Loyola Consumer Law Review

Volume 16 | Issue 3

Article 4

2004

The CAN-SPAM Act of 2003: Was Congress Actually Trying to Solve the Problem or Add to It?

Sameh I. Mobarek

The CAN-SPAM Act of 2003: Was Congress Actually Trying to Solve the Problem or Add to it?

By Sameh I. Mobarek*

I. Introduction

Imagine a world devoid of vacant space where every conceivable surface is filled with advertisements.[1] Imagine also that, after running out of space, marketers developed free-flying robots that roam the planet to hypnotize consumers into buying their products.[2] In that world, the heroes walked around, not with a six-shooter, but with a fly swatter to squash the commercials before they got them.[3] They closed their windows at night to keep the commercial pests from perching onto their pillows and seducing them as they slept.[4] Such a world existed in the fertile imagination of now deceased science-fiction writer, Philip K. Dick.[5] But how far removed from this make-belief world are we in the Spam-infested reality of today?

The problem of unsolicited commercial email advertisements, commonly called "Spam," is quickly growing to replace all other problems caused by the marketing industry. Consumers receive all

* J.D. candidate, May 2005, Loyola University Chicago School of Law; M.B.A. International Finance, 1994, George Washington University; B.S. Electrical Engineering and Computer Science, 1991, George Washington University.

[1] Brent Staples, *The Battle Against Junk Mail and Spyware on the Web*, N.Y. TIMES, Jan. 3, 2004, *available at* http://www.nytimes.com/2004/01/03/opinion/03SAT3.html?ex=1074344547&ei=1&en=6131679deb24459f (last visited Mar. 6, 2004).

[2] *Id.*

[3] *Id.*

[4] *Id.*

[5] *Id.*

types of Spam on a daily, even hourly, basis that create both annoyance and inconvenience. Internet Service Providers ("ISPs") spend millions of dollars each year to ensure that their users are shielded from the aggravations of Spam.[6] But, if recipients do not want it, and ISPs would rather not deliver it, why does Spam still exist?[7]

The term Spam is said to have developed in the 1980s when a computer user created a simple computer program that repeatedly typed the word "Spam."[8] The prankster may have been inspired by a Monty Python comedy sketch that takes place in a restaurant where every meal on the menu contained Spam, a tinned meat product for which Hormel Foods owns the United States trademark.[9] Later, the term Spam came to be applied to articles posted to newsgroups that were unrelated to the discussions involved and violated the rules of the forum.[10] Often, these articles were cross-linked with posts in other newsgroups and quickly became a nuisance.[11] Gradually, the term Spam became associated with junk email messages and advertisements for products and services of a dubious nature.[12]

The proliferation of Spam is largely supported by simple economics. The fact is that it costs much less for marketers to send Spam than for recipients to receive it and ISPs to process it.[13] In 2002, the *Wall Street Journal* undertook a study on the economics of Spam.[14] One case cited a mailing of 3.5 million Spam messages that resulted in 81 sales in the first week, a success rate of 0.0023%, with

[6] *See infra* Part II.

[7] ePrivacy Group, *The Economics of Spam, available at* http://www.eprivacygroup.com/article/articlestatic/58/1/6 (last visited Jan. 12, 2004) [hereinafter ePrivacy *Economics of Spam*]. ePrivacy Group is a privately held company that provides real-time services to verify the identity of senders of email messages and message authenticity. *See* http://www.eprivacygroup.com (last visited Mar. 16, 2004).

[8] John Magee, *The Law Regulating Unsolicited Commercial Email: An International Perspective*, 19 SANTA CLARA COMPUTER & HIGH TECH. L.J. 333, 336 (2003).

[9] *Id.* at 336-37.

[10] *Id.* at 337.

[11] *Id.*

[12] *Id.*

[13] ePrivacy *Economics of Spam*, *supra* note 7.

[14] *Id.*

each sale worth $19 to the marketer.[15] The result to the marketer was a profit of $1,500, after deducting an average cost of $100 per million messages sent, in the first week alone.[16] Now, if the same company sends 100 million messages, it would conceivably make a profit in excess of $25,000.[17] Advances in technology and broadband Internet access made this scenario a reality in less time and money to marketers.

In the face of such motivation, regulators and ISPs struggled to stem the growing tide of Spam. State legislators passed anti-Spam laws, and ISPs pursued civil actions against some of the marketers using Spam.[18] However, because of the patchwork of regulations that state laws created, and the limited resources of ISPs, it became clear that a national solution to the problem was necessary.[19] To this end, Congress debated several proposals to curb the nationwide use of Spam, ultimately enacting the CAN-SPAM Act of 2003 (the "Act") in December 2003.[20]

This article will discuss the background of the problem of Spam and some of the public and private efforts undertaken to address it.[21] In particular, this article will focus on the Act and some of its key provisions with a view to their effectiveness in meeting Congress' objectives.[22] Finally, this article will analyze the Act with regards to the overarching problem of Spam and its impact on both marketers and consumers.[23]

[15] *Id.*

[16] *Id.*

[17] *Id.*

[18] *See generally* Rene Ryman, *The Adverse Impact of Anti-Spam Companies*, 20 No. 1 COMPUTER & INTERNET LAW. 15, 16-17 (2003).

[19] Dannielle Cisneros, *Do Not Advertise: The Current Fight Against Unsolicited Advertisements*, 2003 DUKE L. & TECH. REV. 10, 12 (2003).

[20] *See generally* Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act), Pub. L. No. 108-187, 117 Stat. 2699 (2003) (codified at 15 U.S.C. §§ 7701-13; 18 U.S.C. §§ 1001, 1037; 28 U.S.C. § 994; and 47 U.S.C. § 227).

[21] *See infra* Part II.

[22] *See infra* Part III.

[23] *See infra* Part IV.

II. The Explosive Growth of Spam

The use of Spam has been steadily increasing over the past few years. The increase in just the past two years has been so explosive that Spam is estimated to have accounted for 60% of all email traffic in January 2004, or over 5 billion Spam emails on average per day.[24] The increase is staggering in comparison to 2001, when Spam accounted for only 7% of all email traffic.[25] This proliferation was aided by an increase in the number of companies engaging in such advertising, the availability of easy-to-use tools to send Spam, and a reduction of response rates from email users around the world.[26] Furthermore, this growth was also fueled by marketers' attraction to the Internet as a medium for reaching potential customers.[27] According to recent studies, 8% of all web-advertising dollars in 2000 was spent on email marketing.[28] By 2007, expenditures are expected to reach $15.9 billion, reflecting a 21% annual growth rate.[29] This growth, however, comes at an increasing price to United States corporations and consumers.

Part of the allure of Spam is the ability of marketers to shift some of the costs of advertising to consumers.[30] Some marketers resort to "Dictionary Attacks," a technique that generates millions of

[24] Brightmail, *Spam Statistics*, *available at* http://www.brightmail.com/spamstats.html (last visited Feb. 13, 2004) [hereinafter Brightmail *Spam Statistics*]. Brightmail, a San Francisco-based company founded in 1998, provides anti-Spam technology and software that makes messaging secure and manageable. The company's clients include AT&T WorldNet, EarthLink, MSN, Verizon Online, as well as a number of Global 2000 corporations. *See* http://www.brightmail.com/about_us.html (last visited Mar. 16, 2004).

[25] 15 U.S.C. § 7701(a)(2).

[26] Brightmail, *Brightmail Reports on Spam Trends of 2003* (Dec. 18, 2003), *available at* http://www.brightmail.com/pressreleases/121803_spam_2003.html (last visited Feb. 13, 2004).

[27] Ryman, *supra* note 18, at 17 (noting that, in the period between 1998 and 2000, there was almost a 10% increase in the number of households with computers, and nearly a 100% increase in the number of households with Internet access).

[28] *Id.* at 15.

[29] Research and Markets, *Marketing and Branding Forecast: Online Advertising and E-mail Marketing Through 2007*, *available at* http://www.researchandmarkets.com/reportinfo.asp?report_id=3333 (last visited Mar. 6, 2004).

[30] Cisneros, *supra note* 19, at 10.

email addresses by going through the entire alphabet in each letter placeholder of an email address.[31] Ultimately, the vast majority of these emails bounce back, generating a notification for each email that must be processed.[32] ISPs are then forced to expand their networks and systems to accommodate the avalanche of this daily Spam.[33] Companies are also forced to expand their networks to process the Spam that does match an email address.[34] Additionally, employees become less productive as they are forced to sort through individual emails to eliminate Spam.[35] A recent study estimates that Spam costs United States companies approximately $9 billion annually, and United States and European ISPs an additional $500 million.[36] Ultimately, these additional costs are likely to be passed on to consumers in the form of higher prices for the products and services that these companies provide.

If these costs were not enough to highlight the acuteness of the problem, the intentionally unscrupulous use of Spam certainly aggravates the situation. Of the total number of Spam emails circulating, approximately 12% perpetrated some kind of fraud or scam on their recipients, including pyramid schemes, stock and investment scams, and solicitations for fake charitable causes.[37] The Federal Trade Commission ("FTC") also indicated that a majority of Spam contained deception in the text, the subject line, or the "from" line.[38] For example, the FTC found that nearly half of the Spam that it analyzed contained false information in the subject or "from" line.[39] These messages claimed to be sent by someone having a

[31] Bruce Johnson, *Is There a Constitutional Right to Bombard the Public with Penis Enlargement Proposals?*, 21-SUM COMM. LAW. 3, 3 (2003).

[32] *Id.*

[33] *See generally* ePrivacy *Economics of Spam*, *supra* note 7.

[34] Cisneros, *supra* note 19, at 11, 19.

[35] *Id.*

[36] *Id.*

[37] *See* the chart in Appendix 1 on p. 266 for a breakdown of Spam by category. The information provided in Appendix 1 can be found at http://www.brightmail.com/spamstats.html (last visited Mar. 16, 2004).

[38] David Bender, *Recent Developments in Data Protection Law*, 764 PLI/PAT 9, 18 (2003).

[39] Federal Trade Commission, *False Claims in Spam*, at 7 (Apr. 30, 2003), *available at* http://www.ftc.gov/reports/spam/030429spamreport.pdf.

personal relationship with the recipient.[40] Such claims were manifested by the use of a first name only in the "from" line, suggesting that the sender was someone included in the recipient's email address book.[41] The FTC also noted that some Spam used misleading subject lines, suggesting either a personal relationship with the recipient or matters that bore no relationship to the content of the message.[42] In addition, the FTC found that some marketers use open relays to send Spam to disguise the origin of the messages.[43] The FTC identified open relays in 59 countries, but 90% of these relays were found in only 16 countries.[44]

As a result of these practices, over half of the states promulgated laws to regulate, but not prohibit, Spam.[45] These laws typically: (1) prohibit the sending of unsolicited Spam that uses a third party's Internet address or domain name without permission or contains false or missing routing information; (2) require marketers to include "ADV:" as the first four characters in the subject line of the message; (3) require marketers to identify their email address; or (4) require marketers to include instructions for, and to honor

[40] *Id.* at 4.

[41] *Id.*

[42] *Id.* at 6.

[43] *See* Federal Trade Commission, *Law Enforcement Posse Tackles Internet Scammers, Deceptive Spammers* (May 15, 2003) (defining open relays as unsecured servers that marketers use to mask the origin of their messages, and to avoid filtering programs used by ISPs), *available at* http://www.ftc.gov/opa/2003/05/swnetforce.htm (last visited Feb. 13, 2004).

[44] *Id.* These countries are the United States, China, Korea, Japan, Italy, Poland, Brazil, Germany, Taiwan, Mexico, Great Britain, France, Chile, Argentina, India, Spain, and Canada.

[45] *See generally* ARK. CODE ANN. §§ 5-41-201-205 (Michie 1987); CAL. BUS. & PROF. CODE § 17529.2 (West 2003); COLO. REV. STAT. ANN. §§ 6-2.5-101-105 (West 2000); CONN. GEN. STAT. ANN. §§ 53-451-453 (West 2003); DEL. CODE ANN. tit. 11, §§ 931-939 (West 2004); IDAHO CODE § 48-603E (Michie 2003); IOWA CODE ANN. § 714E.1 (West 2003); KAN. STAT. ANN. § 50-6,107 (West 2002); MD. CODE. ANN., COMM. LAW, § 14-3002 (West 2004); MINN. STAT. ANN. § 325M (West 2003); MO. ANN. STAT. § 407.020 (West 2004); N.C. GEN. STAT. § 14-453 (2004); OKLA. STAT. ANN. tit. 15, § 776 (West 2004); 18 PA. CONS. STAT. ANN. § 1.5903 (West 2003); R.I. GEN. LAWS §§ 11-52-1-52-4 (West 2004); S.D. CODIFIED LAWS § 37-24-6 (Michie 2003); TENN. CODE ANN. § 39-14-603 (West 2003); VA. CODE. ANN. § 18.2-152.3:1 (Michie 2003); WASH. REV. CODE. ANN. §§ 19.190.010-040 (West 2003).

requests from, recipients to be excluded from future mailings.[46] Some states, such as California and Delaware, went further by barring Spam completely, unless recipients expressly consented to receiving it.[47] Virginia, through which half of the Internet traffic passes, went even further by criminalizing the transmission of unsolicited bulk email, the use or aiding in the use of a computer or network with intent to falsify or forge email information, and the routing of information in connection with the transmission of unsolicited bulk email.[48]

ISPs have also reacted aggressively against Spam by suing marketers sending it under a range of theories.[49] These actions have included fraud and misrepresentation, trespass to chattel, trademark infringement, and breach of contract.[50] One of the early cases pursued by an ISP was *CompuServe, Inc. v. Cyber Promotions, Inc.*[51] In that case, CompuServe claimed that Cyber Promotions trespassed on its property by flooding its networks with Spam, whose origin was intentionally masked to circumvent CompuServe's filtering software.[52] The court found that Cyber Promotions' message caused CompuServe real damage by draining its network resources, thereby reducing the value of the company's computer equipment.[53] Thus, the court granted CompuServe injunctive relief and enjoined Cyber Promotions from sending Spam through CompuServe's networks.[54] However, CompuServe was not the only ISP to pursue legal remedies against marketers using Spam. In fact, America Online, Inc. ("AOL") has been the most aggressive ISP, bringing more than 23 cases,

[46] Ryman, *supra* note 18, at 15-17.

[47] *See generally* CAL. BUS. & PROF. CODE § 17529.2 (West 2003); *see also* DEL. CODE ANN. tit. 11, §§ 931-939 (2003).

[48] VA. CODE. ANN. § 18.2-152.3 (Michie 2003); *see also* Bender, *supra* note 37, at 25; *Virginia Claims Toughest Anti-Spam Law in the Nation*, 20 NO. 7 COMP. & INTERNET LAW 34, 35 (2003).

[49] John B. Kennedy & Tracy Hatch, *Recent Development in Consumer Privacy: Focus on Spam and Identity Theft*, 748 PLI/PAT 1219, 1230 (2003).

[50] *Id.*

[51] CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015 (S.D. Ohio 1997); *see also* Magee, *supra* note 8, at 348.

[52] *CompuServe,* 962 F. Supp. at 1019; *see also* Magee, *supra* note 8, at 348.

[53] *CompuServe,* 962 F. Supp. at 1022; *see also* Magee, *supra* note 8, at 348-49.

[54] *CompuServe,* 962 F. Supp. at 1017; *see also* Magee, *supra* note 8, at 349.

mostly successful, against marketers sending Spam through its networks.[55]

ISPs also employed various filtering software to block Spam before it would reach recipients or used Spam-reporting features that allowed recipients to declare particular emails to be Spam.[56] But these techniques encountered problems. Because filtering software was designed to hone in on particular phrases or patterns, email recipients had to constantly check to make sure that the filtering software did not block legitimate emails.[57] ISPs also implemented Spam-reporting features, which helped recipients block Spam from a particular sender.[58] Once a report had been made, the ISPs individually decided whether or not to block all emails from the sender to recipients on their respective networks.[59] However, marketers complained that some recipients used this feature in place of a request to unsubscribe from the senders' email list, thus making a false report of Spam.[60] As a result, marketers sending advertisements with the consent of recipients could be summarily blocked from an ISP's entire network.[61]

Some marketers tried unsuccessfully to challenge ISPs' actions on constitutional grounds. One of the early challenges came in *Cyber Promotions, Inc. v. America Online, Inc.*, decided by a federal court in the Eastern District of Pennsylvania.[62] In *America Online*, AOL blocked messages from Cyber Promotions after AOL's users complained about receiving unsolicited advertisements from the company.[63] Cyber Promotions sued AOL "seeking a ruling that it had a First Amendment right to send its email advertisements through the

[55] *See* AOL Legal Department, *AOL Junk Email Archive, available at* http://legal.web.aol.com/decisions/dljunk/aolarchive.html (last visited Mar. 6, 2004); *see also* Kennedy & Hatch, *supra* note 48, at 1230.

[56] Johnson, *supra* note 31, at 4.

[57] *Id.*

[58] *Id.*

[59] *Id.*

[60] *Id.*

[61] *See generally id.*

[62] Cyber Promotions, Inc. v. America Online, Inc., 948 F. Supp. 436 (E.D. Pa. 1995).

[63] *America Online*, 948 F. Supp. at 437; *see also* Nicole A. Wong et al., *Privacy & Marketing Issues*, 755 PLI/PAT 11, 73 (July 2003).

Internet without AOL's interference."[64] Ultimately, the court dismissed Cyber Promotions' claim on the grounds that it had other channels with which to distribute its advertisements, and that AOL was a private enterprise and did not carry out any governmental functions subjecting it to the constraints of the First Amendment.[65] Similarly, other marketers unsuccessfully attempted to challenge ISPs' actions to curb the marketers' access to their networks on the grounds that such action restrained interstate commerce, and thus, contravened the dormant Commerce Clause in the Constitution.[66]

On the federal level, the FTC brought its own enforcement actions against marketers using Spam.[67] However, its enforcement actions were limited to marketers who perpetrated fraud through Spam.[68] Since the middle of 2003, the FTC brought 53 enforcement actions in cases that involved deceptive content in Spam, relying on Section 5 of the Federal Trade Commission Act ("FTCA"), which barred misrepresentation in marketing material.[69] More recently, the FTC expanded the scope of its actions to combat not only deception in the content of Spam, but also deception in the manner of transmission of the message.[70]

Despite the growing chorus of governmental and private actions against Spam, the use of Spam continued to grow at an alarming rate.[71] Although some private actions stemmed the flow of Spam from particular offenders, these actions were expensive and

[64] *America Online*, 948 F. Supp. at 438.

[65] *Id.* at 445.

[66] Wong et al., *supra* note 63, at 73.

[67] *See generally id.* at 20.

[68] *See generally Unsolicited Commercial Email: Testimony before the Senate Comm. on Commerce, Sci., and Transp.*, 108th Cong. 2-3 (2003) (statement of the FTC), *available at* http://www.ftc.gov/os/2003/05/spamtestimony.pdf (last visited Mar. 6, 2004) [hereinafter FTC Spam Statement].

[69] *Id.* (noting the conclusion of its panel of experts that there is no quick or simple solution to the problem of Spam. Instead, "solutions must be pursued from many directions—technological, legal, and consumer action."); *see also* Federal Trade Commission Act, Pub. L. No. 108-105, § 5, 38 Stat. 717 (2003) (codified at 15 U.S.C.A. § 45).

[70] FTC Spam Statement, *supra* note 68, at 2-3.

[71] *Id.* (noting that Spam continues to grow at an exponential rate, putting email at risk of loosing its utility as an effective method of communication and online commerce).

time consuming, and could only target one offender at a time.[72] Consequently, ISPs preferred to deal with Spam through filters and other technological innovations, which, by themselves, created unintended problems.[73] In addition, the FTC's enforcement actions, though successful in most cases, were limited in number and restricted to addressing only fraudulent Spam.[74] Similarly, state laws did not seem to be effective in stemming the tide of Spam.[75] Despite state requirements that Spam include "opt-out" provisions,[76] the FTC found that 63% of the Spam it analyzed contained non-functional or inoperative return addresses included in the Spam for just that purpose.[77] Furthermore, only 2% of the Spam analyzed by the FTC contained "ADV:" in the subject line, as a majority of states require.[78] Regardless of these requirements, states lacked the necessary resources to provide adequate enforcement actions and to identify Spam originators in a highly anonymous and decentralized Internet.[79] In addition, the wide range and frequently dichotomous array of state regulations presented a substantial hurdle for legitimate marketers to adhere.[80] There was a strong need for a national framework that would unify the approach to Spam regulation and provide a more effective solution to the problem.

III. Congress' First Attempt to Address Spam

Congress' response to the growing problem of Spam was to propose a plethora of legislation that focused on various aspects of

[72] Johnson, *supra* note 31, at 4.

[73] *Id.* (noting that the number of addresses the software can block are limited, and some recipients use the filtering software in place of the unsubscribe mechanisms, thus making a false report of Spam to the ISP).

[74] *Id.*

[75] *Id.* at 5.

[76] Opt-out provisions require that a recipient of a Spam message affirmatively requests the sender to exclude the recipient from the sender's email list for the purposes of future mailings. For that purpose, senders of Spam are required to include an appropriate means, such as an email address or a web site, for the recipients to make such requests. *See* Johnson, *supra* note 31, at 5.

[77] *Id.*

[78] *Id.*

[79] *Id.*

[80] *See* Cisneros, *supra* note 19, at 12.

the problem.[81] In 2003 alone, nine proposals were presented in Congress: (1) Controlling the Assault of Non-Solicited Pornography and Marketing Act ("CAN-SPAM Act");[82] (2) Anti-Spam Act;[83] (3) Ban on Deceptive Unsolicited Bulk Electronic Mail Act;[84] (4) Computer Owners' Bill of Rights;[85] (5) Criminal Spam Act;[86] (6) Reduction in the Distribution of Spam Act;[87] (7) REDUCE Spam Act;[88] (8) Stop Pornography and Abusive Marketing Act;[89] and (9) Wireless Telephone Spam Protection Act.[90] Of this list, only the CAN-SPAM Act of 2003 (hereinafter referred to as the "Act") was enacted by Congress on December 8, 2003,[91] and signed into law by President George W. Bush on December 16, 2003,[92] effective as of January 1, 2004.[93] The following is a discussion of some pertinent provisions of the Act.

A. Scope

At the outset, Congress declared that there was a substantial government interest in the regulation of Spam.[94] However, Congress expressly limited the scope of the Act to preventing fraudulent Spam and ensuring that recipients have the right to be excluded from future

[81] *See generally* Spam Laws, *at* http://www.spamlaws.com/federal/list108.html (last visited Feb. 13, 2004) [hereinafter Spam Laws].

[82] S. 877, 108th Cong. (2003).

[83] H.R. 2515, 108th Cong. (2003).

[84] S. 1052, 108th Cong. (2003).

[85] S. 563, 108th Cong. (2003).

[86] S. 1293, 108th Cong. (2003).

[87] H.R. 2214, 108th Cong. (2003).

[88] H.R. 1933, 108th Cong. (2003).

[89] S. 1231, 108th Cong. (2003).

[90] H.R. 122, 108th Cong. (2003).

[91] *See* 149 Cong. Rec. H12854-08 (daily ed. Dec. 8, 2003), *available at* 2003 WL 22889088.

[92] *See* Fact Sheet, White House, Bush signs anti-Spam law (Dec. 16, 2003), *available at* 2003 WL 22954891.

[93] *See* Spam Laws, *supra* note 81.

[94] CAN-SPAM Act, 15 U.S.C. § 7701(b)(1) (2003).

Spam from the same source.[95] In other words, the Act was not intended to regulate Spam as a whole. Instead, it focused only on the small fraction of Spam messages that contained or perpetrated some kind of fraud.

B. Prohibitions and Requirements

The Act prohibits the use of open relays to transmit Spam.[96] It also prohibits the initiation of Spam that contains materially false or misleading header information.[97] Under the Act, materially false or misleading header information includes technically accurate header information obtained by means of false or fraudulent pretenses or misrepresentation.[98] The Act also prohibits the use of deceptive subject lines and requires that the perpetrator has actual knowledge or "knowledge fairly implied on the basis of objective circumstances" that a reasonable recipient is likely to be misled by the subject line.[99] It also outlaws the use of automated means of identifying email addresses, such as "Dictionary Attacks," to transmit Spam.[100]

Furthermore, the Act requires marketers to use a functioning return address on their messages so that recipients can use it to request that they be excluded from future mailings from the sender.[101] In the alternative, the Act requires that some other mechanism be included whereby the recipient can effectively opt out of future

[95] 15 U.S.C. § 7701(b)(2)-(3); *see also* S. REP. NO. 108-102, at 1 (2003), *available at* 2003 WL 21680759 (noting that the purpose of the Act is to "(i) prohibit senders of electronic mail (e-mail) for primarily commercial advertisement or promotional purposes from deceiving intended recipients or Internet service providers as to the source or subject matter of their e-mail messages; (ii) require such e-mail senders to give recipients an opportunity to decline to receive future commercial e-mail from them and to honor such requests; (iii) require senders of unsolicited commercial e-mail (UCE) to also include a valid physical address in the e-mail message and a clear notice that the message is an advertisement or solicitation; and (iv) prohibit businesses from knowingly promoting, or permitting the promotion of, their trade or business through e-mail transmitted with false or misleading sender or routing information.").

[96] 15 U.S.C. § 7704(a)(1)(C).

[97] 15 U.S.C. § 7704(a)(1)(A).

[98] *Id.*

[99] 15 U.S.C. § 7704(a)(2).

[100] 15 U.S.C. § 7704(b)(1)-(3).

[101] 15 U.S.C. § 7704(a)(3)(A)-(B).

mailings.[102] The Act further requires marketers to honor the recipient's wish to be excluded from future mailings within ten business days from the receipt of such a request.[103] It also requires that Spam be clearly identified as advertisement or solicitation and imposes additional identifiers in the case of Spam containing sexually explicit material.[104]

C. Enforcement and Penalties

The Act makes a violation of its prohibitions and requirements an unfair or deceptive act or practice also proscribed under the FTCA.[105] This formulation allows the FTC to enforce the prohibitions and requirements of the Act using the same enforcement tools and actions it has been using to combat Spam.[106] Furthermore, the Act authorizes other federal agencies to enforce its provisions under pre-existing enforcement regimes when the senders of Spam fall within the scope of that agency's oversight.[107] However, it is unclear how a violation of the Act would be considered a violation under some of the existing laws for the purposes of applying their enforcement provisions.[108]

The Act also authorizes states to pursue their own civil actions against violators when the interest of a state resident is threatened or adversely affected.[109] This authority is limited to actions against using false or misleading header information, omitting the proper warning in the header for Spam containing sexually explicit material, or engaging in a pattern of failing to include means for recipients to opt out of receiving future mailings or failing to

[102] *Id.*

[103] 15 U.S.C. § 7704(a)(4)(A)(i)-(ii); *see also* 15 U.S.C. § 7704(c) (allowing the FTC discretion to change the 10-day period if it deems necessary to fulfill the objectives of the Act while not imposing undue burdens on senders of legitimate commercial advertisements).

[104] 15 U.S.C. § 7704(d) (requiring that the FTC, in consultation with the Attorney General, develop a list of identifiers within 120 days of the Act's enactment to be used by senders of Spam containing sexually explicit material to identify it as such).

[105] 15 U.S.C. § 7706(a).

[106] *See generally* 15 U.S.C. § 7706(a).

[107] 15 U.S.C. § 7706(b).

[108] *See generally* 15 U.S.C. § 7706(b).

[109] 15 U.S.C. § 7706(f)(1).

honor such requests after a given time period.[110] The Act also limits the amount of damages that can be sought in such an action to the greater of (a) actual loss suffered or (b) an amount, not exceeding $2 million, calculated by multiplying the number of violations by up to $250.[111] Furthermore, the Act allows an increase in the limit on damages to $6 million if a court determines that the violation was willful or if automated means, such as "Dictionary Attacks," were used to generate email addresses to which Spam was sent.[112]

In addition, the Act authorizes ISPs to bring civil actions against violators that use false or misleading header information, use automated means to generate email addresses to which Spam was sent, send Spam containing sexually explicit material without the proper warning, or engage in a pattern of violating the Act's requirements.[113] In this type of action, the Act limits the amount of damages that can be sought to the greater of (a) actual loss suffered or (b) an amount, not exceeding $1 million, calculated by dividing the number of violations by $100 in the case of false or misleading header information, or $25 in all other cases.[114] The Act also allows a court to increase the limit on damages to $3 million if the court determines that the violation was willful or if automated means were used to generate email addresses to which Spam was sent.[115]

D. Do-Not-Email Registry

The Act requires the FTC to develop a plan and a timetable for implementing a national Do-Not-Email Registry and to report this plan and timetable to Congress no later than June 1, 2004.[116] The Act also authorizes the FTC to implement this plan no earlier than September 16, 2004.[117]

[110] *Id.*

[111] 15 U.S.C. § 7706(f)(3)(A)-(B).

[112] 15 U.S.C. § 7706(f)(3)(C).

[113] 15 U.S.C. § 7706(g).

[114] 15 U.S.C. § 7706(g)(3)(A)-(B).

[115] 15 U.S.C. § 7706(g)(3)(C).

[116] 15 U.S.C. § 7708(a).

[117] 15 U.S.C. § 7708(b).

E. Effects on Other Laws

Congress stresses that the Act's provisions are not to be construed to affect the enforcement of certain criminal statutes or the FTC's authority to bring enforcement actions under the FTCA.[118] In addition, nothing in the Act is to be construed as limiting or prohibiting ISPs from instituting and enforcing limits on the transmission, routing, relaying, handling, or storing of certain types of email.[119]

Significantly, the Act supersedes any statute, regulation, or rule of a state that expressly regulates the use of email to send commercial messages.[120] However, this provision does not apply to any state statute or regulation that prohibits false statements or deception in Spam.[121] The Act will also not preempt state laws that are not specific to email, such as laws relating to trespass, contract, and tort law, or other laws that relate to acts of fraud or computer crime.[122]

IV. A Small Step in the Direction of Effective Spam Regulation

The Act is certainly a step in the direction of addressing the growing problem of Spam. The Act's co-authors, Senators Conrad Burns and Ron Wyden, noted that it targets the most egregious behavior by marketers using Spam and provides criminal sanctions to combat them.[123] Furthermore, it mandates truthfulness in header information in Spam and the inclusion of pre-designated labels to indicate the nature of its content.[124] They stressed that these requirements will assist ISPs in preventing these messages from reaching their recipients through more effective use of software filters upon request from recipients.[125] They also stressed that these

[118] 15 U.S.C. § 7707(a).

[119] 15 U.S.C. § 7707(c).

[120] 15 U.S.C. § 7707(b)(1).

[121] 15 U.S.C. § 7707(b)(2)(B).

[122] 15 U.S.C. § 7707(b)(2)(A).

[123] Sen. Conrad Burns & Sen. Ron Wyden, *New Law Packs Potent Tools*, USA TODAY, Dec. 23, 2003, at 14, *available at* 2003 WL 5325709.

[124] *Id.*

[125] *Id.*

requirements will provide recipients effective means to opt out from future mailings, thereby controlling access to their email accounts.[126]

However, even Senators Burns and Wyden recognized that the Act is not "a silver bullet that will completely rid the world of Spam."[127] Critics of the Act charge that it fails to provide the most fundamental element of any anti-Spam law: prohibiting the very use of Spam.[128] While the Act attempts to curb abusive practices, it ignores the fact that 80% of Internet users found Spam to be "very annoying" and 74% even favored making it illegal.[129] In essence, the Act legitimizes the Spam that does not use fraudulent header information or promote fraud in its content. The Act's supporters point out that the absence of fraudulent header information will make filtering programs more effective in blocking unwanted Spam.[130] However, this objective ignores the fact that making the ISPs' task of filtering Spam easier will not eliminate the added costs to ISPs of processing the messages or ensuring that marketers will not find other ways to circumvent the software's function. Furthermore, this claim also ignores the inconvenience to recipients, who waste time in making sure that the filters do not block legitimate messages.[131]

Moreover, some commentators noted that marketers can use the Act as a defense from prosecution if they implemented reasonable practices to prevent violations of the Act, and yet, violations still occur despite their good faith efforts to comply with those practices.[132] Moreover, aside from the right of ISPs to pursue Spam users for specific violations, the Act does not evince a private right of

[126] *Id.*

[127] *Id.*

[128] Coalition Against Unsolicited Commercial Email (CAUCE), *CAUCE Statement on CAN-SPAM Act* (Dec. 16, 2003), *available at* http://www.cauce.org/news/index.shtml (last visited Feb. 13, 2004) [hereinafter CAUCE Statement]. CAUCE is an Internet-based advocacy group that works to promote awareness of the problem of Spam and lobbies legislators to pass laws to curb the abuses of Spam. CAUCE is not "an industry lobbying group" in that it does not accept donations or charge for its membership. The organization is web-based and relies on volunteers to do all its work. *See* http://www.cuace.org/about/index.shtml (last visited Mar. 16, 2004).

[129] Dawn Estes & Bhaveeni Parmar, *Spam, Spam and More Spam*, 5 NO. 7 E-COM. L. REP. 5, 5 (2003).

[130] Burns & Wyden, *supra* note 123.

[131] Cisneros, *supra* note 19, at 11.

[132] Bender, *supra* note 38, at 27.

civil action to consumers to protect themselves against repeated infractions by marketers.[133]

In addition, the Act's preemption of state anti-Spam laws significantly retards progress towards a resolution of the problem.[134] One can speculate that such preemption was an attempt by Congress to make laws regulating Spam more uniform to relieve the burden of compliance from legitimate marketers.[135] However, since laws in some states were stronger in that they require affirmative consent by recipients *prior* to receiving Spam, the Act's preemption of these laws and replacement of their provisions with more narrowly defined requirements serves to only weaken consumer rights.[136]

Last, the Act's mere authorization, and not requirement, of the FTC to institute a Do-Not-Email Registry brings back memories of the plodding pace with which the Do-Not-Call Registry, originally authorized in the Telephone Consumer Protection Act of 1991 ("TCPA"),[137] was developed. The TCPA authorized the Federal Communications Commission to develop such a registry.[138] Ultimately, the establishment of the Do-Not-Call Registry took 12 years and another law *requiring* its formation by a completely different government agency.[139] Thus, based on this experience, an enabling law alone is not likely to ensure that a Do-Not-Email Registry would be established with the urgent pace that the problem of Spam demands.

[133] CAUCE Statement, *supra* note 128 (noting that "[a]t the FTC's Spam forum in May 2003, FTC officials and a representative of the National Association of Attorney's General stated clearly that neither the FTC nor state law enforcement agencies have the time, money, or resources, needed to engage in enough anti-Spam prosecutions to make a dent in the problem. Similarly, attorneys representing ISPs noted that they cannot afford to bring cases without the risk of spending more money than they'd ever recover from spammers.").

[134] *Id.*

[135] *Congress Preempts States, Particularly Cal., on Privacy and Spam,* WARREN'S WASH. INTERNET DAILY, Nov. 28, 2003, Vol. 4, Issue 229, *available at* 2003 WL 16118721.

[136] *See id.*; *see also supra* Part II.

[137] Telephone Fraud Consumer Protection Act of 1991, 47 U.S.C. § 227 (2002).

[138] *See generally* Rules and Regulations Implementing the Telephone Consumer Protection Act (TCPA) of 1991, 68 Fed. Reg. 16250 (April 3, 2003) (to be codified at 47 C.F.R. pt. 64).

[139] Ian Heath Gershengorn, *Telemarketing Restrictions and the First Amendment,* 20-SUM COMM. LAW. 3, 4 (2002).

V. A Blind Man in a Room Full of Deaf People

The initial impact of the legislation is not encouraging. Brightmail, a company specializing in filtering Spam, reported that the level of Spam in email traffic actually increased to 60% of total email traffic in January 2004 from 58% in December 2003.[140] Even worse, AOL reported a 10% increase in the Spam received from overseas in the same period, perhaps a bid by marketers to evade the provisions of the Act.[141] Marketers were openly relieved at the Act's preemption of what most of them perceived as draconian state laws, such as the California law requiring affirmative consent by recipients prior to sending any Spam.[142] Moreover, marketers admitted that, while they were planning to curtail their use of Spam to comply with the various state laws, they no longer felt that such moves were necessary.[143]

The long-term impact of the Act is also unclear. Some of the Act's benefits are derived from the ISPs' ability to develop and maintain filtering software that can detect and block Spam from reaching its recipients. Such software is necessarily dependent on the skill and resources of ISPs to continuously update it in an effort to counteract the virtually certain efforts by marketers to bypass this software. The Act also depends on the effective enforcement of its provisions in the faceless labyrinth of the Internet, a task that agencies like the FTC admit to be daunting.[144] In addition, eviscerating the states' ability to identify and address problems with Spam within their borders is unlikely to make state agencies enthusiastic participants in a federal cause that expressly disavows their views.[145]

Perhaps the clearest impact of the Act is that it will not stop

[140] Brightmail *Spam Statistics*, *supra* note 24.

[141] Anick Jesdanum, *New Tools Failing to Keep Spam in Control*, PASADENA STAR NEWS, Jan. 11, 2004, *available at* http://www.pasadenastartnews.com/stories (last visited Mar. 16, 2004).

[142] *See generally* CAL. BUS. & PROF. CODE § 17529.2 (West 2003); *see also* Jesdanum, *supra* note 129.

[143] Jesdanum, *supra* note 141.

[144] Kris Oser, *One Step Closer*, DIRECT, Nov. 1, 2003, at 1 (noting FTC's concern about enforceability of the Act because of the anonymous nature of Spam), *available at* 2003 WL 8203894.

[145] *See generally supra* Part III.E.

Spam.[146] As some critics of the Act contend, the Act practically legalizes the use of non-deceptive Spam.[147] Although reduction or elimination of deceptive Spam is certainly a worthwhile objective, this feat, by itself, represents only an element and not the core of the problem. Ultimately, Spam pits the privacy interests of consumers against the commercial interests of marketers. When such interests collide, the interest of consumers must outweigh the interests of marketers; a position that is squarely consistent with Congress' expressed view when it promulgated the Do-Not-Call Implementation Act of 2003 to regulate telephone access to consumers in the telemarketing industry.[148]

VI. Conclusion

The CAN-SPAM Act is Congress' first attempt to address the problem of Spam on a national level. The Act was designed to stop Spam that perpetrates fraud and uses fraudulent means in its dissemination.[149] Although the Act is certainly a step in the direction of controlling the problem of Spam, it weakens other legal tools that were promulgated for that very purpose. In particular, preempting state laws and replacing them with a mere prohibition on fraud gives marketers a virtual green light to send Spam to anyone they choose. Furthermore, Congress' failure to require the creation of a Do-Not-Email list in the Act ignores its own experience with the glacial pace by which the Do-Not-Call Registry was created for the telemarketing industry. Ultimately, the Act is unlikely to stem the growing tide of Spam and may actually help increase its rate of growth as marketers develop methods of circumventing filtering software. If Congress intended to give regulators a fly swatter, they ended up giving them one with holes so large that the commercial robotic pests of Phillip K. Dick's world could fly through them with relative ease.

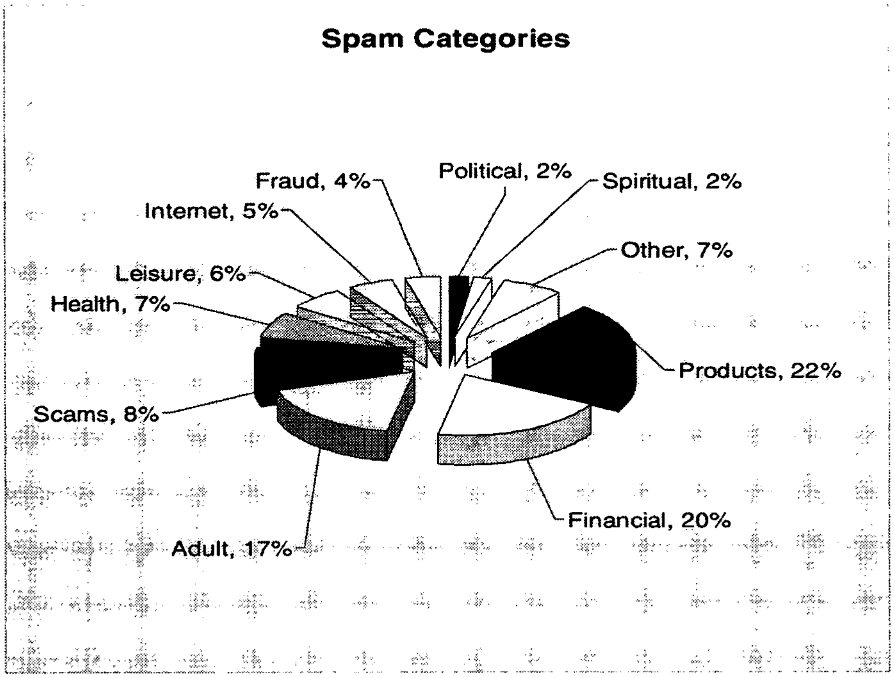
[146] CAUCE Statement, *supra* note 123.

[147] *See supra* Part III.A, Part IV.

[148] *See generally* Do-Not-Call Implementation Act of 2003, Pub. L. No. 108-10, 117 Stat. 557 (2003) (codified at 15 U.S.C. §§ 6101-6108).

[149] *See generally* Part III.A.

Appendix 1



Source: Brightmail, *Spam Statistics*, *available at* http://brightmail.com/spamstats.html (last visited Feb. 13, 2004).