March 2016

Recent Developments in Private Enforcement of the CAN-SPAM Act

Vanessa J. Reid

RECENT DEVELOPMENTS IN PRIVATE ENFORCEMENT OF THE CAN-SPAM ACT

Vanessa J. Reid

Abstract 281
I. Introduction 282
II. Facts and Background on the Spam Problem 283
A. What is Spam, Anyway? 283
B. What's the Harm in Spamming? 284
III. A Brief History of Spam Control 288
A. Self-Help and Vigilantism: The Internet's Wild West Era 288
B. State Laws: A Patchwork Regulatory Approach 288
C. Taking it Federal: The CAN-SPAM Act 289
IV. Private Enforcement of the CAN-SPAM Act 290
A. *MySpace v. The Globe.com*: A New Precedent and the End of an Era 291
B. *Facebook v. ConnectU*: The Social Networking Trend Continues 294
C. *Haselton v. Quicken Loans*: Pushing the Standing Envelope 296
D. Subsequent Social Networking Cases: Record-Breaking Judgments 297
E. *Gordon v. Virtumundo*: The Ninth Circuit Weighs In 298
V. Looking Ahead: What the Courts Got Right and the Future of Private CAN-SPAM Enforcement 302
VI. Conclusion 306

ABSTRACT

This note discusses recent developments in the area of private enforcement of the federal CAN-SPAM Act. The article is divided into four sections. The first section describes the history and background of the spam problem, while the second outlines historical attempts to

combat spam, culminating in the passage of the CAN-SPAM Act. The third section details a series of recent cases in which private entities have attempted to enforce the CAN-SPAM Act, and how courts have attempted to fashion a broader standard for the Act's private standing provision without opening the door to an excessive number of lawsuits. The final section discusses whether the courts got the balance right and makes recommendations for the future of private enforcement in this area.

I. INTRODUCTION

Unwanted "spam" messages have long plagued users of the Internet, clogging e-mail inboxes and aggravating businesses and consumers. Spam is more than an expensive nuisance—it has increasingly become a tool for committing fraudulent and criminal online behavior. Legislatures and technical experts alike have grappled with approaches to the problem, but no permanent long-term solution has yet emerged. One open policy question is how to divide responsibility for battling spam between government and private entities. While private companies have long employed their own technological methods for combating spam, several recent cases have opened up the possibility of a larger role for private enforcement of federal anti-spam laws.

The federal CAN-SPAM Act, passed in 2003, controls and regulates commercial e-mail.[1] The Act was initially interpreted by courts and commentators to provide a cause of action for government actors and a limited category of Internet service and e-mail providers.[2] A number of recent cases have permitted other types of private organizations to sue under the Act, particularly large social networking websites.[3] While enlisting new parties with the means and the motivation to combat spam is a step in the right direction, courts should respect the policy decisions and laws established by Congress, and avoid over-reaching in their interpretations of existing legislation.

Several recent district court decisions allowing large players like Facebook and MySpace to enter the enforcement arena strike the right balance between respecting congressional intent and sound public policy, while a case allowing a smaller, more traditional website to enter

1. Controlling the Assault of Non-Solicited Pornography and Marketing Act, 15 U.S.C. §§ 7701-7713 (2003).

2. MySpace, Inc. v. The Globe.com, Inc., 2007 WL 1686966, at *3 (C.D. Cal. 2007).

3. *Id.* at *4.

the fray goes too far beyond the boundaries of congressional intent.[4] A recent Ninth Circuit decision properly reined in an attempt to further expand the Act's standing provision, but the court may have overstepped in creating framework without sufficient basis in the statute.[5] Courts should continue to interpret the Act's standing requirements with enough flexibility to respond to rapidly evolving technologies, but without losing sight of Congress's intention in creating a balanced statutory scheme with a limited private cause of action.

II. FACTS AND BACKGROUND ON THE SPAM PROBLEM

A. What is Spam, Anyway?

Broadly defined, spam is any unwanted, unsolicited electronic communication.[6] Spam is sometimes described as unsolicited bulk e-mail or unsolicited commercial e-mail, but a precise definition remains elusive, as one person's junk commercial advertising is another's bonanza of surprise holiday shopping deals.[7] The term may also refer to similar abuses of other electronic media, such as Internet message boards, chat programs, and text messages.[8] There is little consensus about the precise volume of spam sent and received, as spam can be difficult to measure and identify,[9] spam levels vary significantly,[10] and

4. *See, e.g.*, Haselton v. Quicken Loans, Inc., 2008 WL 3046980 (W.D. Wash., May 23, 2008).

5. *See* Gordon v. Virtumundo, Inc., 575 F.3d 1040 (9th Cir. 2009).

6. Adam Hamel, *Will the CAN-SPAM Act of 2003 Finally Put a Lid on Unsolicited E-mail?*, 39 NEW ENG. L. REV. 961, 963 (2005) ("In general, spam refers to any unwanted e-mail").

7. Eric Goldman, *Where's the Beef? Dissecting Spam's Purported Harms*, 22 J. MARSHALL J. COMPUTER & INFO. L. 13, 14 (2003) ("Any attempt to intelligently discuss spam is immediately hampered by the word's imprecision. Simply put, the term 'spam' lacks a single well-accepted definition"). *See also* MESSAGING ANTI-ABUSE WORKING GROUP, E-MAIL METRICS PROGRAM: THE NETWORK OPERATORS' PERSPECTIVE REPORT 1 (2006), *available at* http://www.maawg.org/sites/maawg/files/news/FINAL_2Q2006_Metrics_Report.pdf ("The one thing this report does not attempt to define is 'spam.' Even though a great deal of time and energy has been devoted to clarifying this term, there is no universally accepted definition"); *Gordon*, 575 F.3d at 1045, n.1 ("While 'spam' in this context does not have a precise definition, it is typically understood to refer broadly to unsolicited e-mail messages").

8. *See, e.g.*, Edwin N. Lavergne, *FCC Gives Teeth to the CAN-SPAM Act of 2003: New Rules Strictly Limit Commercial Email to Cell Phones*, 1 N.Y.U. J. L. & Bus. 861, 861 (2003) (discussing new rules adopted by the FCC to prevent cellular phones and other wireless devices from being "deluged with unwanted commercial advertisements").

9. *See generally supra* notes 6 and 7.

10. *See, e.g.*, Gregg Keizer, *Spam Traffic Varies after Source Shut*, COMPUTERWORLD, Nov. 30, 2008, *available at* http://www.pcworld.com/businesscenter/article/154552/spam_traffic_varies_after_source_shut.html (stating that the purported 40 percent to 70 percent drop in global spam rates

many of the available statistics are provided by vendors of anti-spam products.[11] Studies from a variety of sources estimate that spam may account for anywhere from 40 percent to 97 percent of all e-mail.[12] While uncertainty persists, most commentators agree that spam is pervasive and makes up a large portion of e-mail traffic.[13]

B. What's the Harm in Spamming?

E-mail has radically altered the way we interact, communicate, and do business. Fundamentally, spam causes e-mail to be less useful as a medium for communication. The extent to which the potential of e-mail is compromised by spam is an open question and an ongoing battle, but spam undeniably creates frustration and expense for consumers and businesses alike. Once merely a time-consuming inconvenience, spam has become increasingly malicious and harmful in recent years.

1. Why Spammers Spam: Low Costs, Big Payoffs

Spam proliferates because it is essentially costless to spammers,[14] and it requires only a miniscule response rate to turn a profit. A recent study by a team of computer scientists from the University of California, Berkeley, and the University of California, San Diego, determined that spammers in their experiment received only one response per 12.5

---

after the Nov. 11, 2008, shutdown of California-based McColo Corp., a company that hosted a large volume of fraudulent Internet activities).

11. *See, e.g.*, CISCO 2008 ANNUAL SECURITY REPORT 13, *available at* http://cisco.com/en/US/prod/vpndevc/annual_security_report.html (explaining that Cisco, which sells anti-spam and other computer security products, reports that spam accounts for 90 percent of worldwide e-mail).

12. *See, e.g.*, THE NETWORK OPERATORS PERSPECTIVE REPORT, *supra* note 7 (reporting that 80 percent of e-mail from its sample was spam); CISCO 2008 ANNUAL SECURITY REPORT, *supra* note 11 (estimating that spam accounts for nearly 200 billion messages each day, or 90 percent of worldwide e-mail); Don Evett, SPAM STATISTICS 2006, *available at* http://spam-filter-review.toptenreviews.com/spam-statistics.html (stating that 40 percent of all e-mail is considered spam); YALE ENV'T 360 DIGEST, *The Environmental Cost of Spam* (Apr. 15, 2009), *available at* http://e360.yale.edu/content/digest.msp?id=1832 (estimating that 62 trillion "junk e-mails" were sent in 2008, accounting for 97 percent of all e-mail).

13. *See* FEDERAL TRADE COMMISSION SPAM SUMMIT: THE NEXT GENERATION OF THREATS AND SOLUTIONS (Dec. 20, 2007), *available at* http://www.ftc.gov/os/2007/12/071220spamsummitreport.pdf [hereinafter FEDERAL TRADE COMMISSION, *Spam Summit*] ("Spam is one of the most intractable consumer protection problems faced by computer users"); *see also supra* notes 11 and 12.

14. *See* 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, 127 (describing the minimal operating costs of sending bulk e-mails).

million e-mails sent (a response rate of less than 0.00001 percent), but they still managed to turn a healthy profit.[15]

2. How Spam Creates Costs for Third Parties: Time, Technology, and Bandwidth

The elimination of spam requires an investment of time, money, or both. These costs are passed on entirely from spammers to Internet Service Providers (ISPs),[16] individuals, and businesses. Individual recipients must waste large amounts of time sifting through unwanted mail messages by hand and/or spend money on commercial spam filters, which generally still require human intervention.[17] Desired e-mails can often be lost in the filtering process, as hand-sorting can be exhausting while spam filters can offer only a rough guess as to which e-mails are undesirable to a particular recipient.[18] Legitimate e-mail marketers and other businesses also incur additional costs because of spam. These businesses are often unable to reach existing and potential customers when their messages are erroneously blocked by over-zealous anti-spam technologies.[19] A 2005 Federal Trade Commission (FTC) report estimated that businesses spent $1 billion on anti-spam products in 2004 and that over the previous two years consumers had spent more than $2.6 billion on filtering software to block spam.[20]

Because so much of all e-mail sent through ISPs is spam,[21] ISPs bear the burden of purchasing additional bandwidth and increasing the capacity of their technology to keep pace with the increasing volume of spam. ISPs also invest in anti-spam products,[22] leading to an endless

---

15. Adam Hartley, *Spam Gets 1 Response Per 12,500,000 Emails: New Study Details How Junk Mailers Still Make Money*, TECHRADAR UK (Nov. 10, 2008), *available at* http://www.techradar.com/news/computing/spammers-get-1-response-to-12-500-000-e-mails-483381.

16. There is some dispute as to the precise definition of an Internet Service Provider, *see infra* note 56, but one basic definition is a company that offers its customers access to the Internet.

17. *See* Ledbetter, *supra* note 14, at 107-08.

18. *See* PREPARED STATEMENT OF THE FEDERAL TRADE COMMISSION ON UNSOLICITED COMMERCIAL EMAIL (2001), *available at* http://www.ftc.gov/os/2001/04/unsolicommemail.htm (explaining that server-based filtering can cause desired messages to be missed, but client-level filtering requires users to spend more time and energy dealing with spam).

19. FEDERAL TRADE COMMISSION EFFECTIVENESS AND ENFORCEMENT OF THE CAN-SPAM ACT: A REPORT TO CONGRESS 15 (Dec. 2005), *available at* http://www.ftc.gov/reports/canspam05/051220canspamrpt.pdf.

20. *Id.*

21. *See* YALE ENV'T 360 DIGEST, *supra* note 12.

22. *See* FEDERAL TRADE COMMISSION, *Spam Summit*, *supra* note 13, at 2 (citing an FTC study finding that ISPs' spam filters continue to serve a key role in reducing the amount of spam delivered to consumers' inboxes).

game of technological one-upmanship, as spammers continue to develop wily new techniques for getting around increasingly sophisticated spam filters.[23]

Because of all this wasted time and energy, spam also creates environmental costs. According to a recent study, "[t]ransmitting, deleting, and reading the estimated 62 trillion junk e-mails sent worldwide [in 2008] wasted enough electricity to power 2.4 million American homes and created greenhouse emissions equivalent to 3.1 million cars."[24] The report explains that "[r]oughly 80 percent of the greenhouse gas emissions caused by the avalanche of spam came from the electricity consumed as computer users sifted through, viewed, and deleted junk e-mails," while "the remaining energy consumption was due to transmitting spam . . . and the electricity consumed by spam filters."[25]

3. Objectionable Content: Pornography, Fraud, and Scams, Oh My!

In addition to wasting the time and money of third parties, and contributing to environmental problems, spam is often fraudulent[26] or pornographic in nature.[27] Consumers have reported being especially bothered by unwanted sexually explicit material.[28] A 2003 Pew report goes so far as to speculate that, "[s]o extreme was the reaction to pornography that eliminating it alone among all unsolicited e-mail would go a long way toward softening spam's negative impact on Internet users."[29]

---

23. *See* Ledbetter, *supra* note 14, at 126 (describing increasingly advanced techniques used by spammers to get around anti-spam systems).

24. YALE ENV'T 360 DIGEST, *supra* note 12.

25. *Id.*

26. *See* DEBORAH FALLOWS, PEW INTERNET & AMERICAN LIFE PROJECT, SPAM: HOW IT IS HURTING E-MAIL AND DEGRADING LIFE ON THE INTERNET 36 (2003), *available at* http://www.pewinternet.org/Reports/2003/Spam-How-it-is-hurting-email-and-degrading-life-on-the-Internet.aspx?r=1 (finding that spam messages have a high rate of fraud and falsity, and that 12 percent of e-mail users reported responding to an e-mail offer only to find that it was phony or fraudulent).

27. *See, e.g.*, United States v. Kilbridge, 507 F. Supp. 2d 1051 (Ariz. Dist. Ct. 2007) (finding defendants liable for using their spamming operation to distribute pornography and commit fraud and money laundering).

28. Fallows, *supra* note 26, at 57 ("In nearly every measure we tested, pornography soared to the top as the most offensive, objectionable, destructive type of spam").

29. *Id.*

4. Spam Takes a Turn for the Worse: Malicious Bots and Criminal Vectors

Spam has lately become much more than just frustrating, time-consuming or offensive for recipients, and can now be genuinely destructive in terms of personal property and sensitive information. A 2007 FTC report states that the agency has seen "a change in the underlying motives for sending spam," and that "this new generation of spam is no longer a mere annoyance to e-mail recipients and ISPs; often it is a vector for criminal activity."[30] Spam is no longer used only for unwanted commercial advertising, but may now dupe consumers into divulging personal information, infect a consumer's computer with spyware or a virus, or hijack a consumer's computer for use in a "botnet."[31]

This use of "malicious bots" for sending spam has been credited with increasing the volume of spam[32] and making spammers increasingly difficult to catch.[33] Spammers will send out a computer virus in a spam message, which infects an innocent computer, turning that computer into a "bot." The infected computer will then periodically connect back to a central server from which the sender of the virus can take control of the "bot," allowing spammers to perpetrate a variety of malicious acts on the Internet remotely and anonymously.[34] Victims are usually completely unaware their computers have been hijacked and made part of a network of hijacked computers—a "botnet"—making it increasingly difficult for authorities to distinguish culpable spammers from innocent victims or discover the true origin of spam e-mails.[35] Because botnets provide tremendous computing power, they also allow spammers to commit more serious cybercrimes, such as breaking encryptions and recovering messages, passwords, or data.[36]

30. FEDERAL TRADE COMMISSION, *Spam Summit*, *supra* note 13, at 3.

31. *Id.*

32. *See, e.g.*, Keizer, *supra* note 10 (exemplifying how much botnets contribute to the quantity of spam). Shutting down a single central command site in California temporarily reduced the entire *global* spam volume by as much as 75 percent. *Id.*

33. FEDERAL TRADE COMMISSION, *Spam Summit*, *supra* note 13, at 2-3.

34. *Id.*

35. *Id.*

36. Michael Ena, *Securing Online Transactions: Crime Prevention Is the Key*, 35 FORDHAM URB. L.J. 147, 158 (2008).

III. A BRIEF HISTORY OF SPAM CONTROL

A. *Self-Help and Vigilantism: The Internet's Wild West Era*

In the heady, early years of the Internet, spam was most frequently combated through individual vigilantism. Dr. Brian Reid, a co-creator of the Usenet hierarchy in the early 1980s,[37] recalls that:

> [I]n the era when people had to send spam with their own computers or computers that could be traced to them, spam was a very personal thing, and you saw a lot of personal revenge. Having located a perpetrator's computer, the revenge-taker would then flood them with bogus replies to the spam, pounding relentlessly to fill the sending computers' disks with hundreds of thousands of copies of the fake spam replies. Spamming the spammer, as it were.[38]

The self-help approach proved increasingly ineffective as spammers discovered more insidious techniques. "Vigilante response by technical experts was pretty common until the spammers figured out that they could send the spam indirectly by bouncing it through stolen machines. At that point, vigilante response was essentially hopeless."[39]

B. *State Laws: A Patchwork Regulatory Approach*

Starting in the 1990s, state legislatures began to attempt to remedy the spam problem on a state level. Nevada passed an anti-spam law in 1997, and thirty-five other states followed suit.[40] A number of these state laws allowed for a range of private rights of action in addition to government enforcement.[41] Concerns over differing standards, difficulty of compliance, and the apparent ineffectiveness of state laws[42] in the

---

37. *See Giganews Usenet History: Brian Reid, available at* http://www.giganews.com/usenet-history/reid.html.

38. Telephone interview with Brian Reid, Father of the Author and Director of Engineering and Technical Operations, Internet Sys. Consortium (Dec. 16, 2008).

39. *Id.*

40. *See* John E. Brockhoeft, *Evaluating the CAN-SPAM Act of 2003*, 4 LOY. U. NEW ORLEANS SCH. L. - L. & TECH. ANN. 1, 2 (2003) (citing all thirty-six state statutes individually).

41. *Id.* at 25-32.

42. The congressional record described state law ineffectiveness:

> 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 for law-abiding businesses to know with which of these disparate statutes they

face of the growing spam problem[43] prompted the federal government to pass the CAN-SPAM Act of 2003.[44]

C. *Taking it Federal: The CAN-SPAM Act*

The CAN-SPAM Act, *inter alia*, requires that unsolicited commercial e-mails give recipients an opt-out method,[45] bans false or misleading e-mail header information, and prohibits deceptive subject lines.[46] The Act does not ban all unsolicited commercial e-mails, but instead regulates their dissemination and provides penalties for their misuse.

In passing the statute, members of Congress emphasized that they took the threat of spam seriously. "Spam, is much more than a technological nuisance," Sen. Patrick Leahy said. "In the past few years, it has become a serious and growing problem that threatens to undermine the vast potential of the Internet."[47] Discussion in Congress also acknowledged that legislation alone was unlikely to solve the difficult problem of stopping spam, and that technological solutions and efforts by non-government parties would also need to play a major role. "We believe that stopping spam is going to take a multi-pronged effort, including technology, increased FTC enforcement, and [the] enhanced ability of ISPs to go after the bad actors," Sen. John McCain said.[48]

---

are required to comply.

149 CONG. REC. S13012-01 (2003).

43. *Id.* ("The convenience and efficiency of electronic mail are threatened by the extremely rapid growth in the volume of unsolicited commercial electronic mail").

44. Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act of 2003, Pub. L. No. 108-187, 117 Stat. 2699-2719 (2003) (codified as amended at 15 U.S.C. §§ 7701-7713).

45. Reid, *supra* note 38.

> [T]his opt-out requirement has caused one of the most insidious effects in the industry. If a person responds to the opt-out request, that proves to a potential spammer that the person actually read the message. An e-mail address that reached someone who actually read the message and understood it enough to ask for opt-out is a treasure, and sells for ten times the price of more random e-mail addresses. In my experience, most spam that contains an opt-out provision is really just using that to build lists of more valuable names that can be sold.

Id.

46. Controlling the Assault of Non-Solicited Pornography and Marketing Act, 15 U.S.C. §7704(a) (2003).

47. 149 CONG. REC. S15938-01 (2003).

48. 149 CONG. REC. S13012-01 (2003).

IV. PRIVATE ENFORCEMENT OF THE CAN-SPAM ACT

The CAN-SPAM Act gives the FTC primary enforcement responsibility,[49] and in some cases it allows enforcement actions by state attorneys general,[50] or the Department of Justice, in the case of more severe criminal violations.[51] However, the Act provides a private right of action for a "provider of Internet access service" who has been "adversely affected by a violation" of certain sections of the Act pertaining to the transmission of "commercial electronic mail."[52] Providers of "Internet access service" meeting these requirements may seek injunctive relief, recover monetary damages for actual loss incurred as a result of the violation, and/or collect statutory damages based on the number of unlawful messages transmitted."[53]

For the purposes of the CAN-SPAM Act, "Internet access service" is defined as:

> [A] service that enables users to access content, information, electronic mail, or other services offered over the Internet, and may also include access to proprietary content, information, and other services as part of a package of services offered to consumers. Such term does not include telecommunications service.[54]

This definition is quite broad on its face. It is not clear from the text alone whether this language was intended to describe a specific category of existing companies, or was intentionally crafted to be sufficiently open-ended to encompass a variety of entities not specifically contemplated by Congress at the time of the bill's enactment.

The Senate Report submitted along with the Act does little to resolve the ambiguity of the statutory language. The Report mentions that a provider of Internet access service adversely affected by a violation of the Act "could include a service provider who carried unlawful spam over its facilities, or who operated a website or online service from which recipient e-mail addresses were harvested in connection with a violation . . .", although it does not make such harvesting unlawful in and of itself.[55] This description leaves open the

49. 15 U.S.C. § 7706(a), (d), (e).

50. 15 U.S.C. § 7706(f).

51. 15 U.S.C. § 7703.

52. Controlling the Assault of Non-Solicited Pornography and Marketing Act, 15 U.S.C. §§ 7706(g), 7704 (2003).

53. 15 U.S.C. §7706(g).

54. 15 U.S.C. §7702(11) (referring to the Communications Act of 1934, 47 U.S.C. §231(e)(4) (1934)).

55. S. REP. NO. 108-102, at 21 (2003).

question of whether this category was intended to be limited to traditional ISPs and e-mail providers, or may potentially include other entities that provide other forms of "access" to services provided over the Internet.

The Senate Report mentions traditional ISPs and e-mail providers like America Online (AOL), Microsoft, and Earthlink in its discussion of the harms caused by spam,[56] and many commentators subsequently assumed that ISPs were the only private entities with standing to bring a claim under CAN-SPAM.[57] Earthlink,[58] Microsoft,[59] AOL,[60] and other traditional ISPs brought the lion's share of private actions under the CAN-SPAM Act for the first several years after its passage. However, in a number of recent cases, courts have found the broad language of the statute to allow some previously unexpected parties to bring private claims under the CAN-SPAM Act.

A. MySpace v. The Globe.com*: A New Precedent and the End of an Era*

On February 27, 2007, the Central District of California found for the first time that the operator of a social networking site had standing to bring an action under the CAN-SPAM Act.[61] In addition to setting a new precedent for private standing under the CAN-SPAM Act, *MySpace v. The Globe.com* also sounded the final death knell for a company that was once one of the brightest stars of the dot-com boom.

---

56. S. REP. NO. 108-102, *supra* note 55, at 2-3.

57. *See, e.g.*, Brockhoeft, *supra* note 40, at 41 (arguing that the CAN-SPAM Act's limitation of enforcement to "Government and ISPs" was an improvement over the broader private right action granted by many of the earlier state anti-spam statutes).

58. *See* Paul Roberts, *'Buffalo Spammer' Convicted,* IDG NEWS SERVICE, Apr. 1, 2004, *available at* http://www.pcworld.com/article/115503/buffalo_spammer_convicted.html (noting that spammer Marcak lost a civil case to EarthLink earlier in 2004).

59. *See* Press Release, Microsoft, *Microsoft and Former "Spam King" Scott Richter Announce Settlement* (Aug. 9, 2005), *available at* http://www.microsoft.com/presspass/press/2005/aug05/08-09MSRichterSettlementPR.mspx.

60. *See* Elizabeth Montalbano, *AOL Gives Away Spammer's Loot*, IDG NEW SERVICE, Aug. 11, 2005, *available at* http://www.pcworld.com/article/122193/aol_gives_away_spammers_loot.html (announcing that AOL had seized $100,000 in cash and gold bars and a Hummer H2 vehicle as part of a judgment awarded under the CAN-SPAM Act).

61. MySpace, Inc. v. The Globe.com, Inc., 2007 WL 1686966, at *5 (C.D. Cal. Feb. 27, 2007).

The Globe.com was a social networking startup founded in 1994 by two Cornell undergraduates, Stephan Paternot and Todd Krizelman.[62] The company made waves in 1998 when its Initial Public Offering (IPO) posted what was then the largest-ever one-day gain in stock price,[63] making multi-millionaires of its young founders.[64] The two quickly became what one reporter referred to as "poster boys for the concept of ephemeral Internet wealth,"[65] suffering from a spate of bad publicity over their decadent lifestyles.[66] The company expanded into other areas over the next few years, but, by 2000, the economic tide had turned, and Paternot and Krizelman were forced out of the company.[67] In 2001, The Globe.com shut down its flagship site and laid off nearly 50 percent of its employees.[68]

By 2006, what remained of The Globe.com was primarily a handful of gaming magazines and Internet communications products trying to stay afloat.[69] In January of that year, the company began to set up "dummy" profiles on the popular social networking site MySpace.com and then used those accounts to send almost 400,000 unsolicited commercial messages to MySpace users advertising The Globe.com

62. Jonathan Lawrence, *A Student-Created Company Is the Talk of the Web*, CORNELL CHRON. (Apr. 11, 1996), *available at* http://www.news.cornell.edu/chronicle/96/4.11.96/webgenesis.html.

63. Dawn Kawamoto, *TheGlobe.com's IPO One for the Books*, CNET NEWS (Nov. 13, 1998), *available at* http://news.cnet.com/2100-1023-217913.html. *But see* Richard Shim, *TheGlobe.com to Cut Staff, Fold Sites*, CNET NEWS (Aug. 3, 2001), *available at* http://news.cnet.com/TheGlobe.com-to-cut-staff,-fold-sites/2100-1023_3-271110.html (noting that the record was beaten in 1999 when VA Linux Systems posted a 697 percent first-day gain).

64. *See* George Mannes, *Spinning theglobe: The Net Bubble through the Eyes of Callow Youth*, THESTREET.COM (Sep. 1, 2001), *available at* http://www.thestreet.com/tech/georgemannes/10000562.html (stating that the two 24-year-old co-CEOS were briefly worth $97 million on paper).

65. *Id.*

66. Edward Helmore, *So Who's Crying over Spilt Milk?*, THE GUARDIAN (May 10, 2001), *available at* http://www.guardian.co.uk/technology/2001/may/10/internet.onlinesupplement (noting that Paternot famously appeared in a 1999 CNN interview dancing on a table in black pleather pants with his model girlfriend and stating, "Got the girl. Got the money. Now I'm ready to live a disgusting, frivolous life").

67. Shim, *supra* note 63 (describing the company as "the poster child for companies that successfully managed to cash in on the Internet frenzy that hypnotized Wall Street, but then crashed hard").

68. *Id.*

69. *See* Vonguard, *Game Mags Gone Because of MySpace Spam?*, GIGAGAMEZ (Mar. 13, 2007), *available at* http://gigaom.com/2007/03/13/game-mags-gone-because-of-myspace-spam/ (describing TheGlobe.com as a "media conglomerate" which owned several gaming magazines). *See also* MySpace, Inc., 2007 WL 1686966, at *1 (referring to the defendant as "a public company that provides internet-based communications services" and "operates one or more websites under various domain names").

products.[70] MySpace brought a civil suit against the company, alleging violations of the CAN-SPAM Act, the Lanham Act, and sections of the California Business and Professions Code.[71]

The court found that MySpace had standing to bring a private action under the CAN-SPAM Act as a "provider of Internet access service" providing access to "electronic mail."[72] The court described MySpace.com as "an online social networking service that allows members to create personal profiles in order to find and communicate with other people," emphasizing that "[a] MySpace member accesses his e-message account on the internet, at the MySpace.com website."[73] The court declared that "the plain meaning of the statutory language" defining an Internet Access Provider was "unambiguous," and clearly included "traditional Internet Service Providers, any e-mail provider, and even most website owners,"[74] drawing a distinction between the terms "Internet *Access* Provider" (IAP) and "Internet *Service* Provider" (ISP).[75] The court also found that MySpace messages constituted "e-mail" for the purposes of the Act.[76] The court reasoned that CAN-SPAM limits standing to those entities "adversely affected" by conduct in violation of the provisions regulating electronic mail, and therefore, only those Internet access providers which provide access to electronic mail had standing to bring a private action under the Act.[77]

The Globe.com disputed MySpace's standing to bring this action, arguing that the CAN-SPAM provision allowing private actions was intended only for traditional ISPs and that MySpace was not an ISP.[78] The defendant also argued that MySpace e-messages did not sufficiently resemble traditional e-mail as envisioned by the Act, relying on the proposition that only providers of access to e-mail could be granted

---

70. *MySpace, Inc.*, 2007 WL 1686966, at *1.

71. *Id.*

72. *Id.* at *5.

73. *Id.* at *1.

74. *Id.* at *3.

75. Some courts have treated these terms as interchangeable for purposes of the CAN-SPAM Act. *See, e.g.*, Brosnan v. Alki Mortgage, LLC, 2008 U.S. Dist. LEXIS 14739, at *3-4 (N.D. Cal. 2008).

76. *MySpace, Inc.*, 2007 WL 1686966, at *4.

77. *Id.* CAN-SPAM defines an "electronic mail message" as "a message sent to a unique electronic mail address," while "electronic mail address" is defined as "a destination, commonly expressed as a string of characters, consisting of a unique user name or mailbox . . . and a reference to an Internet domain . . . to which an electronic mail message can be sent or delivered." *Id.* (citing Controlling the Assault of Non-Solicited Pornography and Marketing Act, 15 U.S.C. § 7702(5)-(6) (2003)).

78. *Id.* (rejecting defendant's position that "only traditional ISPs have a right to sue under CAN-SPAM").

standing.[79] The court rejected defendant's arguments, reasoning that it would be contrary to congressional intent to limit protection only to traditional e-mail and traditional ISPs, stating that "[r]egardless of who has a private right of action under the statute, the overarching intent of this legislation is to safeguard the convenience and efficiency of the electronic message system and to curtail overburdening of the system's infrastructure."[80] The court held that MySpace therefore met the definition of a provider of Internet access service for purposes of the CAN-SPAM Act.[81]

The court granted MySpace.com's motion for summary judgment in part.[82] The court found The Globe.com to be in violation of the CAN-SPAM Act and sections of the California Business code, and ordered defendant to pay $50 per electronic message sent after March 17, 2006.[83] This judgment, which The Globe.com reported would cost it $5.5 million, combined with the anticipation of a large federal judgment (potentially as high as $120 million), effectively shuttered operations for good.[84] This first case expressly granting private enforcement of the CAN-SPAM Act to a social networking site also put the final nail in the coffin of one of the Internet's earliest social networking startups.

B. Facebook v. ConnectU*: The Social Networking Trend Continues*

Another California district court reached a similar conclusion regarding private enforcement of the CAN-SPAM Act in 2007.[85] In *Facebook v. ConnectU*, the Northern District of California found that Facebook had standing to bring a CAN-SPAM civil action against competing social networking site ConnectU.[86]

---

79. *Id.*

Defendant maintains that MySpace e-messages do not constitute CAN-SPAM protected e-mail because: (1) unlike e-mail, MySpace e-messages have no real "route" because the messages always remain within the "walled garden" of MySpace; (2) MySpace e-messages are not e-mail because they do not use simple mail transfer protocol ("SMTP"); and (3) unlike e-mail addresses, MySpace e-message addresses have no domain part.

Id.

80. *Id.*
81. *Id.* at *5.
82. *Id.* at *11.
83. *Id.*
84. *See* Vonguard, *supra* note 69.
85. Facebook, Inc. v. ConnectU LLC, 489 F. Supp. 2d 1087, 1094 (N.D. Cal. 2007).
86. *Id.*

The suit arose out of a dispute between the ConnectU founders and Mark Zuckerberg, the founder and chief executive of Facebook.[87] In 2003, when all parties involved were undergraduate students at Harvard, the ConnectU founders hired Zuckerberg to help program their campus-wide social networking site, then called HarvardConnection.[88] Zuckerberg went on to develop a competing site at thefacebook.com (now known as Facebook) early in 2004, ending his work with the ConnectU founders, brothers Cameron and Tyler Winklevoss and their colleague, Divya Narendra.[89] Facebook has since become an enormously popular and profitable social networking site,[90] while ConnectU has had little success.[91] The ConnectU founders filed suit against Zuckerberg for breach of contract and misappropriation of trade secrets,[92] and Facebook filed counterclaims accusing ConnectU of a variety of unfair business practices, including violations of the CAN-SPAM Act.[93]

Facebook alleged that ConnectU collected e-mail addresses of registered Facebook users posted on the Facebook website and then sent solicitation e-mail to those persons in violation of the CAN-SPAM Act.[94] ConnectU contended that Facebook was not a "provider of Internet access service adversely affected" by violations of the CAN-SPAM Act, and so lacked standing to pursue its claim.[95] The court found that Facebook did indeed have proper standing, but unlike the *MySpace* court, which found the statute's language "unambiguous," the *Facebook* court indicated that it believed this interpretation to be a

87. Jason Pontin, *Who Owns the Concept if No One Signs the Papers?*, N.Y. TIMES, Aug. 12, 2007.

88. *Id.*

89. *Id.* (noting that "Mr. Zuckerberg abandoned the project in February 2004, a month after registering the domain name thefacebook.com").

90. *See, e.g.*, Saul Hansell, *Yahoo Woos a Social Networking Site*, N.Y. TIMES (Sep. 22, 2006) (describing Yahoo's offer to purchase Facebook for $900 million in 2006).

91. Pontin, *supra* note 88 (noting that as of the publication of the article, ConnectU had no more than 70,000 registered users).

92. Trial Pleading for Petitioner at 1, ConnectU LLC v. Zuckerberg, 2004 WL 2778369 (D. Mass. Sept. 2, 2004) (showing that ConnectU's complaint includes breach of contract, misappropriation of trade secrets, breach of fiduciary duty, unjust enrichment, intentional interference with prospective business advantage, and fraud).

93. Facebook, Inc. v. ConnectU LLC, 489 F. Supp. 2d 1087, 1089-90 (N.D. Cal. 2007). *See also* Brad Stone, *Facebook to Settle Thorny Lawsuit Over Its Origins*, N.Y. TIMES, Apr. 7, 2008, *available at* http://bits.blogs.nytimes.com/2008/04/07/facebook-to-settle-thorny-lawsuit-over-its-origins/.

94. *Facebook, Inc.*, 489 F. Supp. 2d at 1089.

95. *Id.* at 1094.

departure from the group of entities originally contemplated by Congress. The court reasoned that:

> [A]lthough this definition appears primarily to contemplate services that provide consumers their initial *connection* point to the Internet, the language is broad enough to encompass entities such as Facebook that provide further access to content and communications between users for persons who may initially access the Internet through a conventional "internet service provider."[96]

The court's decision helped solidify the principle that operators of social networking sites have standing to bring private claims under the CAN-SPAM Act, while acknowledging that this was an expansion of the category, at least as it had been put into practice until these cases were brought.

The court found that while Facebook did indeed have standing to pursue the claim, ConnectU's alleged conduct did not amount to a violation of the CAN-SPAM Act.[97] The court pointed out that to state a claim under CAN-SPAM, Facebook was required to allege that ConnectU sent e-mail containing "materially false or materially misleading" header information, which includes "information that is technically accurate but includes an originating electronic e-mail address . . . the access to which for purposes of initiating the message was obtained by means of false or fraudulent pretenses or representations . . ."[98] Facebook contended that ConnectU had acted deceptively in gathering the destination e-mail addresses from the profiles of its registered users, and that this was sufficient to satisfy the requirements of the statute.[99] The court disagreed, finding that because Facebook had not alleged that any e-mails sent by ConnectU contained false or misleading header information, their alleged actions did not amount to a violation of CAN-SPAM.[100]

C. Haselton v. Quicken Loans: *Pushing the Standing Envelope*

A Washington district court took the broadening of standing for private actors under CAN-SPAM a step further in October of 2008,

96. *Id.*

97. *Id.* at 1095.

98. *Id.* at 1094-95 (citing 15. U.S.C. §7704(a)(1)).

99. *Id.* at 1095.

100. *Id.* (noting that after Facebook asserted at the hearing that it could truthfully allege that at least some e-mails sent by ConnectU did contain false or misleading header information, the court dismissed the claim but gave leave to amend).

finding plaintiff Peacefire.org to qualify as "a provider of Internet access service adversely affected" by a violation of the Act.[101]

Peacefire.org describes itself as a website created "to represent the interests of people under 18 in the debate over freedom of speech on the Internet," and primarily provides information about how to disable various content-blocking software programs.[102] The site also sends a weekly newsletter to subscribers.[103] Peacefire.org is run by anti-filtering activist Bennett Haselton, the site's administrator and sole employee, who sued Quicken in his individual capacity as well as suing on behalf of his company.

In finding Peacefire.org to qualify as an Internet Access Provider for the purposes of a CAN-SPAM claim, the court relied on the Act's language defining an IAP as "a service that enables users to access content, information . . . or other services offered over the Internet."[104] Because Peacefire.org helps users gain access to information that would otherwise be censored, the court found that the service "enables users to access content," falling within the ordinary meaning of the statute's language.[105] The decision made no reference to whether this interpretation was consistent with Congress's intent.

The court did not inquire into the question of whether the site provided electronic messages of any kind, noting only that the plaintiff had experienced "significant adverse effects" from spam, including the "purchase of spam filters and software to combat spam; loss of productive time expended in monitoring and deleting spam; [and] the consequences of erroneously deleting legitimate and important e-mail."[106]

D. Subsequent Social Networking Cases: Record-Breaking Judgments

Two cases subsequent to the first rulings on social networking sites have added to the body of case law confirming that these sites have the right to sue under CAN-SPAM.[107] In both cases, major social networking sites took notorious professional spammers to task for spamming social network users. In *MySpace v. Wallace*, the court relied

101. Haselton v. Quicken Loans, Inc., 2008 WL 3046980, at ¶2.1.1 (W.D. Wash. 2008).

102. *About Peacefire.org, available at* http://www.peacefire.org/info/about-peacefire.shtml.

103. *Id.*

104. *Haselton*, 2008 WL 2386040, at ¶2.1.1.

105. *Id.*

106. *Id.* at ¶2.1.2.

107. MySpace, Inc. v. Wallace, 498 F. Supp. 2d 1293, 1301 (C.D. Cal. 2008); Facebook, Inc. v. Guerbuez, 2008 U.S. Dist. LEXIS 108921 (N.D. Cal. 2008).

on reasoning from *MySpace v. The Globe.com* to hold, in a pre-trial motion, that messages sent from MySpace member accounts qualify as "electronic mail messages" and are thus protected by the CAN-SPAM Act.[108] *Facebook v. Guerbuez* awarded statutory damages to Facebook for aggravated violations of the CAN-SPAM Act, and the court enjoined the defendant from accessing Facebook in any way.[109] Both cases ultimately resulted in default judgments against the spammers, for $230 million and $873 million respectively, the largest judgments of their kind.[110] While these default judgments are likely to be difficult to collect, the size of the awards indicate that the social networking sites have become major players in the private enforcement of the CAN-SPAM Act, on par with more traditional ISPs and e-mail providers. The size of the judgments may also reflect the advances in technology that have allowed spammers to exponentially increase the volume of messages sent. The CAN-SPAM Act imposes a monetary fine per message sent, and as technology allows spammers to increase the volume of messages sent many times over, the fines have correspondingly ballooned in size.

E. Gordon v. Virtumundo*: The Ninth Circuit Weighs In*

In August of 2009, the Ninth Circuit ruled on the question of standing under the CAN-SPAM Act for a private individual who leased server space and managed e-mail addresses for himself, friends, and family members but used them primarily for the purpose of collecting spam in order to file lawsuits against spammers.[111] The court found that the plaintiff lacked standing to bring a private action under the CAN-SPAM Act,[112] and attempted to establish some guidelines for courts addressing this question in the future.[113]

The plaintiff, Gordon, registered the Internet domain "gordonworks.com" and leased server space through GoDaddy, a domain registrar and web hosting company.[114] Through this service and

108. *Wallace*, 498 F. Supp. 2d at 1300.

109. *Guerbuez*, 2008 U.S. Dist. LEXIS 108921, at *1-2.

110. *See* Deborah Gage, *Facebook Wins $873 Million Case against Spammer*, SAN FRAN. CHRON., Nov. 25, 2008, at D1, *available at* http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2008/11/24/BUBO14B6J6.DTL (noting that the Facebook judgment was the largest ever under CAN-SPAM).

111. Gordon v. Virtumundo, Inc., 575 F.3d 1040, 1045-46 (9th Cir. 2009).

112. *Id.* at 1048.

113. *Id.* at 1049 ("Neither we nor any of our sister circuits have comprehensively addressed this issue. We endeavor to do so here, at least in part").

114. *Id.* at 1045.

through the use of a Verizon broadband connection, he was able to post content on the Internet, create e-mail accounts, and set user names and passwords.[115] He created a personal e-mail address for himself and six friends and family members.[116] However, instead of attempting to avoid or block spam messages, Gordon intentionally enrolled these accounts in as many mailing lists as possible for the express purpose of accumulating spam in order to bring lawsuits against spammers.[117] Gordon then brought suit under the CAN-SPAM Act against Virtumundo, Inc. and Adknowledge, Inc., of whom the court stated, "[i]n the parlance of our time, they are 'spammers.'"[118] The district court granted defendants' motion for summary judgment on the grounds that Gordon lacked standing under the Act, and Gordon appealed to the Ninth Circuit.[119]

In examining the question of Gordon's standing under CAN-SPAM, the court found as an initial matter that "the statutory standing provision read as a whole is ambiguous," and that "the case law regarding the relevant legal standards is 'scant.'"[120] The court therefore applied techniques of statutory construction to attempt to discern Congress's intent with regard to the proper interpretation of this provision.[121]

The court enumerated four main factors which influenced its analysis. The first was that "the purpose of the CAN-SPAM Act was not to stamp spam out of existence," and the second was that "Congress conferred standing only on a narrow group of possible plaintiffs . . . ."[122] The third was that in limiting the private right of action, "[w]e surmise that Congress's intent was to limit enforcement actions to those best suited to detect, investigate, and, if appropriate, prosecute violations of the CAN-SPAM Act . . . ."[123] The court also speculated that one of Congress's reasons for granting the private right of action to only a narrow group of private plaintiffs was that "lawmakers were wary of the possibility, if not the likelihood, that the siren song of substantial

115. *Gordon*, 575 F. 3d at 1045.

116. *Id.*

117. *Id.* at 1052. "Gordon has filed and continues to file numerous actions in state and federal courts against various defendants, often representing himself pro se." *Id.* at 1056, n.14. "As Gordon concedes, he is a professional plaintiff." *Id.* at 1056.

118. *Id.* at 1045.

119. *Id.* at 1045.

120. *Id.* at 1048-49.

121. *Gordon*, 575 F. 3d at 1049.

122. *Id.*

123. *Id.* at 1050.

statutory damages would entice opportunistic plaintiffs to join the fray, which would lead to undesirable results."[124] Fourth, the court cited "the unique nature of the subject matter at issue," and the fact that "in this arena, the engine of innovation moves far more quickly and nimbly than the methodical pace of legislation."[125]

The court concluded that "Gordon does not fit any reasonable definition of 'Internet access service' provider."[126] The court reasoned that "he neither has physical control over nor access to the hardware, which GoDaddy owns, houses, maintains, and configures," and that his service was limited to setting up e-mail accounts and log-in passwords, a service which GoDaddy and Verizon provided to him.[127] The court was also particularly "troubled" by the fact that Gordon failed to operate as a genuine e-mail provider; instead monitoring the e-mail addresses himself in order to gather spam messages as fodder for lawsuits.[128] Gordon admitted to "setting up domains as 'spam traps' with the sole purpose of snagging as many e-mail marketing message as possible."[129]

In addition to finding that Gordon was not an "Internet access service" provider within the meaning of the CAN-SPAM Act, the court found that he was not "adversely affected by" a violation of the Act.[130] While the court found that "Gordon has undoubtedly encountered a large volume of commercial e-mail," this was not sufficient to meet the "adversely affected" requirement.[131] The court expressly stated that the language of the Act was ambiguous with respect to the types of harms that should fall under the "adversely affected by" language, but concluded that "the type of harm envisioned by Congress did not encompass the ordinary inconveniences experienced by consumers and end users."[132] The court held that "[i]t is readily apparent that Gordon, an individual who seeks out spam for the very purpose of filing lawsuits, is not the type of private plaintiff that Congress had in mind when it fashioned [the CAN-SPAM Act's] standing provision."[133]

The court went beyond ruling on the narrow question of whether Gordon had standing under CAN-SPAM, and attempted to establish

124. *Id.*
125. *Id.*
126. *Gordon*, 575 F. 3d at 1052.
127. *Id.*
128. *Id.*
129. *Id.* at 1056.
130. *Id.* at 1052-53.
131. *Gordon*, 575 F. 3d at 1052.
132. *Id.* at 1053.
133. *Id.* at 1055.

some guidelines for the future, although it declined to establish a definitive framework for determining which parties have standing under the Act. The court states that:

> We do not purport to enumerate each and every harm that might satisfy the CAN-SPAM Act's standing provision . . . . At minimum, however, the harm must be both real and of the type experienced by ISPs. While the harm need not be significant in the sense that it is grave or serious, the harm must be of significance to a bona fide IAS provider—something beyond the mere annoyance of spam and greater than the negligible burdens typically borne by an IAS provider in the ordinary course of business. In most cases, evidence of some combination of operational or technical impairments and related financial costs attributable to unwanted commercial e-mail would suffice . . . . Courts should take an especially hard look at the cited harm if it suspects at the outset that a plaintiff is not operating a bona fide Internet access service, as is the case here.[134]

The court went on elaborate that there is also a question of whether the harm is actually attributable to violations of the Act, as, "[a]fter all, network slowdowns, server crashes, increased bandwidth usage, and hardware and software upgrades bear no inherent relationship to spam or spamming practices. On the contrary, we expect these issues to arise as a matter of course."[135] The court stated that "there must be . . . a showing that identified concerns are linked in some meaningful way to unwanted spam and, in turn, represent actual harm. The e-mails at issue in a particular case must, at the very least, contribute to a larger, collective spam problem that causes ISP-type harms."[136] The court did recognize that, "we are troubled by the possibility that imposing a direct causation requirement, although not inconsistent with the statutory text, might create an unworkable standard for private plaintiff standing given the impracticability of tracing a harm to a specific e-mail or batch of e-mails," and reserved a definitive determination of this question for another case where the issue was more squarely before the court.[137]

The court concluded that "the threshold of standing should not pose a high bar for the legitimate service operations contemplated by Congress," because where "well-recognized ISPs or plainly legitimate Internet access service providers file suit[,] adequate harm might be presumed because any reasonable person would agree that such entities

134. *Id.* at 1053-54.
135. *Id.* at 1054.
136. *Gordon*, 575 F. 3d at 1054.
137. *Id.* at 1054, n.12.

dedicate considerable resources to and incur significant financial costs in dealing with spam."[138] Whereas, when "a private plaintiff's status as an IAS provider is questionable and reasonably contested, courts should not only inquire into the plaintiff's purported Internet-related service operations but also closely examine the alleged harms attributable to spam."[139] In essence, the court established two tiers of private plaintiffs with distinctive burdens for establishing standing under the CAN-SPAM Act. Well-recognized ISPs and "plainly legitimate Internet access service providers" are afforded a presumption of harm, while "questionable" IAS providers receive greater scrutiny of their statuses, the alleged harm suffered, and whether that harm was directly attributable to the e-mails in question.

V. LOOKING AHEAD: WHAT THE COURTS GOT RIGHT AND THE FUTURE OF PRIVATE CAN-SPAM ENFORCEMENT

The question of private parties bringing suits under the CAN-SPAM Act is far from resolved, but the last several years of litigation have helped develop the contours of the debate. These cases have expanded the possibility for a wider variety of entities to bring suits against spammers, while coming up against the question of how far is too far when it comes to broadening the interpretation of this provision.

The Ninth Circuit got a lot right in *Gordon v. Virtumundo*, but the court may have strayed too far in creating a new multi-part standard with little basis in the statute. The fact that Congress chose to include a specific "harm" requirement for private parties bringing suit under the Act is a good indication that a "professional plaintiff" who intentionally gathers spam for the purpose of litigation is not the private party that Congress had in mind. The court is also correct that the statutory standing provision taken as a whole is ambiguous, particularly the reference to a "provider of Internet access service." This is simply not a term with a recognized technical meaning in the technology community. It is not clear from the legislative history whether Congress intended to delineate only traditional ISPs with this phrase, and misunderstood or misused the language, or intended the provision to be sufficiently flexible to adapt to new technologies over time. It is clear that the wording of the statute that was passed appears to encompass more than traditional ISPs, and the text alone does not provide much guidance as to how much more. The court's consideration of the circumstances

138. *Id.* at 1055.
139. *Id.*

surrounding the bill's passage, and the structural limitations established in the Act, are helpful in guiding an interpretation of the provision that is sufficiently flexible to serve the Act's broad remedial purpose but not so broad that it tramples the balanced statutory scheme constructed by Congress.

However, the *Gordon* court's attempt to establish a more definitive framework for determining whether the statute's "harm" requirement has been met go beyond the bounds of reasonably interpreting an ambiguous provision. The court attempts to establish a complicated test which creates a presumption of harm for "well-recognized ISPs or plainly legitimate Internet access service providers" while establishing a very high hurdle for other private plaintiffs who might otherwise meet the statutory definition of a provider of Internet Access Service. The court would require these potential plaintiffs to somehow demonstrate that the specific spam messages in question led to the purported harm, rather than being able to rely on a showing that plaintiffs had received prohibited communications from the defendants and suffered a harm related to spam. The court itself admitted that "imposing a direct causation requirement . . . might create an unworkable standard for private plaintiff standing . . . ."[140]

Much as it does in the context of traditional constitutional standing, whether a "causation" requirement is interpreted narrowly or broadly will have a significant impact on the ability of plaintiffs who have been legitimately harmed to have their cases heard. The CAN-SPAM Act has a broad, remedial purpose. At the time the Act was passed, legislators spoke specifically about the need for a multi-pronged approach and the importance of combining state, federal, and private enforcement mechanisms to go after bad actors, as well as the far-reaching pernicious effects on both businesses and individuals that the Act was intended to combat.[141] Private plaintiffs who qualify as *bona fide* providers of Internet access service, however this phrase continues to be interpreted by the courts, should not be further hampered by a nearly insurmountable requirement of traceability of harm. The parties to which Congress has granted the right to enforce this statute for the good of all consumers should be given broad latitude to have this right vindicated.

If the court is convinced that the statute demands evidence that the harm was caused by the specific violations in question, it is not clear

140. *Id.* at 1054, n.12.

141. *Gordon*, 575 F. 3d at 1049.

why "plainly legitimate" service providers should be granted such a presumption. Either a specific showing of narrowly defined causation is required by the statute, or it is not. A better treatment of the issue would be to acknowledge that ambiguity remains with respect to which parties should have standing under this provision and to acknowledge that future courts will have to face this question on a case-by-case basis as the law continues to develop. The court's attempt to create a multi-tiered test for "harm" is simply another way of acknowledging that there will continue to be hard cases relating to this issue, and the Ninth Circuit unnecessarily muddies the analysis without any real grounding in the structure or text of the statute.

The *Facebook* and *MySpace* courts also seem to have found a good balance between construing the CAN-SPAM Act's standing provision liberally in the face of changing technologies without going beyond the bounds of the established statutory scheme. Large social networking sites with hundreds of millions of users, individual accounts, and the capacity to send messages are sufficiently similar to traditional ISPs and e-mail providers that granting them standing does not significantly undermine Congress's work in carving out a limited private cause of action and furthers Congress's intent that those entities best able to go after spammers be the ones to do so.

Interpreting the CAN-SPAM standing provision to include social networking sites such as Facebook and MySpace will further this policy because, much like technological powerhouses Microsoft and AOL, these sites have access to the resources and technology necessary to effectively hunt down major spammers. Social networking sites have both the means and motivation to take up this fight. Given the continuing proliferation of spam, opening the standing door to capable private parties is simply good public policy.

Constitutional standing again provides a useful comparison for how to best understand and construe statutory standing. In order to have Constitutional standing to bring a claim in federal court, a plaintiff must have some "personal stake" in the matter as well as being able to allege a nexus between the harm or injury experienced and the unlawful behavior.[142] Expanding standing to MySpace and Facebook, but not to every website that provides an internet service to consumers, is consistent with these underlying principles of standing. Constitutional standing requirements also provide a check on federal courts interpreting this provision too broadly. No plaintiff without a reasonable "personal

142. *See* Flast v. Cohen, 392 U.S. 83, 101 (1968).

stake," as well as actual injury, causation, and redressability, will have standing to bring a claim under CAN-SPAM in federal court, even if the statutory requirements are otherwise met.

Facebook and MySpace have a personal stake going after spammers, potentially even more so than traditional ISPs and e-mail providers, in that spam disrupts their brands and their communities. Traditional ISPs and e-mail providers are much less likely to sell themselves on the basis of their community experience or brand appeal and are, therefore, less vulnerable to that particular harm. A company like Facebook may be particularly vigilant in protecting the experience of users, because controlling the nature of this experience is the service that it provides. Social networking sites may be even more motivated to combat spam, as they exist in a much more competitive environment. Traditional ISPs exist in a relatively uncompetitive market, where the costs of switching from one provider to another are high. In contrast, many Internet users are already members of multiple social networking websites, giving those companies added incentive to fight spam. The district courts struck the right balance in granting CAN-SPAM standing to the large, sophisticated social networking sites, and this is a category of plaintiffs that will likely continue to play a significant role in private enforcement of the CAN-SPAM Act in the future.

However, the *Haselton* court takes the trend of broadening CAN-SPAM standing too far, and it strains both the statutory scheme and traditional principles of standing to the breaking point. Anti-censorship website Peacefire.org bears more resemblance to the vast majority of websites on the Internet than it does to a traditional ISP or a provider of anything that might ordinarily be understood as "Internet access service." Although not as clearly unqualified as the *Gordon* plaintiff who intentionally sought out the harm of spam, Peacefire.org is also not an appropriate recipient of the Act's private standing grant. Peacefire.org is the type of entity that a court could (and did) attempt to stretch the statutory language to include, but whose inclusion clearly does not fall within the spirit of the limited private right of action established by Congress.

Most significantly, Congress established a limited private right of action in passing the CAN-SPAM Act and specifically declined to follow the example of earlier state laws which provided a broad private right of action. Interpreting the statute's standing provision to encompass a plaintiff like Peacefire.org would potentially open the door to a huge number of small, passive websites that are not uniquely equipped to fight spammers and were clearly not contemplated by

Congress when this statute was passed. In finding that Peacefire.org had standing to bring this claim, the court reasons that by assisting users to bypass censoring software, Peacefire.org is providing "access" to information or content on the Internet. By this logic, virtually any website in existence might qualify, as most of them contain "information or content" and are, in fact, on the Internet. It would be a waste of judicial resources to open the door to a potentially unlimited number of CAN-SPAM suits, the vast majority of which would prove exhausting and fruitless.

From a constitutional standing perspective, Peacefire's "personal stake" in the matter is also less clear-cut than a company like Facebook's. Peacefire.org does not provide users with an individualized account, a mechanism for sending messages, or even a comment board but simply puts subscribers on a weekly mailing list and posts content that can be read by anyone with an Internet connection. Peacefire.org passively offers information to passers-by, while Facebook offers personalized accounts with passwords and other protections, accepting responsibility for the experience of its users.

Granting standing to Peacefire.org clearly flies in the face of both traditional principles of standing and the regulatory scheme established by the CAN-SPAM Act, in which only a limited category of specially qualified private parties were granted standing.

VI. CONCLUSION

In passing the CAN-SPAM Act, Congress prudently determined the desired balance between public and private enforcement. The judicial decisions granting standing in *MySpace* and *Facebook* are consistent with Congress's intent, the larger purposes and structure of the Act, and the ambiguous statutory language. The *Haselton* court went too far in granting standing to Peacefire, disturbing this careful balance and potentially opening the door to a flood of plaintiffs clearly not contemplated by the original statutory scheme. The Ninth Circuit wisely pulled back on this excessively broad reading of the statute, particularly in addressing the dangers of allowing opportunistic plaintiffs to take advantage of the statute's monetary rewards without meeting the spirit of the statute's requirements for private parties. However, the Ninth Circuit's focus on the "harm" requirement and its establishment of elaborate causation requirements is a mistake. Future courts should focus most on whether a given plaintiff has the resources, technology, and motivation to track down spammers and bring meritorious cases to court for the benefit of all users of e-mail and the Internet, ensuring

fidelity to the purposes and limits of the Act as it was originally passed while continuing to evolve in the face of new technologies.