senior Editorial Board for being so great to work with.