Effectiveness and Enforcement of the CAN-SPAM Act

A Report To Congress

Federal Trade Commission
December 2005

Effectiveness and Enforcement of the CAN-SPAM Act: A Report to Congress

December 2005

Federal Trade Commission

Deborah Platt Majoras, Chairman
Thomas B. Leary, Commissioner
Pamela Jones Harbour, Commissioner
Jon Leibowitz, Commissioner

Table of Contents

Executive Summary

Section 10 of the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (the "CAN-SPAM Act," "CAN-SPAM," or "the Act"), 15 U.S.C. § 7709, requires the Federal Trade Commission ("FTC" or "Commission") to submit a report that "provides a detailed analysis of the effectiveness and enforcement of the provisions of this Act and the need (if any) for the Congress to modify such provisions." The Act further directs that the Commission provide analyses and recommendations regarding three specific areas of interest to Congress: (1) the extent to which technological and marketplace developments, including changes in the nature of the devices through which consumers access their electronic mail messages, may affect the practicality and effectiveness of the provisions of the Act; (2) how to address commercial electronic mail that originates in or is transmitted through or to facilities or computers in other nations, including initiatives or policy positions that the Federal Government could pursue through international negotiations, fora, organizations, or institutions; and (3) options for protecting consumers, including children, from the receipt and viewing of commercial electronic mail that is obscene or pornographic. This Report responds to the directive of Section 7709.

In preparing this Report, the Commission used several information-gathering techniques to inform its analyses of the effectiveness and enforcement of CAN-SPAM and the three specific areas of inquiry set forth by Congress. Of course, the Commission's direct enforcement experience under CAN-SPAM, as well as that of other entities empowered to enforce it, provided a broad basis for analyzing the issues addressed in the Report. In addition, FTC staff interviewed scores of individuals, including consumer group representatives, email marketers, Internet service providers ("ISPs"), law enforcers, and technologists. The Commission used its compulsory process powers to require the nine ISPs that collectively control over 60 percent of the market for consumer email accounts to provide detailed information concerning their experiences with spam. The Commission consulted with the federal and state agencies that have authority to enforce CAN-SPAM. The views of the general public about the effectiveness of the Act, provided in response to various CAN-SPAM rulemakings, were also considered. Commission staff also conducted a broad review of articles published about CAN-SPAM since its passage, and engaged in its own independent research. Finally,

the Commission retained the services of two preeminent computer scientists for their independent evaluations of the Act's effectiveness.

Based on its own enforcement and policy work, and on the information gleaned from the extensive research conducted to prepare this Report, the Commission believes that the Act has been effective in achieving two desired outcomes. First, the substantive provisions of the Act have mandated adoption of a number of commercial email "best practices" that many legitimate online marketers are now following. Second, the Act has provided law enforcement agencies and ISPs with an additional tool to use when bringing suit against spammers. The more than 50 cases brought to date by the FTC, the Department of Justice, state Attorneys General, and ISPs demonstrate CAN-SPAM's enforcement efficacy.

Some aspects of the spam problem, such as its international dimension, have not changed materially since enactment of CAN-SPAM. In many other ways, however, the email landscape has changed significantly, largely for the better. The volume of spam sent over the Internet has begun to level off, and, even more significantly, the amount reaching consumers' inboxes has decreased, due to enhanced anti-spam technologies. There has been a significant decrease in the number of spam messages containing sexually-explicit material. And, legitimate online marketers have complied with CAN-SPAM in large numbers. Concurrent with these developments, consumers have begun to report decreased annoyance with spam. In essence, these developments suggest that spam has not, as once feared, destroyed the promise of email.

However, some changes that have occurred since the passage of the Act are troubling. For example, there has been a shift toward the inclusion in spam messages of content that is increasingly malicious. Rather than merely advertising products and services, spam messages now sometimes include "malware" designed to harm the recipient. In addition to modifying the content of their messages, spammers have also sought to frustrate law enforcement by using increasingly complex multi-layered business arrangements. Moreover, spammers continue to hide their identities by providing false information to domain name registrars. The appreciable inaccuracy of data in domain name registrars' "Whois" databases and registrars' failure to take reasonable measures to verify the accuracy of information submitted by registrants continue to hamper law enforcement.

The Commission believes that three steps should be taken to further improve the effectiveness of CAN-SPAM. First, while no modification to CAN-SPAM is recommended, the Commission urges Congress to pass the US SAFE WEB Act, which would significantly improve the ability of the FTC to use CAN-SPAM to trace spammers and sellers whose operations are outside the borders of the United States. This, in conjunction with ongoing international enforcement and education efforts, will improve the ability of law enforcement to tackle the challenges posed by the international nature of spam.

Second, the Commission believes that continued education efforts are necessary to ensure that consumers are aware of the various ways in which they, and their children, can be protected from receipt and viewing of sexually-explicit spam. Tools available from ISPs and commercially available software, combined with the protections inherent in the Act, can significantly reduce the chance that consumers, especially children, will be assaulted by pornography distributed via spam.

Third, the Commission urges the continued improvement in anti-spam technology and, in particular, domain-level authentication. This technology, paired with reputation and accreditation systems, holds the greatest promise in ensuring that spammers will not be able to continue to operate anonymously. The Commission intends to fulfill its promise to work to spur industry efforts to create and deploy authentication technologies broadly.

I. Introduction and Overview

The CAN-SPAM Act has been in effect since January 1, 2004.[1] Since that time, the Commission has brought 20 cases alleging violations of the Act, and the Department of Justice ("DOJ"), state Attorneys General, and Internet service providers ("ISPs"),[2] have brought more than 30 additional actions in federal court to enforce the Act. This enforcement experience provides the basis for the Commission to fulfil the mandate, set forth in Section 10 of the Act, 15 U.S.C. § 7709, that it prepare and submit to the Congress, not later than December 16, 2005, a report that both "provides a detailed analysis of the effectiveness and enforcement of the provisions of this Act and the need (if any) for the Congress to modify such provisions,"[3] and that covers specified topics of particular interest to the Congress. Accordingly, the Commission submits this Report.

The detailed analyses of the effectiveness and enforcement of the Act's substantive provisions, as required by § 7709(a), are included in Appendix 1 of this Report. In general, such analyses demonstrate the Act's effectiveness. The criminal provisions of CAN-SPAM have proven useful to DOJ in prosecuting spammers. The civil provisions of the Act have also proven effective by two measures: by establishing or codifying an email "best practices" guide for legitimate marketers – most of whom have followed the Act's directives – and by enhancing the effectiveness of law enforcement against spammers who flout the law. In particular, the Commission finds that CAN-SPAM's opt-out provisions and prohibitions on falsifying header information have been useful tools for those

---

1. In general, CAN-SPAM sets forth a series of requirements and prohibitions relating to "commercial" and "transactional or relationship" email messages, as defined by the Act. It creates five new federal crimes, and contains numerous civil provisions which, among other things, require: (1) accurate email transmission information, (2) identification of the email sender's physical location, and (3) provision of an opportunity to opt out of receiving future mailings. Under CAN-SPAM, many federal agencies, including the FTC and the Department of Justice, certain state law enforcement authorities, and Internet service providers, may file civil suits to halt unlawful spammers. The Act also conferred rulemaking authority on the FTC and the Federal Communications Commission.

2. For this Report, the Commission uses the popular term "ISP" when referring to an Internet service provider, rather than the term used in the Act, a "provider of Internet access service," except in Appendix 1.E.3, discussing § 7707(c) (non-preemption of such entities' email transmission policies). The Act's term is derived from the definition of "Internet access service" in 15 U.S.C. § 7702(11), which cross-references 47 U.S.C. § 231(e)(4).

3. This Report discusses numerous federal statutes, including the CAN-SPAM Act, 15 U.S.C. §§ 7701 *et seq.,* the FTC Act, 15 U.S.C. §§ 41 *et seq.,* and certain provisions of federal criminal law relating to computers, notably 18 U.S.C. § 1037. To assist the reader, we cite uniformly to the U.S. Code throughout the Report.

enforcing the Act; the remaining civil provisions have also contributed to the overall effectiveness of CAN-SPAM.

Section 7709(b) specifies the particular areas of interest to Congress that the Report must cover, namely:

(1) an analysis of the extent to which technological and marketplace developments, including changes in the nature of the devices through which consumers access their electronic mail messages, may affect the practicality and effectiveness of the provisions of this Act;

(2) analysis and recommendations concerning how to address commercial electronic mail that originates in or is transmitted through or to facilities or computers in other nations, including initiatives or policy positions that the Federal Government could pursue through international negotiations, fora, organizations, or institutions; and

(3) analysis and recommendations concerning options for protecting consumers, including children, from the receipt and viewing of commercial electronic mail that is obscene or pornographic.

Section III of the Report provides the Commission's specific analyses of these three issues, but first, section II of the Report briefly describes the information-gathering methods used by the Commission's staff in preparing this Report. Finally, section IV sets forth an overview of the Commission's findings and recommendations. The Report also includes several appendices. As noted above, Appendix 1 examines the effectiveness and enforcement of each substantive provision of the Act. Appendix 2 provides a list of persons interviewed in preparation for this Report. Appendix 3 contains Part III of the Commission's National Do Not Email Registry Report, which explains in detail how email communication takes place. Appendix 4 summarizes the provisions of the US SAFE WEB Act. Appendices 5 through 7 are tables of CAN-SPAM cases brought by the FTC, ISPs, and states, respectively.

II. Information-Gathering Methods

In preparing this Report, the Commission's staff used a number of methods to obtain information from scores of individuals and organizations. First, during July 2005, FTC staff conducted interviews with 98 individuals representing 65 organizations, including consumer groups, email marketers, ISPs, law enforcers, and technologists. These interviews, which were transcribed by a court reporter, enabled the Commission to draw upon the skills and backgrounds of a wide variety of organizations.[4]

Second, using its compulsory process powers under Section 6(b) of the FTC Act, 15 U.S.C. § 46(b), the Commission required nine ISPs that collectively control over 60 percent of the market for consumer email accounts to provide detailed information concerning their experiences with spam.[5] The 6(b) Orders asked for data concerning the volume and types of spam hitting these companies' mail servers and being delivered to their subscribers' inboxes. The 6(b) Orders also required the ISPs to provide detailed information regarding their anti-spam technologies and enforcement efforts, as well as information relevant to the three specific areas of interest that Congress set forth in § 7709(b) of the Act.

Third, as required by the Act, the Commission consulted with the federal and state agencies that have authority to enforce CAN-SPAM. These agencies are: DOJ; the Federal Communications Commission; the state Attorneys General; the Federal Deposit Insurance Corporation; the Office of the Comptroller of the Currency; the Federal Reserve Board; the Office of Thrift Supervision; the National Credit Union Administration; the Securities and Exchange Commission; applicable state insurance authorities; the Department of Transportation; the Department of Agriculture; and the Farm Credit Administration.

---

4. A complete list of interviewees is attached to this Report as Appendix 2. Citations to these transcripts identify the organization, representative from the organization, and page number of the transcript. For instance, the citation "Oregon: St Sauver, 14" refers to a statement made by University of Oregon employee Joe St Sauver on page 14 of the transcript. The Commission has posted the transcripts online at http://www.ftc.gov/reports/canspam05/transcripts.htm.

5. The Commission issued 6(b) Orders to: America Online, Inc.; BellSouth Corp.; Cox Communications, Inc.; EarthLink, Inc.; Microsoft Corp.; Road Runner HoldCo LLC; SBC Internet Services, Inc.; United Online, Inc.; and Verizon Internet Services, Inc. The Commission, in preparation for its National Do Not Email Registry Report to Congress, previously issued 6(b) Orders to America Online, Inc.; Comcast Corporation; EarthLink, Inc.; Microsoft Corp.; MCI, Inc.; United Online, Inc.; and Yahoo! Inc. To ensure that their anti-spam techniques do not become known to spammers, the ISPs have requested confidential treatment of their 6(b) Order responses. When possible, the Commission has aggregated data from these responses. When the Commission relies on a 6(b) Order response from a particular ISP, this Report does not identify the particular ISP.

Fourth, the Commission solicited comments about the effectiveness of the Act from the general public in a March 11, 2004, Advance Notice of Proposed Rulemaking concerning CAN-SPAM Act rules (the "ANPR"). By the close of the comment period, the Commission received over 300 comments regarding the effectiveness and enforcement of CAN-SPAM.[6]

Fifth, Commission staff conducted a broad review of articles published about CAN-SPAM and studies of spam trends conducted since the Act's passage. This literature review included articles in the general press and technology publications, primary and secondary legal sources, and various online sources.

Sixth, FTC staff engaged in its own independent research. For example, the Commission staff studied 100 top online merchants' compliance with CAN-SPAM's opt-out provisions.[7] The Commission staff also studied the prevalence of email address harvesting and the effectiveness of two major ISPs' spam filters at blocking spam sent to harvested email addresses.[8]

Finally, to ensure that the Commission's assessment of the effectiveness of the Act was well-grounded, the Commission retained the services of two preeminent computer scientists: Matthew Bishop, Ph.D., Professor of Computer Science at the University of California ("UC") Davis and Co-director of the UC Davis Computer Security Laboratory; and Paul Judge, Ph.D., Chief Technology

---

6. Because the ANPR required comments to be filed by April 20, 2004, the comments reflect the commenters' views concerning the effectiveness of the Act just four months after CAN-SPAM was enacted. The Commission issued two subsequent Notices of Proposed Rulemaking ("NPRMs") pursuant to CAN-SPAM. In the first, the Primary Purpose rulemaking, the Commission announced a standard for determining whether the primary purpose of an email is commercial. In the second, the Discretionary rulemaking, the Commission is considering modifying the definitions of "sender" and "valid physical postal address;" shortening the time frame for honoring a recipient's opt-out request; limiting the information collected when a recipient submits an opt-out request; and adding a definition of "person." Comments received in response to these NPRMs address some areas covered by this Report, including the effectiveness of the Act, as well as marketplace developments, international transmission of email, and protecting consumers from pornographic email. In all, 13,890 comments were received in these CAN-SPAM rulemakings. Throughout this Report, citations to comments received in the Discretionary rulemaking identify the commenter's name, the term "Comment" followed by "D," and the page of the comment being referenced. For instance, the citation "LashBack – Comment D, 2" refers to page 2 of the comment submitted by LashBack LLC in the Discretionary rulemaking.

7. *See* Top Etailers' Compliance with CAN-SPAM's Opt-Out Provisions, a report by the FTC's Division of Marketing Practices, at 3 (July 2005), available at http://www.ftc.gov/reports/optout05/050801optoutetailersrpt.pdf.

8. *See* Email Address Harvesting and the Effectiveness of Anti-spam Filters, a report by the FTC's Division of Marketing Practices, at 3 (Nov. 2005), available at http://www.ftc.gov/opa/2005/11/spamharvest.pdf.

Officer of CipherTrust, Inc., an email solution provider.[9] The Commission retained these experts because of their extensive background in analyzing the existence and effectiveness of anti-spam technologies and their knowledge of marketplace changes since the passage of CAN-SPAM. Their views represent independent appraisals of the effectiveness and enforcement of the Act.[10]

III. Analyses and Recommendations Regarding Areas of Interest to Congress

This section provides analyses of the three specific issues that Congress directed the Commission to include in this Report:

- the extent to which technological and marketplace developments may affect the practicality and effectiveness of the provisions of the CAN-SPAM Act;
- commercial email that originates in or is transmitted through other nations; and
- protecting consumers, including children, from the receipt and viewing of obscene or pornographic spam.

---

9. The Commission has posted reports prepared by these two computer scientists online at http://www.ftc.gov/reports/canspam05/expertrpts.htm. Citations to these expert reports identify the name of the expert and the page of the report. For instance, the citation "Bishop Report, 2" refers to a statement appearing on page 2 of the report prepared by Matthew Bishop, Ph.D. Dr. Bishop served as a consultant to the FTC in the preparation of the Do Not Email Registry Report, and Dr. Judge was a participant in the FTC's Spam Forum, held in 2003.

10. The Commission's considerable prior experience with the issue of spam, including its enforcement experience, its three-day Spam Forum held in the Spring of 2003, and the two-day Email Authentication Summit sponsored by the FTC and the Commerce Department's National Institute of Standards and Technology in the Fall of 2004, also guides its analyses of the issues discussed in this Report. The Commission gained further expertise in the technological, legal, and economic issues concerning spam through preparation of three prior reports to Congress pursuant to CAN-SPAM, each of which is available online: (1) National Do Not Email Registry Report (June 2004), http://www.ftc.gov/reports/dneregistry/report.pdf; (2) Informant Reward System Report (Sept. 2004), http://www.ftc.gov/reports/rewardsys/040916rewardsysrpt.pdf; and (3) Subject Line Labeling Report (June 2005), http://www.ftc.gov/reports/canspam05/050616canspamrpt.pdf.

A. Technological and Marketplace Developments in Email since the Enactment of CAN-SPAM

The Commission has identified five technological and marketplace developments that are relevant to the practicality and effectiveness of CAN-SPAM. These include:

- indications that the volume of spam is declining, along with the level of consumer frustration resulting from spam;
- improvements in the effectiveness of anti-spam technologies and broader deployment of such tools;
- evolving types of spam and spamming techniques;
- the development of effective authentication strategies; and
- the increased use of mobile devices to access email.

The following sections discuss each of these topics in detail.

1. Since Enactment of CAN-SPAM, Spam Volume Has Begun to Decline as Has Consumer Frustration

When CAN-SPAM was enacted in 2003, the flood of spam reaching consumers' inboxes seemed like an insurmountable problem. There was widespread concern that the onslaught of spam was destabilizing the email system and posing a serious threat to the burgeoning Internet economy.[11] The Commission shared this view. Indeed, in Congressional testimony delivered in May 2003, the Commission noted that the deceptive nature of the vast majority of spam, the network disruptions that spam may cause, and the use of spam as a vehicle for spreading viruses together posed a serious threat to consumers' confidence in the Internet as a medium for electronic commerce.[12]

---

11. *See, e.g.,* 15 U.S.C. § 7701(a)(2) (In enacting CAN-SPAM, Congress found that "[t]he convenience and efficiency of electronic mail are threatened by the extremely rapid growth in the volume of unsolicited commercial electronic mail."); Senate Comm. on Commerce, Science and Transp., Rep. on the CAN-SPAM Act of 2003, S. Rep. No. 108-102, at 6 (2003) ("Left unchecked at its present rate of increase, spam may soon undermine the usefulness and efficiency of e-mail as a communications tool. Massive volumes of spam can clog a computer network, slowing Internet service for those who share that network.").

12. *Unsolicited Commercial E-Mail: Hearing Before the Senate Comm. on Commerce, Science and Transp.,* 108th Cong., 1st Sess. (2003) (testimony of then Commissioners Orson Swindle and Mozelle Thompson on behalf of the FTC). The Commission's testimony was informed by, among other things, a consensus view that emerged among participants in the Commission's Spam Forum in the Spring of 2003: the volume of email had reached a "tipping point," requiring some action to avert deep erosion of public confidence in email that could hinder, or even destroy it, as a tool for communication and online commerce. Transcripts from the FTC's Spam Forum are available at http://www.ftc.gov/bcp/workshops/spam/index.html.

Today, email continues to thrive notwithstanding the dire warnings prior to the enactment of CAN-SPAM. According to DoubleClick, a digital marketing and advertising concern, 90 percent of those surveyed in 2005 reported using email multiple times per day; 44 percent of those surveyed described their usage as "constant."[13] DoubleClick reports that this represents an increase in email usage over each of the previous four years, indicating that email remains a viable means of communication.[14]

One particularly significant development since the enactment of CAN-SPAM is that the volume of spam has begun to decrease.[15] MX Logic, an email filtering company, reported that during the first eight months of 2005, spam accounted for 67 percent of email passing through its system, a nine percent decrease from the same period one year earlier.[16] Some ISPs report an even more dramatic decline. For example, America Online ("AOL") reported that its members received 75 percent less spam in 2004 than in 2003.[17] Studies from other countries similarly report a decrease in the amount of spam reaching consumers' inboxes.[18] As the Executive Director of the Institute for Spam and Internet Public Policy succinctly stated, "the average inbox doesn't have that much spam anymore."[19]

---

13. DoubleClick 2005 Consumer Email Study, PowerPoint presentation, June 27, 2005 (on file with the FTC). In its "2005 Broken Link Study," Silverpop Systems, Inc., an email marketing concern, reported that 71 percent of companies it studied regularly conducted email marketing campaigns, up from 30 percent in 2002. *See* http://www.clickz.com/stats/sectors/email/article.php/3558196.

14. In a 2005 presentation, DoubleClick compared its 2005 findings with those in its four previous annual surveys. From 2001 to 2004, the percentage of those reporting email usage more than once a day ranged between 72 and 88 percent. DoubleClick 2005 Consumer Email Study, PowerPoint presentation, June 27, 2005 (on file with the FTC).

15. The sources relied upon for this assertion are cited below. *See infra* notes 16-19 and accompanying text. The methodologies used in these several studies to measure the volume of spam vary. Therefore, this Report avoids comparisons of data from different sources. The Report only sets out comparative data analyses that use year-over-year figures from single sources.

16. Press release, *MX Logic Reports Spam Accounts for 67 Percent of All Emails in 2005* (Sept. 22, 2005), available at http://www.mxlogic.com/news_events/press_releases/09_22_05_SpamStats.html. *See also* MessageLabs, Spam Intercepts: Average Global Ratio of Spam in Email, available at http://www.messagelabs.com/publishedcontent/publish/threat_watch_dotcom_en/threat_statistics/spam_intercepts/DA_114633.chp.html (chart showing that, while spam rates rose from the time of the enactment of CAN-SPAM until July 2004, they have been on the decline since, nearly reaching the levels they were at when the Act was passed – 65 percent in July 2005 versus 63 percent in late December 2003). According to MX Logic, the decrease "could indicate that improved email defense technology and high-profile prosecutions of spammers might be having some effect."

17. *See* press release, *America Online Announces Breakthroughs in Fight Against Spam* (Dec. 27, 2004), available at http://media.timewarner.com/media/newmedia/cb_press_view.cfm?release_num=55254331.

18. *See infra*, section III.B.3.b (discussing the results of studies in Canada and Finland that show a decrease in the amount of spam received by consumers in those countries, and decreasing annoyance with spam).

19. Crayton Harrison, *It Cost Millions, But Users Now Protected From Most E-mail Spam,* Aug. 23, 2005 (*quoting* Anne Mitchell), available at http://www.menafn.com/qn_news_story.asp?StoryId=CqWQFqeicv1jllvnqqu0TqKLAueXvuW.

Moreover, the burden that spam imposes on the Internet's infrastructure is actually less than that resulting from other email messages. According to VeriSign, the manager of the .com and .net domains, during the three-month period from July 1 to September 30, 2004, spam represented 80 percent of traffic by volume, but constituted only 21 percent of email bandwidth because the average size of a spam message was 3K bytes, while the average size of a legitimate message was 40K bytes.[20] Thus, while spam clearly creates costs for operators of email servers, the volume of spam does not appear to be destabilizing the email system.

At the same time, consumers apparently have grown more tolerant of spam, having come to view it more as an acceptable nuisance rather than a cause for abandoning email. An April 2005 report by the Pew Internet & American Life Project ("Pew") found that fewer consumers were annoyed with spam than the previous year.[21] From February 2004, just after the Act became effective, to January 2005, the percentage of consumers annoyed with spam dropped from 77 percent to 67 percent. This decrease forecasts a positive trend that may be attributable to the reduction in spam entering consumers' inboxes.[22]

Another marketplace development is that CAN-SPAM has established a framework for lawful commercial email, and legitimate marketers are largely complying with it, as evidenced by a July 2005 FTC staff study of CAN-SPAM compliance by 100 top online marketers or "etailers" with the opt-out provisions of the Act.[23] FTC staff found that all of the studied companies provided recipients with both notice of their right to choose not to receive future commercial emails and with a mechanism to enable consumers to exercise that right. FTC staff also

---

20. VeriSign, Internet Security Intelligence Briefing, Nov. 2004, v. 2, issue 2, at 5-6, available at http://www.verisign.com/static/017574.pdf. Of course, bandwidth is not the only cost imposed by spam. *See infra* notes 55-56.

21. Deborah Fallows, *CAN-SPAM a Year Later*, Pew Data Memo, April 2005, available at http://www.pewinternet.org/pdfs/PIP_Spam_Ap05.pdf. According to Pew, "fewer email users now say that spam is undermining their trust in email, eroding their email use, or making life online unpleasant or annoying. These findings suggest that at least for now, the worst case scenario – that spam will seriously degrade or even destroy email – is not happening, and that users are settling into a level of discomfort with spam that is tolerable to them."

22. The Pew study did not link the reported decline in hostility toward spam to any particular development since the enactment of the Act. Technological improvements during the past two years, particularly in email filtering technology, have resulted in consumers receiving less spam in their inboxes.

23. *See* Top Etailers' Compliance with CAN-SPAM's Opt-Out Provisions, a report by the FTC's Division of Marketing Practices, at 3 (July 2005), available at http://www.ftc.gov/reports/optout05/050801optoutetailersrpt.pdf.

found that 89 percent of the companies honored opt-out requests.[24] These findings suggest that consumers' opt-out preferences are being honored by top etailers, resulting in the receipt of less unwanted commercial email.

2. Anti-Spam Technologies Have Become More Effective and More Broadly Deployed

As explained in Appendix 3, there can be five types of participants in the transmission of an email message: senders, senders' mail servers (the "senders' ISPs"), intermediate mail servers, recipients' mail servers (the "recipients' ISPs"), and recipients. During the last two years, senders' ISPs, intermediate mail servers, recipients' ISPs, and recipients all have instituted improved anti-spam technologies.

Responsible senders' ISPs have instituted anti-spam measures to limit the amount of spam being sent from their networks. These practices are particularly effective in thwarting spammers' use of "zombie drones," computers on which email server or proxy software has been downloaded which, without the knowledge of the computer owner, causes the computer to spew out spam or to serve as a relay or proxy for spam. As discussed further in section III.A.3, zombies have been spammers' preferred method of delivering spam, with estimates that between 60 and 80 percent of all spam is sent via these compromised machines.[25] As described below, however, techniques for thwarting zombie drones have been developed.

In June 2004, the Anti-Spam Technical Alliance ("ASTA"), a group comprised of several major technology companies allied to develop and promote practices that limit spam, published a list of best practices for senders' ISPs that includes blocking or limiting access to port 25, and rate-limiting outbound email traffic.[26] Port 25 is the communications channel through which Internet mail servers usually transmit email.[27] In the usual course, email sent from an individual's computer would be transmitted through that individual's ISP's mail

---

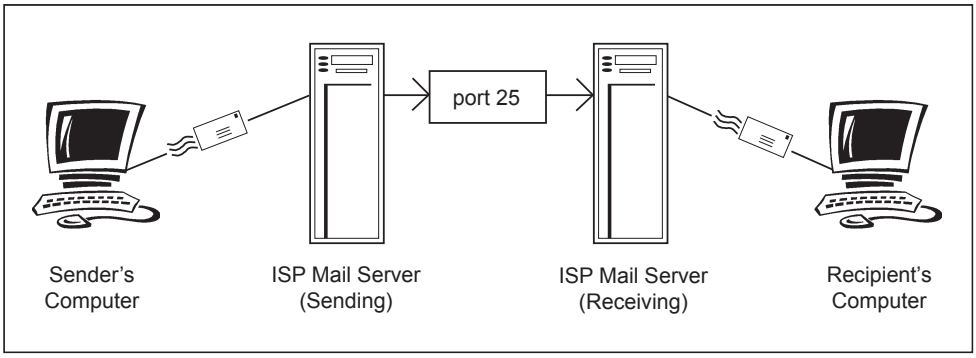
24. *Id.*

25. *See, e.g.,* Confidential 6(b) response (75 percent of the spam received by one ISP in 2004 originated from zombies); FTC, A CAN-SPAM Informant Reward System: A Report to Congress at 10-13 (Sept. 2004) (including estimates that between 60 and 80 percent of all spam is sent via zombies), available at http://www.ftc.gov/reports/rewardsys/040916rewardsysrpt.pdf.

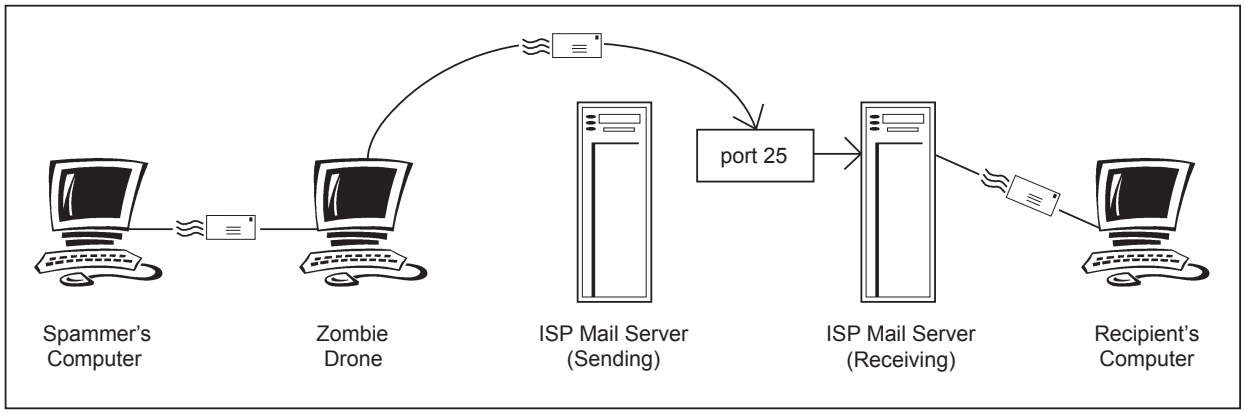
26. *See* ASTA, Anti-Spam Technical Alliance Technology and Policy Proposal, v. 1.0, June 22, 2004. A complete list of ASTA's best practices is available at http://docs.yahoo.com/docs/pr/pdf/asta_soi.pdf.

27. *See* Judge Report, 2; Bishop Report, 22.

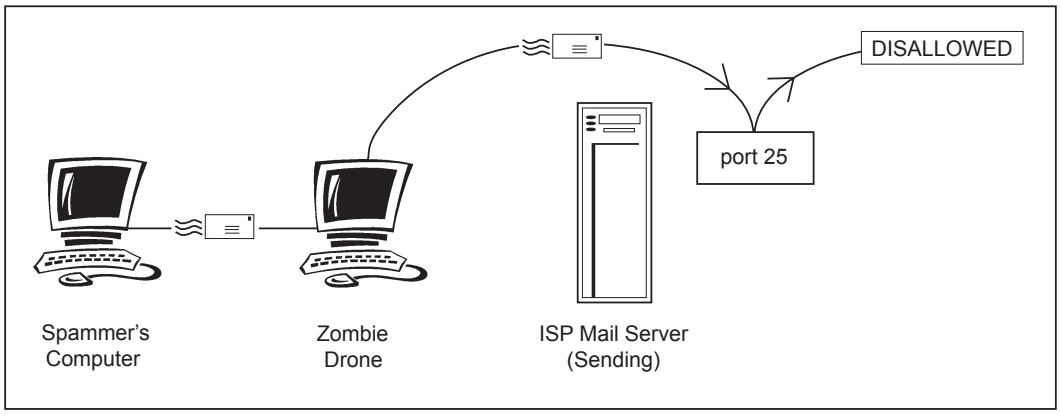
Typical Process for Sending Email



How Zombie Drones Circumvent Scrutiny



Email Process with Blocking of port 25



server, which would route the message through port 25 to the recipient's ISP.[28] In order to avoid the scrutiny to which some senders' ISPs subject outgoing mail sent through their mail server, some zombie drones are configured to act as mail servers in their own right, and are programmed to send email directly through the sender's ISP's port 25 connection without going through the sender's ISP's mail server.[29] Many ISPs have now effectively foreclosed the use of port 25 by zombie drones, forcing spammers to attempt to send spam directly through zombie drones' ISPs' outgoing mail server. By blocking or limiting port 25 access, senders' ISPs can ensure that anti-spam technologies are applied to all outgoing email coming from computers on their networks.

Because so many ISPs have effectively foreclosed the use of port 25 by zombie drones, spammers now attempt to send spam directly through the zombie drones' ISPs' outgoing mail server. One technique developed by ISPs to thwart the use of their networks by spammers is rate-limiting, whereby the amount of outgoing email that a subscriber can send is limited.[30] Alone or in conjunction with blocking or limiting access to port 25,[31] limiting the number of messages that a subscriber can send makes high-volume spamming impossible. Adoption of both of these practices has been shown to be highly effective in combating spam sent via zombie drones. One ISP reported that by implementing rate-limiting and curtailing email sent through port 25, the percentage of spam sent via zombie drones from its network in 2004 approached zero.[32] While closure of port 25 and rate-limiting are effective, there are thousands of ISPs in the world.[33] Unless all senders' ISPs institute such measures, spammers likely will continue to use zombie drones.

Recipients' ISPs also have taken steps to ensure that less spam enters consumers' inboxes. In their confidential responses to the 6(b) Orders issued

---

28. *See* Bishop Report, 13-14.

29. Senders' ISPs routinely monitor outgoing email passing through their mail servers to screen for spam. Confidential 6(b) responses.

30. *See* Judge Report, 12-13; Bishop Report, 22.

31. *See supra* note 26, at 11-12 ("[B]locking port 25 can be problematic for customers who need to run their own mail server or communicate with a mail server on a remote network to submit e-mail (such as a web hosting company or a hosted domain's mail server)."). To limit inconvenience, ASTA's guidelines suggest routing such customers' mail through alternative ports and using rate limiting to block high volume sending.

32. Confidential 6(b) response.

33. U.S. CIA, The World Factbook, available at http://www.cia.gov/cia/publications/factbook/print/xx.html (latest available figures estimate that there were 10,350 ISPs worldwide in 2000).

by the Commission, nine ISPs, which collectively control approximately 60 percent of the market share for personal email service, explained that they actively use filtering, spam blocking, and other technologies to limit the amount of spam reaching their subscribers' inboxes.[34] During the past two years, those technologies have evolved and become substantially more sophisticated and accurate.[35] According to some ISPs interviewed in preparation for this Report, more than 80 percent of email traffic hitting ISPs' servers is blocked at the point of attempted connection to the ISP's network because it can be identified clearly as spam.[36] There are several reasons why an ISP would choose to block certain email. For example, an ISP may block a message because it comes from an IP address that the ISP has determined to be an open relay or open proxy used by spammers, or because an IP address or domain is associated with the sending of high volumes of spam. ISPs then filter the remaining 20 percent once it enters their networks, but before it is delivered to subscribers' inboxes, using a variety of techniques to separate spam from legitimate email messages.[37] In an effort to reduce the incidence of "false positives,"[38] some ISPs now have created separate "junk mail" folders into which questionable email messages can be sent. Recipients can review the email in their junk mail folders to determine if it is spam or not. Using junk mail folders helps to reduce over-filtering while still limiting the amount of spam that is delivered to subscribers' inboxes.[39]

In addition, recipients' ISPs have instituted a number of other anti-spam technologies. One such technique[40] used by some ISPs, including AOL, involves limiting the number of messages the ISP will allow to come into their system from a particular IP address, a procedure known as Second Received Line ("SRL")

---

34. *See also* Digital Impact: Jalli, 20-25.

35. Confidential 6(b) responses; Time Warner: Jacobsen, 18; AT&T: Gasster, 18; AT&T: Barszcz, 19-20; Aristotle: Bowles, 20; and Digital Impact: Jalli, 20-25.

36. *See* AT&T: Barszcz, 19-20; Aristotle: Bowles, 20 (noting that email from IP addresses that almost exclusively send spam are blocked, and that the remainder of email messages are subjected to filtering). According to AT&T's representative, the messages being blocked come from IP addresses recognized as belonging to, or having been exploited by, spammers. AT&T: Barszcz, 19.

37. Filters analyze the content of email messages – including the header information – looking for spam characteristics. Messages can be scored based on this analysis, and compared to a threshold level that determines whether the message is likely spam. This enables recipients' ISPs to decide whether particular messages should be delivered to subscribers' inboxes, placed in a "spam" folder, or simply deleted. Confidential 6(b) responses.

38. *See infra* note 56 (concerning false positives).

39. Several ISPs offer this type of service, including AOL, United Online, and Microsoft.

40. A variety of other techniques were outlined by ISPs in their Confidential 6(b) responses.

rate limiting.[41] The first "received line" in an email header identifies the sender's ISP's outgoing mail server. The second "received line" identifies the specific IP address from which the email was sent.[42] Where a given sender's ISP's outgoing mail server is considered trustworthy by other ISPs, SRL rate limiting analyzes the volume of email emanating from the second "received line" address at that mail server, rather than the volume of email emanating from the mail server itself. This enables recipients' ISPs to be more targeted and more accurate in their spam-blocking efforts.[43]

The Commission staff's independent research confirms that recipients' ISPs can now effectively block or filter the vast majority of spam messages. In July and August of 2005, FTC staff studied the effectiveness of spam filtering by ISPs. The study showed that two free web-based ISPs' anti-spam filters effectively blocked almost all spam sent to email addresses that FTC staff had posted on the Internet. One ISP blocked 86 percent of spam messages, while the other ISP blocked 95 percent of spam messages.[44]

Intermediate mail servers, which are often used in the transmission of email messages, have also implemented anti-spam measures.[45] When these servers are "open," or unsecured, they can be used as a means of distributing spam.[46] A secured email server checks to make sure that the sender's computer and email account are authorized to use that server. Only if that authorization is successful is email sent. However, an unsecured server will forward mail even if the senders are not authorized users of the email server. As a result of education efforts by the FTC and other government agencies worldwide, as well as efforts by ISPs to crack down on open proxies and relays, intermediate mail servers are more likely to be secured today than they were at the time CAN-SPAM was enacted.[47]

---

41. *See* Larry Seltzer, ISPs Need to Keep Moving Against Spam, available at http://www.eweek.com/article2/0,1759,1759508,00.asp.

42. *See* Appendix 3 (containing a sample header).

43. *See supra* note 41.

44. *See* Email Address Harvesting and the Effectiveness of Anti-spam Filters, a report by the FTC's Division of Marketing Practices, at 3 (Nov. 2005), available at http://www.ftc.gov/opa/2005/11/spamharvest.pdf.

45. Appendix 3 explains that while email can be transmitted in a relatively simple four-computer model (involving only a sender's computer, a sender's ISP, a recipient's ISP, and a recipient's computer), it is commonly the case that messages are routed through intermediate servers "that narrow the destination down to the proper receiving server." *See* Appendix 3, at 8.

46. *See* Appendix 3, at 9 for details regarding open relays and "secure" servers.

47. *See* http://www.ftc.gov/bcp/conline/edcams/spam/secureyourserver/index.htm. *See also infra,* section III.B.2.c (for discussion of the FTC's Operation "Secure Your Server").

Individual recipients also play a key role in implementing anti-spam technologies and solutions. The FTC's consumer education efforts over the past several years have emphasized that recipients can reduce the amount of spam they receive by taking simple steps, such as safeguarding email addresses, either by refraining from public dissemination or by using disposable email addresses.[48] To help consumers easily locate other useful tips about online safety issues, including spam avoidance techniques, the FTC partnered with private industry, other government agencies, and agencies all over the world to launch a new interactive consumer education campaign called "OnGuard Online" in September 2005. From the OnGuard Online website (www.onguardonline.gov), consumers can access up-to-date information about evolving spam scams and anti-spam technologies, as well as access all the FTC's past publications on eliminating unwanted spam.

Other steps can be taken by consumers in partnership with their ISP. An example is the use of the "report spam" features that several ISPs now provide, which allow recipients to become active participants in improving the effectiveness of spam filters.[49] Using another feature available from some ISPs, recipients can create a "whitelist" of those senders from whom they are willing to accept email. Messages from senders not on the recipient's whitelist are subject to challenge-response systems that require the sender to answer a question in order to have its message delivered.[50] Recipients can also have their ISPs block email of certain senders, or even certain domains, accepting messages only from approved senders or domains.[51] As noted in the Consumer Reports 2005 State of the Net survey, published in September 2005, "the most immediate help for consumers [in easing the spam burden] is from some leading Internet service providers . . . ."[52]

---

48. These and other tips for reducing spam are included in the FTC publication "Putting a Lid on Deceptive Spam," July 2002, available at http://www.ftc.gov/bcp/conline/features/spam.pdf.

49. *See, e.g.,* http://help.yahoo.com/help/us/mail/spam/spam-20.html (Yahoo! allows users to report spam with the click of a button). *See also* Confidential 6(b) responses.

50. *See, e.g.,* http://www.earthlink.net/software/free/spamblocker/.

51. Confidential 6(b) responses.

52. *See* Consumer Reports 2005 State of the Net Survey, "Help on the Way?," Sept. 2005, Consumer Reports; available at http://www.consumerreports.org/main/content/display.jsp?FOLDER%3C%3Efolder_id=760035&ASSORTMENT%3C%3East_id=333133&bmUID=1128523344058 (recommending that consumers should consider choosing an ISP based in part on its provision of anti-spam and other security features).

Many costs associated with technological advances to block spam are borne by consumers and businesses. For example, Consumers Union estimates that consumers spent more than $2.6 billion over the past two years on software to protect their computers, including money spent on filtering software to block spam.[53] Businesses reportedly spent $300 million on anti-spam products in 2003,[54] a figure that had reportedly risen to nearly $1 billion by 2004.[55] Legitimate email marketers incur additional costs in the form of lost business and customer dissatisfaction, which results when their messages are erroneously stopped by ISPs' anti-spam technologies.[56]

3. Evolving Spamming Techniques and Types of Spam

Spammers have used and continue to use various methods to disguise the origin of their messages, thus eluding adverse action by ISPs or law enforcement authorities, including: spoofing, open relays, open proxies, and zombie drones.[57] In addition, spammers continue to hide their identities by providing false information to domain name registrars.[58] The appreciable inaccuracy of data in domain name registrars' "Whois" databases and registrars' failure to verify the accuracy of information submitted by registrants continue to hamstring law enforcement.

In addition, since the enactment of CAN-SPAM, spammers have begun changing their tactics, both in the ways they run their operations and in the types of messages they send. Spammers have embraced two strategies in particular to

---

53. *Net Threat Rising,* ConsumerReports.org, available at http://www.consumerreports.org/cro/electronics-computers/laptop-desktop-computers/protect-yourself-online-905/overview.htm.

54. Crayton Harrison, *It Cost Millions, But Users Now Protected From Most E-mail Spam,* Aug. 23, 2005, available at http://www.menafn.com/qn_news_story.asp?StoryId=CqWQFqeicv1jllvnqqu0TqKLAueXvuW.

55. Jon Swartz, *Anti-Spam Industry Consolidating,* USA Today, July 20, 2004 ("Spending on anti-spam products and services will swell to nearly $1 billion this year, up 50% from 2003, says market researcher The Radicati Group."), available at http://www.usatoday.com/money/industries/technology/2004-07-20-spam_x.htm.

56. The extent of harm caused by such "false positives," *i.e.,* mistakes made by ISPs' anti-spam technologies, is difficult to calculate. Lyris Technologies, a developer of email marketing software and services that track false positive rates, reported a significant decrease in inappropriate spam filtering during the first six months of 2005. Lyris found that "inappropriate spam filtering among U.S. domains fell from an average of 3.3 percent in the [first quarter of 2005] to an average of 1.4 percent in [the second quarter of 2005]. This may be reflective of an overall trend toward more accurate and sophisticated spam filtering by ISPs and [email service providers]." "Lyris Q2 2005 ISP Deliverability Report Card," available at http://www.lyris.com/email-marketing-resources/reports/deliverability_report_Q22005.pdf.

57. For an explanation of each of these obfuscating techniques, *see* FTC, National Do Not Email Registry: A Report to Congress at 8-10 (June 2004), available at http://www.ftc.gov/reports/dneregistry/report.pdf.

58. For instance, in *FTC and State of California v. Optin Global*, No. C-05-1502 SC (N.D. Cal. filed Apr. 12, 2005), defendants listed a non-existent Canadian address in their domain name registrations.

improve their odds of getting their messages into consumers' inboxes: the use of "bot networks" and affiliate marketing programs.

Bot networks are comprised of multiple zombie drones controlled by the same entity.[59] Over the past two years, the use of zombie drones and bot networks to send spam has increased, while the use of open relays, which were commonly used at the time the Act was passed, has decreased.[60] Estimates of the percentage of spam being sent via zombie drones range from 48 percent[61] to 75 percent of all email.[62]

The second tactic involves spammers decentralizing their operations, often through the use of affiliate marketing programs. In such programs, a marketer contracts with affiliates who send spam advertising the marketer's product or service. The marketer pays a commission to an affiliate whenever the affiliate's spam results in a sale or drives traffic to a designated website. Marketers attempt to use affiliate programs to insulate themselves from liability under CAN-SPAM. Although complicated affiliate arrangements can make it more expensive and time-intensive for law enforcers and others empowered to sue under the Act, decentralizing spam operations does not effectively insulate those who, under the Act's relatively broad definition, "initiate" the sending of a commercial email message, or those "senders" "whose product, service, or Internet website is advertised or promoted by the message."[63]

A more troubling shift in spamming tactics over the past two years involves the types of messages sent: spam advertising commercial products or services is being replaced by spam that is potentially more harmful, as opposed to merely

---

59. *See* Appendix 3 (setting forth a detailed explanation of spammers' tactics to remain anonymous while sending large volumes of spam).

60. Joe St Sauver, *Spam Zombies and Inbound Flows to Compromised Customer Systems,* presented at the Messaging Anti-Abuse Working Group ("MAAWG") General Meeting, Mar. 1, 2005, available at http://darkwing.uoregon.edu/~joe/zombies.pdf.

61. Press release, *MX Logic Reports Spam Accounts for 67 Percent of All Emails in 2005* (Sept. 22, 2005), available at http://www.mxlogic.com/news_events/press_releases/09_22_05_SpamStats.html.

62. Confidential 6(b) responses.

63. 15 U.S.C. §§ 7702(9), (16). The Act defines the term "initiate" to include not only the origination of a message, that is, "pushing the button," but also procuring the origination of such message. The Act defines the term "procure" to mean "intentionally to pay or provide other consideration to, or induce another person to initiate such message on one's behalf." 15 U.S.C. § 7702(12). Thus, any entity paying another party to send commercial email messages or inducing them to do so, is responsible for CAN-SPAM compliance. This is one of the strengths of the CAN-SPAM Act.

annoying.[64] For example, phishing spam, which attempts to trick recipients into providing personally identifiable information to scam artists posing as legitimate businesses, has increased significantly since the enactment of CAN-SPAM.[65] The Act does not cover phishing emails because they fall outside its definition of both "commercial electronic mail message" and "transactional or relationship message." The FTC does not recommend that the Act be modified to cover phishing emails because existing laws already enable criminal and civil law enforcement authorities to bring suit against those perpetrating phishing scams. By way of example, the FTC has brought actions against phishing schemes using its authority under Section 5 of the FTC Act.[66] DOJ has also prosecuted phishers.[67]

Another troubling development is an increase in the use of spam that deploys malware[68] on recipients' computers.[69] This can occur when a recipient clicks on a link in spam that lures the recipient to a website where his computer will become infected with spyware or other types of malware. In some instances, even less action is required on the part of the recipient. Instances have been reported where merely opening a malicious email can subject the recipient to harm from malware.[70] Surreptitious deployment of this kind of code can result in: slowed computer performance; installation of key-logger software that can record and report every keystroke on a consumer's personal computer; deployment of

---

64. Confidential 6(b) response.

65. Statistics available from the Anti-Phishing Working Group, an industry association, show that in January 2004, only 176 unique phishing attacks were reported. That number increased significantly to 14,135 unique attacks in July 2005. *See* http://www.antiphishing.org/resources.html#consumer. *See also CAN-SPAM A Year Later,* Pew Internet & Am. Life Project, Apr. 2005 (35 percent of those surveyed said they had received unsolicited email requesting personal financial information). Recent reports suggest that they comprise less than 10 percent of all email sent. *See Fight Fraud and Phishing with New Tools,* PC World, Apr. 25, 2005, available at http://www.pcworld.com/reviews/article/0,aid,120501,00.asp.

66. *See, e.g.*, *FTC v. Minor (C.J.)*, No. 03-CV-5275 (C.D. Cal. filed July 24, 2003); *FTC v. Hill*, No. 03-CV-5537 (S.D. Tex. filed Dec. 3, 2003); *FTC v. Minor (M.M.)*, No. CV-04-2086 (E.D.N.Y. filed May 18, 2004).

67. For a description of criminal cases brought by DOJ against phishing scams, *see* U.S. Department of Justice Criminal Division Annual Report, at 51-53 (2004), available at http://www.usdoj.gov/criminal/CRMAnnualReport2004.pdf.

68. "Malware," short for "malicious software," is a term used to refer to a wide variety of harmful programs that can be installed, often surreptitiously, on computers. Examples include spyware, viruses, and trojan horses. The harm resulting from malware can range from invasion of privacy, such as in cases when spyware monitors the Internet browsing habits of victims, to serious financial consequences, when data is destroyed or keystroke logger programs are used to facilitate identity theft.

69. *See* Confidential 6(b) responses; John Leyden, *Anti-spam Success Drives Malware Authors Downmarket,* The Register, June 30, 2005, available at http://www.theregister.co.uk/2005/06/30/digital_mafia_rountable/.

70. *See* Judge Report, 17-18.

viruses; and exploitation of vulnerabilities in unsecured machines that renders them zombie drones.[71]

The most promising tool to combat these new spammer techniques is authentication technology that would remove the cloak of anonymity under which spammers currently operate. Developments in authentication technology are discussed in the following section.

4. Development of Effective Authentication Strategies May Counter the Rising Threat of Malicious Spam

While existing server-level and consumer-level anti-spam measures appear to have begun to turn the tide on the types of spam addressed by the Act, authentication technologies are needed to combat the increasing amount of spam serving as a vector for viruses and malware. As the Commission noted in its Report to Congress on a National Do Not Email Registry, one of the most encouraging marketplace developments regarding email involves the creation of domain-level email authentication systems that are designed to combat the fundamental problem facing the email system today – the ability of spammers to send email anonymously.[72]

The current email system (SMTP) does not require that an email message contain accurate routing information, except for the intended recipient of the email.[73] Therefore, a spammer may "spoof" or falsify some portions or all of the header of an email message, making it virtually impossible for investigators to identify the true source of an illegal email message. Domain-level authentication technology addresses this problem by enabling a receiving mail server to know if

---

71. Purely malicious spam – spam that is not primarily "commercial" in nature – is not covered by CAN-SPAM. Such malicious spam can be a means to disseminate spyware, or other malware that causes some of the same problems as spyware. The FTC has actively pursued spyware companies using its authority under Section 5 of the FTC Act. *See FTC v. Seismic Entertainment,* No. 04-377-JD, 2004 U.S. Dist. LEXIS 22788 (D.N.H. filed Oct. 21, 2004); *FTC v. MaxTheater,* No. 05-CV-0069 (E.D. Wash. filed Mar. 7, 2005); *FTC v. Odysseus Marketing*, No. 05-CV-330 (D.N.H. filed Sept. 21, 2005). Additionally, the FTC has taken action against marketers that use deceptive spam to trick recipients into believing that their computers have been infected with spyware. In *FTC v. Trustsoft*, the defendants' spam allegedly made false claims that convinced consumers to conduct free scans of their computers. These scans identified innocuous software as spyware, which coaxed consumers into purchasing defendants' spyware removal products. In this case, because defendants' spam was commercial in nature, and not purely malicious, the Commission alleged violations of both the FTC Act and CAN-SPAM. *See FTC v. Trustsoft,* No. H-05-1905 (S.D. Tex. filed May 31, 2005).

72. FTC, National Do Not Email Registry: A Report to Congress at 8-13 (June 2004), available at http://www.ftc.gov/reports/dneregistry/report.pdf. Authentication technologies also serve to limit false positives. *See* Judge Report, 9-11.

73. SMTP stands for simple mail transfer protocol. *See* Appendix 3 for a description of how the current email system works.

an email was sent from an IP address that is registered to the purported sender. In other words, if an email message purported to come from *abc@ftc.gov*, domain-level authentication would make it possible for a recipient to know if, in fact, the email came from the ftc.gov domain.

One of the current proposals in the marketplace, Sender ID, would require all email senders to register the IP addresses from which they send email in the domain name system ("DNS").[74] Receiving mail servers could then compare the IP addresses listed in the header of an email message with the IP addresses in the DNS to "authenticate" the domain from which the message was sent. Authenticated email would be given a positive score, and non-authenticated email a negative score. These scores can be used by existing filtering technology as an additional indicator of whether an email message is spam. While lack of authentication alone may not prevent delivery of an email message, it will be an additional criterion applied by existing anti-spam filtering policies, making it more likely that non-authenticated messages will be blocked.[75]

In the National Do Not Email Registry Report, the Commission pledged to encourage rapid development of domain-level authentication standards. Toward that end, the Commission, together with the Department of Commerce's National Institute of Standards and Technology ("NIST"), conducted a two-day Email Authentication Summit in November 2004 to advance the dialogue on nascent domain-level email authentication protocols and to encourage rapid movement by industry in this area.[76] Over 300 people attended the Summit, including representatives from ISPs, small and large businesses, consumer groups, and technology firms.

During the Summer of 2005, industry representatives took the next step, and organized an Email Authentication Implementation Summit.[77] Over 500

---

74. There are other authentication technologies being developed in the marketplace, including DomainKeys Identified Mail ("DKIM"), which uses public key cryptography to verify the source and contents of email messages. For further discussion, *see infra* notes 76-77.

75. *See* "The Urgent Need to Implement E-mail Authentication: A Value Proposal for Senders, Users, and Domain Holders," Craig Spiezle, June 6, 2005, available at http://www.microsoft.com/technet/community/columns/sectip/st0605.mspx.

76. In preparation for this Summit, the Commission and NIST solicited comments to help shape the agenda in this rapidly-evolving area. Forty-three comments were received and posted on the Summit website. The comments are available at http://www.ftc.gov/os/comments/emailauthentication/index.htm.

77. *See* http://www.emailauthentication.org. A second industry summit is planned for April 2006. *See* http://www.emailauthentication.org/summit2006/summit2006.html.

attendees participated in the one-day event, discussing specific case studies on implementation and reviewing primary authentication proposals. At this event, industry members proposed a timeline for the implementation of domain-level email authentication. According to that timeline, beginning in November 2005, non-authenticated email messages are subject to heightened scrutiny.[78]

Much of the promise of domain-level email authentication technology lies in how it can vastly improve other anti-spam technologies. For instance, the utility of accreditation and reputation services will increase substantially when domain-level authentication systems are widely deployed. Accreditation services certify that a particular sender uses best practices.[79] Reputation scoring looks at the practices of senders and assigns a reputation score depending on whether the messages sent appear to be spam or legitimate email.[80] ISPs' anti-spam filters can incorporate accreditation and reputation scores into their algorithms. Used in conjunction with domain-level authentication, a recipient's ISP could have a fairly good measure of certainty that an email that purports to be from an accredited sender or a sender with a positive reputation actually came from that sender.

5. Consumers Are Increasingly Using Mobile Devices to Access Their Email

This section contains § 7709(b)(1)'s required analysis of "changes in the nature of the devices through which consumers access their electronic mail messages" and the way these may impact the effectiveness of CAN-SPAM.[81] Since CAN-SPAM's enactment, there has been a measurable increase in the number of individuals who view their electronic mail via mobile devices, such as personal digital assistants ("PDAs") and cellular phones. Although the types of devices used to view email have not changed much since passage of the Act,[82] the increased usage of mobile devices to receive and view email is a notable

---

78. *See* http://emailauthentication.org/summit2005/02_BoA_EJohnson.pdf, slide n.8. The FTC will continue to monitor the industry's progress toward domain-level email authentication technologies. The Direct Marketing Association is advising its members to start authenticating their email or face disciplinary action by the DMA. *See* press release, Direct Marketing Association, DMA Requires Members to Adopt E-Mail Authentication Systems (Oct. 17, 2005) available at http://www.the-dma.org/antispam/EMail_Authentication_Guidelines.pdf.

79. *See* Judge Report, 6-7.

80. *See* Judge Report, 6-7.

81. 15 U.S.C. § 7709(b)(1).

82. Cellular telephones with email capability, known as "smart phones," and PDAs remain the two primary methods by which mobile users access their email, as was the case in late 2003. Newer models, some including features allowing or improving access to email from these devices, have been introduced, but the fundamental access method remains the same.

development.[83] By 2005, nearly five percent of the 191 million U.S. wireless users were accessing e-mail via mobile devices.[84] The growth in adoption of these kinds of devices as a means to access email and the Internet has been accompanied by a concomitant growth in the number of spam messages received by users of the devices.[85]

By their very nature, mobile devices differ from most desktop or laptop computers that consumers use to receive and view email messages. The most important difference, of course, is their diminutive size and weight, making these devices conveniently portable. Most fit comfortably into the palm of one's hand, and many weigh just ounces. Despite their miniaturized size, though, many mobile devices allow for access to email and the Internet, as well as other functionality.[86]

In preparation for this Report, the Commission sought to determine whether certain CAN-SPAM provisions are less effective when a consumer receives and views electronic mail on mobile devices, in particular because of the reduced screen size. The weight of the evidence leads to the conclusion that CAN-SPAM is equally effective for those using mobile devices as for those using conventional computers to receive and view email.[87]

---

83. According to some predictions, growth of these devices, however robust to date, "is set to explode" over the coming years. *See BlackBerry: Bring It On!,* Newsweek, Sept. 26, 2005 (noting that there are only six million wireless e-mail accounts in use today, but that the potential demand – with more than 650 million corporate e-mail accounts alone – is potentially enormous). *See also* Confidential 6(b) response.

84. *See The Utilitarian Life of the Mobile Internet,* ClickZ.com, Sept. 9, 2005, available at http://www.clickz.com/stats/sectors/wireless/print.php/3547651.

85. *See, e.g.,* press release, *Mobile Spam Volume Doubles to Forty-Three Percent*, Wireless Services Corporation (Feb. 28, 2005), available at http://www.wirelesscorp.com/pressrelease_2_28_05_spam.htm. The FCC's CAN-SPAM rules do not apply to all mobile spam. Pursuant to § 7712(b) of the Act, the FCC was charged with developing rules to enable consumers to avoid receiving unwanted "mobile service commercial messages ("MSCM")," defined as a "commercial electronic mail message[s] that [are] transmitted directly to a wireless device that is utilized by a subscriber of commercial mobile service." 15 U.S.C. § 7712(d). In publishing the Order implementing its Rule, the FCC clarified that the definition of MSCM "includes any commercial electronic mail message as long as the address to which it is sent or transmitted includes a reference to the Internet and is for a wireless device. . ." and specifically noted that messages sent using Internet-to-phone SMS (short message service) technology would be covered under the CAN-SPAM rules. CAN-SPAM Order, 19 FCC Rcd at 15933-34, ¶ 16. The FCC further explained, however, that because phone-to-phone SMS messages do not reference Internet domains, they are not subject to CAN-SPAM; rather, they are regulated under the Telephone Consumer Protection Act. *Id*. at ¶ 17.

86. In addition to facilitating communication, many mobile devices allow users to synchronize the data on their personal computer with their mobile device, use global positioning services, take photographs, and store and access media, such as pictures and music.

87. Confidential 6(b) responses largely suggested that there is no data on whether new methods of accessing email are impacting the practicality and effectiveness of the Act. However, one response noted that an increase in exploits targeting smart phones and other mobile devices has been observed. These include phishing and malware installations, neither of which is covered by the Act.

Some sources consulted for this Report pointed out that email-receiving cell phones and PDAs have been in use for the past several years.[88] While mobile devices are gaining in popularity,[89] they are rarely the only means through which recipients view email.[90] Rather, most recipients receive email both on their primary computer and on their mobile device. Thus, email sent to a recipient would be viewable through both the recipient's primary computer and his PDA.

When asked whether increased usage of mobile devices to view and receive email impairs CAN-SPAM's effectiveness, most of those consulted believed that it did not. Even with the smaller screen size of mobile devices, commenters said that recipients would be able to read the subject line, and that opt-out links and mechanisms would generally function.[91] Some suggested, though, that opt-out mechanisms that required accessing the Internet, such as web-based forms, might be inoperable from a mobile device or could cause recipients who choose to opt out from their mobile device to incur airtime costs.[92] However, others countered that these concerns were unfounded, stating that recipients typically manage email deletion and opt-out functions from their primary computers, not from their mobile devices.[93]

Currently, it appears that consumers who receive email on mobile devices from legitimate marketers can effectively opt out of receiving future messages either directly from their mobile devices or from their personal computers.[94] Therefore, the Commission concludes that while more consumers are accessing their email from mobile devices today than when CAN-SPAM was enacted, the protections afforded by CAN-SPAM currently are not diminished when email is viewed from a hand-held device. Thus, at this time the Commission does not

---

88. Microsoft: Goodman, 14-15; DMA: Cerasale, 12; Skylist: Baer, 19.

89. IETF: Levine, 9; Confidential 6(b) responses.

90. Microsoft: Goodman, 14-15; DMA: Cerasale, 12; Skylist: Baer, 19.

91. Aristotle: Bowles, 15; Microsoft: Goodman, 14-15; Skylist: Baer, 17; Acxiom: Colclasure, 9-10 (describing the care taken by companies to ensure that marketing messages sent to mobile devices comply with CAN-SPAM).

92. Oregon: St Saveur, 11-12 (noting that subject lines may be truncated and that certain anti-spam software programs are not designed to be used on mobile devices); Columbia: Bellovin, 12 (noting that SMS messages often cost the recipient money).

93. Aristotle: Bowles, 15; Microsoft: Goodman, 14-15; Skylist: Baer, 17.

94. To increase the ability of consumers to exercise their opt-out rights directly from their mobile devices, the Commission notes that a best practice for marketers would be to include an email-based opt-out mechanism in every commercial message. With such a mechanism, the user of a mobile device that does not include an Internet browser would be able to opt out of receiving future commercial email messages using the mobile device.

recommend any modification of the Act explicitly to address the use of mobile devices to view email. Nevertheless, given the rapidity with which technological changes can occur, the Commission intends to continue monitoring changes in the ways that consumers receive and view email to ensure that the Act's protections are not thwarted by new developments.

6. Impact of Technological and Marketplace Developments on CAN-SPAM's Effectiveness

When enacting CAN-SPAM, Congress found that "[t]he problems associated with the rapid growth and abuse of unsolicited commercial electronic mail cannot be solved by federal legislation alone. The development and adoption of technological approaches and the pursuit of cooperative efforts with other countries will be necessary as well."[95] The past two years have borne out Congress's finding. With most legitimate marketers complying with CAN-SPAM and technological advances making a dent in the volume of spam, there is reason to believe that legislation and technology together are helping to solve the spam problem.

Compliance with CAN-SPAM by top online marketers is high, and has been unaffected by any of the technological or marketplace developments described above. Moreover, CAN-SPAM provides law enforcement and ISPs with certain useful weapons in the fight against spam. However, CAN-SPAM has no impact on – and does not even apply to – the growing proportion of spam that serves as a vector for viruses or malware and contains no commercial message. The Commission believes that technological advances provide the greatest promise in stopping outlaw spammers that send virus-laden messages or hide their identities and locations. Still, as explained in the next section, passage of the US SAFE WEB Act[96] would improve the Commission's ability to enforce CAN-SPAM against senders who operate from or transmit their spam through foreign countries.

B. International Issues

Section 7709(b)(2) of the CAN-SPAM Act requires that the Commission provide "analysis and recommendations concerning how to address commercial electronic mail that originates in or is transmitted through or to facilities or

95. 15 U.S.C. § 7701(a)(12).

96. *See infra* section III.B.3.a.

computers in other nations, including initiatives or policy positions that the Federal Government could pursue through international negotiations, fora, organizations, or institutions." Accordingly, this section of the Report:

- provides background on both the international nature of spam and obstacles that international issues have posed for anti-spam law enforcement;
- describes FTC efforts to address these obstacles; and
- sets forth the FTC's recommendations in this area, including passage of the US SAFE WEB Act.

1. The International Nature of Spam and the Obstacles It Presents for Law Enforcers

The Commission has found no reliable statistics on the percentage of spam that comes from marketers located within or outside of the United States.[97] Rampant spoofing, and the use of open relays, proxies, and zombie drones often make it impossible to determine the country from which a spam message has originated.[98]

Despite the difficulty in determining where spam messages originate, it is clear that spam is often transmitted through facilities or computers in countries other than the U.S. or contains hyperlinks to websites registered or hosted abroad.[99] This international aspect of spam frustrates FTC law enforcement efforts because the Commission has no mechanism to compel information from third parties located abroad about spam that may have come through their systems or about websites registered or hosted offshore.

---

97. During numerous teleconferences among the FTC, ISPs, technologists, and others in July 2005, no participants offered calculations in this regard. *See, e.g.,* Pew: Fallows, 35 ("I find it very difficult to sort through [the wide-ranging origination figures being reported]"). MX Logic described the reported figures of spam's origin as "cloudy and murky" and "very complicated because origins can be so easily masked, for example by proxies and zombies." Telephone conversation with MX Logic (Aug. 24, 2005); Word to the Wise: Adkins, 43-45 (noting that the term "'origin' is ill defined [in the reporting] . . . [Different reports measure] different things, some of them are measuring where the website happens to be hosted. Some of them are measuring the language the spam is sent in. Some of them are measuring the compromised machines that were used to send it. Some of them are measuring the spammers they believe were responsible for it, where they live . . ."); Microsoft: Goodman, 32 (determining where a spam message came from is "a difficult technical question because there are so many ways to obscure" its origin).

98. FTC, National Do Not Email Registry: A Report to Congress at n.123 (June 2004), available at http://www.ftc.gov/reports/dneregistry/report.pdf.

99. *Unsolicited Commercial E-Mail: Hearing Before the Senate Comm. on Commerce, Science and Transp.,* 108th Cong., 1st Sess. (2003) (testimony of then Commissioners Orson Swindle and Mozelle Thompson on behalf of the FTC).

Even when a spammer cannot be identified, CAN-SPAM makes it possible for the Commission to take action against the seller who profits from the spam.[100] Nevertheless, law enforcers can encounter significant obstacles in locating sellers as well as spammers. Obtaining information is one such obstacle. For example, investigations often involve spam advertising a commercial website that may be registered with a foreign domain registrar. The Commission is unable to compel foreign registrars or other foreign entities to disclose information; therefore, the Commission is unable to identify the party responsible for the website. Another obstacle is the Commission's inability to require that an investigation be kept confidential. Investigations often involve civil investigative demands ("CIDs")[101] sent to third parties such as ISPs and domain registrars to obtain information about subjects under investigation. The success of an FTC action against a spammer often depends upon the investigation remaining confidential so that the subjects are not prematurely tipped off. Once notified of an impending FTC action, a target of an investigation may disappear and move assets offshore beyond the reach of U.S. courts. A third obstacle is locating and compelling repatriation of assets. Like typical fraud operators, spammers often hide their ill-gotten gains in foreign bank accounts. It is difficult for the Commission to obtain information about these assets. Even if the Commission may locate these assets, it is difficult to recover them and provide redress to defrauded U.S. recipients of spam or use them to pay court-ordered penalties.

These obstacles are formidable, and in some instances, insurmountable. Despite the Commission's successes in stopping some spammers and sellers who take advantage of international borders,[102] the FTC needs additional tools

---

100. *See* Appendix 1.C.

101. The FTC Act permits the Commission to issue compulsory process through a type of administrative subpoena known as a civil investigative demand. 15 U.S.C. § 57b-1; 16 C.F.R. § 2.7.

102. Examples of successful enforcement of international spam cases under CAN-SPAM include the following: (1) *FTC v. Phoenix Avatar*, No. 04C 2897 (N.D. Ill. filed Apr. 23, 2004) (U.S.-based defendants caused spam promoting websites whose domain names were registered with Swiss and French registrars to be sent to U.S. consumers from various locations around the world; settlement obtained in March 2005 with defendants agreeing to an injunction and a judgment of $230,000, suspended but for $20,000 based upon inability to pay); (2) *FTC v. Creaghan Harry*, No. 04C 4790 (N.D. Ill. filed July 21, 2004) (U.S.-based defendant caused spam to be sent to U.S. consumers from computers around the world, forwarded proceeds to Latvia, and used a Swedish address for contact information; settlement obtained in June 2005 with defendant agreeing to an injunction and to pay $485,000 in consumer redress); and (3) *FTC v. Cleverlink Trading*, No. 05C 2889 (N.D. Ill. filed May 16, 2005) (U.S.-based defendants operated a company registered in Cyprus and caused adult-oriented spam to be sent to U.S. consumers from computers all over the globe; temporary restraining order and preliminary injunction obtained after the FTC, with assistance from the Cypriot government, linked the defendants with the Cyprus corporation).

to help overcome the obstacles present in the international context and to allow the Commission to proceed against spammers more quickly and efficiently. The specific recommendations discussed in section III.B.3 below, if implemented, would give the Commission some of these tools and would enhance the Commission's ability to enforce CAN-SPAM.

2. FTC Efforts to Address Spam in the International Arena

In working to overcome the obstacles discussed above, the FTC has taken steps to leverage international resources in combating spam by building international enforcement cooperation, advocating the multifaceted approach to combating spam adopted by the U.S.[103] at every opportunity in international conferences and policy discussions, and undertaking international initiatives to educate businesses.

a. Building Enforcement Cooperation

During spam investigations and litigation, the FTC often requests help from its foreign counterparts to obtain information, such as corporate records, telephone number subscriber information, court pleadings, and reports. To improve this type of international cooperation, the FTC has undertaken efforts to build informal enforcement cooperation networks.[104]

The London Action Plan on International Spam Enforcement Cooperation ("LAP") is one example of such collaboration. Begun by the FTC and the United Kingdom Office of Fair Trading in 2004, the LAP is an informal network of government agencies responsible for spam enforcement and private sector representatives interested in enforcement of spam laws. Currently, LAP membership spans five continents, with 33 government agencies from 23 participating countries, as well as 24 private sector entities participating.[105] LAP members exchange information about spam investigations and enforcement actions, mainly through periodic telephone conference calls.

---

103. The anti-spam approach adopted by the U.S. involves several components, including: enforcement, regulation/legislation, encouragement of the development of technological solutions, encouragement of self-regulatory efforts by industry, and education of consumers and businesses about spam and their role in limiting its negative effects.

104. The international dimension to the spam problem affects criminal, as well as civil, law enforcement under the Act. *See* Appendix 1.A. Because criminal law enforcement authority under CAN-SPAM lies with DOJ, the Commission consulted with the Computer Crime and Intellectual Property Section of DOJ's Criminal Division, which has principal authority over DOJ's position on international law enforcement in connection with spam, in the preparation of this section of the Report.

105. Additional information on the LAP is available at http://www.ftc.gov/opa/2004/10/spamconference.htm.

Another avenue for enforcement cooperation in which the FTC participates is the International Consumer Protection and Enforcement Network ("ICPEN"), which consists of governmental agencies responsible for consumer protection enforcement. Though many countries do not yet have anti-spam laws, members of ICPEN do have the authority to enforce laws against deceptive practices. Because much of spam contains false representations,[106] many ICPEN agencies use these laws to take action against deceptive spam. ICPEN also encourages international cooperation among its participating agencies. For example, the FTC and the U.K. Office of Fair Trading have used the ICPEN network to promote participation in the LAP. Finally, the FTC has entered into two Memoranda of Understanding ("MOU") with foreign agencies that focus on spam enforcement. The first is among the FTC and government agencies in the United Kingdom and Australia, and the second is between the FTC and Spain's data protection authority, Agencia Española de Protección de Datos. These MOUs are "best efforts" agreements intended to improve cooperation on spam enforcement among participating nations.[107]

These informal cooperation arrangements are extremely helpful in building contacts to assist in FTC spam investigations and cases. For example, as a result of the MOU with the Australian agencies, the FTC obtained assistance in one spam case targeting unsubstantiated health and diet claims. In this case, the defendants were located in Australia, but they caused illegal spam to be sent to U.S. consumers. The Australian agency provided information and helped the FTC serve the defendants.[108]

Although useful, the informal information-sharing networks that the FTC has cultivated have limitations. Often, foreign agencies will not share information with the FTC because of the Commission's inability to reciprocate; current law prohibits the FTC from sharing with foreign agencies certain information that the

---

106. FTC staff, False Claims in Spam at 10 (2003), available at http://www.ftc.gov/reports/spam/030429spamreport.pdf.

107. DOJ supports the FTC's efforts to develop these new information-sharing arrangements in connection with enforcing the civil provisions of CAN-SPAM. However, DOJ utilizes existing criminal enforcement information-sharing channels for international cooperation to combat criminal spam, as well as other computer crimes that are facilitated by spam (*e.g.,* online fraud, spyware, and virus and worm transmission). For example, the U.S. government, led by DOJ, advocates use of the Council of Europe's Convention on Cybercrime as an existing multilateral tool to address the problems posed by criminal spam. Thus, DOJ believes that any additional international arrangements that relate to spam enforcement cooperation should be limited to cooperation among civil agencies.

108. *FTC v. Global Web Promotions*, No. 04C 3022 (N.D. Ill. filed Apr. 28, 2004).

FTC obtains during investigations.[109] Foreign agencies are also unwilling to share information with the FTC because the FTC cannot guarantee the confidentiality of the information provided – there may be circumstances when the FTC is required to disclose the information. The FTC believes that legislative changes are needed to address these issues, as discussed further in section III.B.3 below.

b. International Advocacy

The global nature of illegal spam necessitates a global approach to combating the problem. Spammers, unlike enforcement authorities and courts, disregard international borders. Thus, the FTC has energetically advocated the interests of U.S. consumers in various international fora.[110]

The goals of the FTC's advocacy have been threefold. First, the Commission has encouraged other countries to enforce their anti-spam laws aggressively. Second, the Commission has urged other countries to be mindful of the tension between the need to combat spam and the need to preserve the convenience and speed of global email communication. Toward this end, the FTC has discouraged attempts to combat spam by blocking email from particular countries – an overly broad measure that could result in unnecessary restriction of the flow of email worldwide. Third, the Commission has assisted in efforts to educate foreign governments, businesses, and consumers about how to combat illegal spam.

One of the various fora in which the FTC has worked to advance these goals is the Organization for Economic Cooperation and Development ("OECD") Spam Task Force. One of this task force's activities has been to develop an anti-spam "toolkit" for OECD member and non-member countries to use in their fight against spam. The toolkit will include a presentation of spam statistics, guidance on fostering and developing technological solutions, a survey of anti-spam legislation in different countries, and recommendations on cross-border enforcement cooperation to combat spam. The FTC also participates in working groups within the Asia Pacific Economic Cooperation forum and the World Summit on the Information Society, both of which work to counter spam.

---

109. *See infra* note 117.

110. DOJ also participates in these international fora and advocates the U.S. approach to spam. At these meetings, DOJ often emphasizes to other countries that the law relating to spam in the U.S. is unique in that one of the penalties for criminal spam is incarceration.

c. International Education Campaigns

The FTC has also worked to educate governments and businesses internationally about what they can do to help combat illegal spam. For example, the Commission has provided technical training to foreign governments on how to conduct spam investigations. Two of the most recent training sessions were held in Colombia in May 2004 and Korea in June 2005.

Moreover, the FTC has worked to educate small businesses through several international education initiatives designed to alert small businesses that they may unwittingly become spammers if their computers are not secured. The FTC has undertaken two major initiatives in this regard.

Most recently, in May 2005, the FTC announced "Operation Spam Zombies" in partnership with over 30 agencies from around the world.[111] In this educational campaign, participating agencies sent letters to more than 3,000 ISPs worldwide to urge them to take measures to prevent their subscribers' computers from becoming zombie drones. The letter included recommended practices for ISPs, such as (1) blocking port 25 and (2) applying rate-limiting controls.[112] The next phase of this ongoing campaign will be to identify ISPs with zombie drones on their networks, inform those ISPs, and urge them to implement corrective measures, *e.g.,* blocking port 25 and implementing rate-limiting controls.

Previously, in 2004, the FTC launched a similar campaign, "Operation Secure Your Server," a joint project of agencies of nearly 30 countries to educate businesses about how to protect their servers from being used as open proxies or open relays to send spam.[113] As part of this project, participating countries sent letters to the managers of potentially unsecured servers worldwide explaining the problems caused by such servers and how to solve them.

3. Recommendations

The FTC intends to continue its strategic participation in international discussions to build enforcement cooperation, promote technological solutions, and provide technical assistance. Greater results could be achieved, however, if Congress were to enact the "Undertaking Spam, Spyware, And Fraud

---

111. *See* http://www.ftc.gov/bcp/conline/edcams/spam/zombie/index.htm.

112. *See supra* section III.A.2 for a description of port 25 and rate limiting.

113. *See* http://www.ftc.gov/bcp/conline/edcams/spam/secureyourserver/index.htm.

Enforcement With Enforcers beyond Borders Act of 2005" or the "US SAFE WEB Act of 2005."[114]

a. Passage of the US SAFE WEB Act

As explained above in section III.B.1, the international nature of spam significantly limits the FTC's ability to enforce the CAN-SPAM Act. To help overcome these limitations, the FTC recommends that Congress enact the US SAFE WEB Act.[115] The US SAFE WEB Act would give the FTC new tools to better trace spammers and sellers whose operations are, in whole or in part, beyond U.S. borders.

In a report to Congress in June 2005, the FTC described how the US SAFE WEB Act would improve the FTC's cross-border enforcement efforts in several areas.[116] For purposes of this Report on the effectiveness of CAN-SPAM, the Commission highlights two specific areas in which the US SAFE WEB Act would help the FTC in spam investigations.

First, as noted above, under current law, the FTC cannot share certain information it obtains in spam investigations with its foreign counterparts. By way of example, even if the FTC and a Canadian agency were investigating a Canadian spammer that is defrauding U.S. consumers, in many cases the FTC could not share information it obtained pursuant to CIDs with the Canadian agency. This is true even though a Canadian action against the spammer would benefit U.S. consumers.[117] This is not a hypothetical concern: in one recent case, the FTC obtained an order against a spammer defrauding U.S. consumers and found that the spammer had an affiliate that was perpetrating the same scam from a foreign country, targeting both U.S. and foreign consumers. The FTC was prevented by current law from sharing the information it obtained pursuant to CID

---

114. S. 1608, 109th Cong. §§ 1-13 (2005).

115. Predecessor legislation entitled the "International Consumer Protection Act," which was virtually identical to the US SAFE WEB Act, was passed by the Senate and three House Committees in the 108th Congress.

116. The staff of the FTC issued a Report to Congress, "The US SAFE WEB Act: Protecting Consumers from Spam, Spyware, and Fraud," in June 2005. That report is available at http://www.ftc.gov/reports/ussafeweb/USSAFEWEB.pdf. For a summary of the major provisions of the legislation, *see* Appendix 4 of this Report.

117. The Commission cannot disclose "documentary material, tangible things, reports or answers to questions and transcripts of oral testimony" that are "received by the Commission pursuant to compulsory process in an investigation" without the consent of the person who submitted the information, except as specifically provided. 15 U.S.C. § 57b-2(b)(3)(C); 16 C.F.R. § 4.10(d).

with its foreign counterpart. The US SAFE WEB Act would allow the FTC to share such information and provide investigative assistance in appropriate cases.

Second, the US SAFE WEB Act would improve the FTC's ability to gather information, whether it be about spammers, sellers, or related persons, in spam investigations. In such investigations, the FTC often relies on CIDs sent to third parties such as ISPs and domain registrars to obtain information about persons involved. The success of FTC actions against spam often depends on investigations remaining confidential so that the subjects are not prematurely tipped off. Once notified of an impending FTC action, these subjects can disappear and move assets offshore, beyond the reach of U.S. courts, making it much more difficult to obtain redress for U.S. fraud victims. The US SAFE WEB Act contains provisions that would give the FTC authority already granted to the Securities and Exchange Commission and the Commodity Futures Trading Commission to obtain information from third parties without tipping off subjects.[118]

Although not a panacea for all of the problems faced by the FTC in its spam investigations, the US SAFE WEB Act would give the FTC new tools to better trace spammers that try to use geographical borders as a shield from law enforcement. Thus, to help the FTC combat spam, the Commission recommends that Congress enact the US SAFE WEB Act.

b. International Policy Recommendations

Section 7709(b)(2) of CAN SPAM requires that the Commission make recommendations on "initiatives or policy positions that the Federal Government could pursue through international negotiations, fora, organizations, or institutions." As outlined above, the FTC and other government agencies participate in a number of international initiatives aimed at combating spam. The Commission recommends a continuation of these efforts.

The Commission notes, however, that just as studies conducted within the U.S. are showing that consumers seem to be less annoyed by spam,[119] studies undertaken overseas show similar results. One 2004 public opinion survey in

---

118. 15 U.S.C. § 78u(h). *See* FTC staff report, "An Explanation of the Provisions of the US SAFE WEB Act" at 9-10 and nn.38-39 (June 2005), available at http://www.ftc.gov/reports/ussafeweb/Explanation%20of%20Provisions%20of%20US%20SAFE%20WEB%20Act.pdf.

119. *See supra* section III.A.1 regarding the drop in spam messages reaching consumers' inboxes and rising level of tolerance toward spam messages that consumers do receive.

Canada reported that Canadians believe they are receiving less spam now than a year ago.[120] A recent Finnish study indicates that while it may be "a nuisance factor" for some users affecting their email use, spam "is not a very serious problem in terms of quantities."[121] These results seem to mirror the conclusions of studies conducted within the U.S. that show a decrease both in the amount of spam received by consumers and consumer annoyance with spam.

Despite studies suggesting a lessening of the spam problem, there continues to be a proliferation of international policy initiatives, meetings, discussions, and agreements on spam.[122] Rather than expending resources on a multitude of international policy initiatives, the Commission recommends that the U.S. government strategically focus its resources on practical international initiatives that further the specific goals outlined below:

- **Building Enforcement Cooperation** – Building spam enforcement cooperation across borders is critical. To be successful in combating spam, enforcement agencies must cooperate in sharing information, tracking spammers, exchanging evidence, and enforcing anti-spam laws. Informal enforcement networks such as the London Action Plan and ICPEN are particularly useful fora in which to build this cooperation.
- **Advocating Technological Tools to Combat Spam** – One of the inherent limitations of international policy discussions on spam is that they tend to be led by governments. By contrast, it is industry that must lead in developing technical tools. The U.S. government should encourage its foreign partners to support industry-led efforts to develop technological tools to combat spam, such as filtering and authentication. Indeed, email authentication promises to be one of the most potent tools for combating spam, as it would allow for better anti-spam filtering and could facilitate the tracking of spammers by enforcement agencies. The FTC energetically encourages the private sector to develop authentication

---

120. *See Canadians Winning the War Against Spam; Spam Volumes Dropping for the First Time in Four Years, and Attitudes Towards Email As a Communications Tool are Improving,* Canadian Inter@ctive Reid Rep., Mar. 10, 2005, press release available at http://www.ipsos-na.com/news/pressrelease.cfm?id=2594.

121. *See Finnish People's Communication Capabilities in Interactive Society of the 2000s,* Statistics Finland, Reviews 2004/7 (on file with the FTC).

122. For example, several groups within the Asia Pacific Economic Cooperation ("APEC") forum have work plans relating to spam, including the APEC Electronic Commerce Steering Group and the APEC Telecommunications and Information Working Group. As discussed earlier, the Spam Task Force of the OECD has been organized to, among other things, facilitate international cooperation on spam. The International Telecommunication Union ("ITU") has also organized a study group to discuss spam. The World Summit on the Information Society ("WSIS"), an ITU-organized summit, has held meetings on spam and continues to be active in efforts to combat spam. In addition, the eCommerce Group of the Security and Prosperity Partnership of North America (whose members are the U.S., Canada, and Mexico) has included spam in its work plan.

standards.[123] These efforts to foster private sector development of email authentication standards and related technologies should be advocated internationally.

- **Providing Targeted Technical Assistance** – In many developing countries, the promise of a global electronic marketplace cannot be realized because governments and businesses may not know how to alleviate security risks posed by spam to their networks. Additionally, consumers may not know how to alleviate similar risks to their personal computers. Moreover, developing countries with fewer resources and weaker Internet infrastructures can unknowingly become havens for fraudulent spam sent around the world. At a July 2004 meeting of the ITU and WSIS, developing countries acknowledged the problems they face with spam, and they called for more support from the developed countries and the international community in this area.[124] The FTC recommends that the U.S. government work with private sector partners to educate developing countries about various technological solutions to alleviate spam and ways in which enforcement actions can be brought against spammers. This will help U.S. consumers by fulfilling the promise of the global marketplace and by protecting consumers from spam that emanates from overseas.

C. Protecting Consumers from Pornographic Email

Section 7709(b)(3) of the CAN-SPAM Act requires that the Commission provide "analysis and recommendations concerning options for protecting consumers, including children, from the receipt and viewing of commercial electronic mail that is obscene or pornographic."[125] This section of the Report responds to that directive.

In passing CAN-SPAM, Congress found that "some commercial email contains material that many recipients consider vulgar or pornographic in nature."[126] This finding reflects consumers' serious concern regarding pornographic or obscene content in email messages. Prior to CAN-SPAM's

---

123. *See supra* section III.A.4 for a discussion of domain-level email authentication. The most recent action by the Commission in this area was the launch of a website where technologists can share the results of tests on various authentication standards. *See* http://www.ftc.gov/opa/2005/06/fyi0545.htm.

124. *See* ITU WSIS Thematic Meeting on Countering Spam, Spam in the Information Society: Building Frameworks for International Cooperation, paper available at http://www.itu.int/osg/spu/spam/contributions/Background%20Paper_Building%20frameworks%20for%20Intl%20Cooperation.pdf. The ITU chairman's report from the meeting, which concludes that developing countries require technical assistance, is available at http://www.itu.int/osg/spu/spam/chairman-report.pdf.

125. 15 U.S.C. § 7703(b)(3).

126. *Id.* § 7701(a)(5).

enactment, a report issued by Pew in October 2003 found that 53 percent of computer users considered pornographic email to be the most offensive of the email they receive.[127] Noting this, the Commission is encouraged by several recent reports suggesting that the amount of pornographic email has decreased significantly in the two years since the Act was enacted in late 2003.[128]

For instance, in April 2005, Pew reported that the number of users who reported ever receiving pornographic spam had decreased from 71 percent to 63 percent over the previous year.[129] Similarly, in July 2005, Clearswift, an Internet security company, reported that pornographic email accounted for only five percent of spam the company analyzed that month, nearly one-fourth of the amount it reported in 2003.[130] One major ISP has observed a similar trend, reporting that sexually-oriented email accounted for only six percent of email it received in January and February 2005, as compared to 23 percent for the same two-month period in 2004.[131] While the decline in pornographic email cannot be directly attributed to any single development, recent law enforcement actions and enhancements in spam filtering technology likely have contributed to the decline.[132]

In the sections that follow, this Report discusses:

- civil law enforcement under the Adult Labeling Rule issued by the Commission pursuant to CAN-SPAM to require subject line labeling of sexually-explicit email messages;
- criminal law enforcement under CAN-SPAM by DOJ;
- technologies that consumers may use to protect themselves from receiving and confronting such material;

---

127. Deborah Fallows, *Spam: How It Is Hurting Email And Degrading Life On The Internet*, Pew Internet & Am. Life Project, Oct. 22, 2003.

128. AOL: Archie, 37 (noting that AOL has seen a dramatic drop in the amount of pornographic email consumers are receiving); Microsoft: Goodman, 38 (commenting that Microsoft has seen fewer pornographic emails entering its system).

129. Deborah Fallows, *CAN-SPAM a Year Later*, Pew Data Memo, Apr. 2005. In addition, of those who have received pornographic email, 29 percent said they were receiving less than in the prior year, compared to 16 percent who said they received more and 52 percent who saw no change. *See also* Pew: Fallows, 46.

130. *See Pornographic Spam in Decline,* Clearswift, July 13, 2005, available at http://www.clearswift.com/news/item.aspx?ID=864.

131. Confidential 6(b) responses (2004 and 2005). The ISP analyzed all pre-filtered email it received during January and February of both years. Pre-filtered email constitutes the messages that enter the ISP's servers, before it applies its anti-spam filters.

132. Columbia: Bellovin, 80; ESPC: Hughes, 57; ICC: Halpert, 39 (noting that CAN-SPAM has made pornographic spam a risky business because marketers are more concerned about prosecution).

- state initiatives to establish electronic registries in an effort to protect children from unsuitable material; and
- the Commission's recommendations on protecting consumers, including children, from receiving and viewing commercial email that is obscene or pornographic.

1. Civil Enforcement of the "Adult Labeling Rule"

Section 7704(d) of CAN-SPAM provides that sexually-oriented[133] commercial email must: (1) contain a mark or notice in the message's subject line that alerts the recipient to the message's content; (2) exclude from the initially-viewable area of the message any sexually-oriented material; and (3) include in the initially-viewable area of the message only the required mark or notice, the sender's valid physical postal address, an opt-out mechanism, and instructions on how to access the sexually-oriented material.[134]

Pursuant to § 7704(d)(3) of CAN-SPAM, the Commission promulgated a rule that prescribed the phrase "SEXUALLY-EXPLICIT: " be included in the subject line and initially-viewable area of any commercial email containing sexually-oriented material. This "Adult Labeling Rule" ("ALR") took effect on May 19, 2004.[135]

CAN-SPAM and the ALR afford consumers two useful protections with respect to unwanted pornographic email. First, the required subject line label alerts recipients that the email contains sexually-explicit content and makes it easier for recipients to filter out those types of messages. Second, if consumers inadvertently open such messages, they are protected from being exposed to sexually-explicit content because the Act and the ALR specifically prohibit such content from appearing in the portion of the email the recipient initially sees when the message is opened. This virtual "brown paper wrapper" offers consumers a second layer of protection from unwitting exposure to pornographic or obscene commercial email.

While the Commission is not aware of reliable statistics relating to compliance with the ALR, as previously noted, studies and anecdotal reports

---

133. Under the Act, "sexually oriented material" means any material that depicts "sexually explicit content," as "sexually explicit content" is defined in 18 U.S.C. § 2256.

134. 15 U.S.C. § 7704(d)(1). These requirements do not apply if the recipient has given "prior affirmative consent" for the receipt of such message. *Id.* § 7704(d)(2).

135. 16 C.F.R. § 316.4.

indicate that pornographic spam is on the decline.[136] Aggressive law enforcement by the Commission and DOJ likely contributes to this development.[137]

In January 2005, the Commission filed an action against Global Net Solutions, Inc., its first case alleging violations of the ALR, and obtained a temporary restraining order ("TRO") and an asset freeze against the defendants.[138] The court entered a stipulated preliminary injunction in that case, and the case later settled. In its second case, in May 2005, the Commission charged Cleverlink Trading Limited with violating many provisions of CAN-SPAM and the ALR, and sought consumer redress, restitution and disgorgement of the company's ill-gotten gains.[139] Like the earlier case, the court issued a TRO, halting Cleverlink's allegedly unlawful spamming practices and freezing the defendants' assets. The court entered a stipulated preliminary injunction in that case in June 2005, and the matter remains in litigation.

In July 2005, the Commission announced seven additional cases against senders of sexually-explicit email that violated the ALR.[140] In these cases, brought by DOJ at the FTC's request, the Commission sought civil penalties for the ALR violations.[141] The defendants in these actions operated "affiliate marketing" programs in which they paid others to send spam on their behalf. Settlements in four of the cases imposed over $1.1 million in civil penalties. Each settlement bars illegal email practices in the future and requires that the defendants closely monitor their affiliates to ensure they also do not violate

---

136. *See supra* notes 129-132 and accompanying text. In 2005, one major ISP analyzed two months' worth of pre-filtered sexually-oriented email and found that 25 percent contained the "SEXUALLY-EXPLICIT: " label in the subject line. Confidential 6(b) response.

137. The FTC consulted with two DOJ units in the preparation of this section of the Report: the Civil Division's Office of Consumer Litigation ("OCL") and the Criminal Division's Child Exploitation and Obscenity Section ("CEOS"). To date, OCL has filed three civil suits and four civil settlements in federal court at the Commission's request; and CEOS has brought criminal charges against four individuals for sending allegedly obscene spam.

138. *See FTC v. Global Net Solutions,* No. CV-S-05-0002-PMP-LRL (D. Nev. filed Jan. 3, 2005).

139. *See FTC v. Cleverlink Trading*, No. 05C 2889 (N.D. Ill. filed May 16, 2005).

140. *See United States v. Impulse Media Group,* No. 05-CV1285 2:05-cv-01285-RSL (W.D. Wash.); *United States v. Cyberheat,* No. 4:05-cv-00457-DCB (D. Ariz.); *United States v. APC Entertainment, Inc.,* No. 05-CV-61194 (S.D. Fla.); *United States v. MD Media,* No. 2:05-cv-72836-JF-WC (E.D. Mich.); *United States v. BangBros.com,* No. 1:05cv21964 (S.D. Fla.); *United States v. Pure Marketing Solutions,* No. 8:05-cv-01353-RAL-EAJ (M.D. Fla.); and *United States v. TJ Web Productions,* No. 2:2005cv00882 (D. Nev.). All seven cases were filed in court on July 20, 2005. Additionally, ISPs have used CAN-SPAM as a tool to pursue senders of unlawful sexually-explicit email. Earthlink and Yahoo! have filed two civil lawsuits in this area, but did not allege violations of the ALR in those cases. *See* Appendices 5 through 7 regarding civil suits.

141. Pursuant to 15 U.S.C. § 56(a), in an action where the Commission seeks civil penalties, the FTC refers the case to DOJ, which proceeds with the litigation on behalf of the FTC with the United States as plaintiff.

CAN-SPAM or the ALR. In the three remaining cases still in litigation, the FTC through DOJ seeks, among other things, civil penalties and a permanent bar on the illegal spamming practices.

2. Criminal Enforcement by DOJ

In August 2005, DOJ announced its first criminal CAN-SPAM actions targeting senders of pornographic spam messages.[142] A grand jury in Arizona charged three individuals with criminal violations of the Act for allegedly sending spam advertising pornographic websites with obscene images embedded in the email messages.[143] Earlier, in February 2005, a fourth individual pled guilty to related criminal charges, including a CAN-SPAM count and conspiracy.[144]

3. Other Protections from Pornographic Email; Services Offered by ISPs and Commercially Available Products

Beyond CAN-SPAM's legal protections, ISPs offer their subscribers a variety of technological features to help safeguard consumers and children from pornographic material. Commercially-available software programs also may provide a line of defense against sexually-explicit spam.[145]

One of the most significant software features offered by ISPs is the ability to block certain images that may appear in email messages.[146] Many email programs[147] also offer this capability. Rather than embed an image directly in the body of an email message, email marketers typically host their images on a web

---

142. *See Three Defendants Indicted, Fourth Pleads Guilty in Takedown of Major International Spam Operation,* Aug. 25, 2005, DOJ press release available at http://www.usdoj.gov/criminal/press_room/press_releases/2005_4197_ereadattachment_Service.pdf. *See also* Appendix 1.A for a discussion of other criminal CAN-SPAM actions brought by DOJ.

143. *Id.*

144. *Id.*

145. As mentioned in section III.A.2 *supra*, OnGuard Online offers practical advice about computer safety, including ways to protect children while online. *See* http://www.onguardonline.gov.

146. Such image-blocking features have practical implications for email messages viewed in HTML-enabled email programs. An email message viewed in these programs can display a variety of content, such as images and links to other documents. Text-based email programs cannot display images so an image-blocking feature would be unnecessary.

147. This section uses the term "email programs" to refer to both "email clients" and web-based email programs. An "email client" is an application that runs on a personal computer or workstation that enables one to send, receive and organize email. Microsoft's Outlook, Mozilla's Thunderbird, and Eudora Mail are some examples of email clients. Web-based email programs, or "webmail," offer functions similar to email clients – although typically not as advanced – but are accessed via the Internet, and are often free to their subscribers. Yahoo! Mail, Google's GMail, and Microsoft's Hotmail are some examples of web-based email programs.

server.[148] When the recipient opens the message, the recipient's email program downloads the image from the web server so that it can be viewed within the email.[149] To prevent certain potentially offensive images from automatically downloading, ISPs and email programs use image-blocking software to interrupt this process; many do so specifically for messages that have been identified as spam.[150] Several sources with whom the Commission consulted regard image blocking as a very useful tool for consumers to protect themselves and their children from viewing pornographic, obscene, or otherwise unwelcome visual content in commercial email messages.[151]

In addition to image blocking, ISPs provide other technological options that specifically aim to protect children online. Many ISPs provide "parental controls" in their various email packages and allow parents to customize protection settings based on a child's age.[152] These parental controls facilitate blocking access to known pornographic websites and monitoring a child's online activity by maintaining lists of websites the child has visited.[153]

---

148. A web server is a computer that delivers (serves up) files. *See* Bishop Report, 23.

149. *See* Bishop Report, 23.

150. For example, Google and AOL state that some of their products disable images in email from unknown senders. Microsoft states that its Hotmail email program disables all images directed to a recipient's "junkmail" folder. Yahoo! offers its email users different levels of image blocking protection. Thunderbird, an open source email program, states that it blocks remote images by default unless the sender appears in the recipient's personal address book. *See* http://mail.google.com/support; http://discover.aol.com/product/spam.adp; http://join2.msn.com; http://antispam.yahoo.com/tools?tool=6; http://www.mozilla.org/projects/thunderbird/changes.html; Microsoft: Goodman, 40. *See also* AT&T: Barszcz: 40 (AT&T offers its subscribers image blocking as well). Microsoft's Outlook 2003 blocks images by default unless the sender appears on the recipient's "safe" list. *See* http://office.microsoft.com/en-us/assistance/HP010440221033.aspx.

151. Oregon: St Sauver, 44; Bigfoot: Della Penna, 54; Nortel: Lewis, 54; Microsoft: Goodman, 38. The Commission notes that image-blocking also can protect consumers from material that may not constitute "sexually explicit content" that is regulated by CAN-SPAM and the ALR, but nevertheless may be offensive or inappropriate for children. However, the typical image-blocking feature blocks all images, not just those that contain sexually-explicit content. This fact may implicate CAN-SPAM disclosure requirements, which are discussed in detail in Appendix 1 sections B.3 to B.5. To remain compliant with CAN-SPAM's requirement for conspicuous disclosures, marketers must ensure that all the mandatory CAN-SPAM disclosures are clear to recipients even with images disabled, such as by including disclosures in plain text, even when the image-blocking feature is turned on. *See also* Word to the Wise: Adkins, 55; Cantor – Comment D, 1 (expressing frustration with marketers who embed the required opt-out notice in an explicit image. Thus, in order to take advantage of the opt-out mechanism, the recipient must download the explicit image); LashBack – Comment D, 2 ("If the user has images disabled in their email client to protect [their] privacy or [if] the image fails to load, then the user has no way of knowing there is an unsubscribe option.").

152. *See, e.g.,* http://join.msn.com/?pgmarket=en-us&page=features/parental (MSN's parental controls); http://site.aol.com/info/parentcontrol.html (AOL's parental controls); http://www.earthlink.net/software/free/parentalcontrols/tour/control/ (Earthlink's parental controls).

153. *Id.*

Moreover, ISPs' general anti-spam tools can reduce the likelihood that consumers will receive sexually-explicit spam. Most ISPs offer a feature known as "whitelisting" in which an email program will accept email only from friends, known senders, and legitimate companies whose email addresses the subscriber has entered into the email program's address list.[154] Some of these whitelisting programs are specifically designed to protect children. For example, several ISPs allow parents to establish children's accounts so that email is received only from senders that their parents have approved.[155]

In addition to the tools offered by various ISPs, several commercially-available products can protect children from viewing pornographic material, whether in an email message or on a website. For example, ConsumerReports.org, an arm of Consumers Union, rates several Internet filters that block inappropriate content for children.[156]

Finally, parents' and guardians' vigilance provides some of the best protection for children online.[157] A Pew report, "Protecting Teens Online," found that 73 percent of online teens say their Internet computer is located in a public place inside the house. The report also found that 64 percent of parents of online teenagers say they set "house rules" about their children's online usage.[158]

4. State Initiatives Aimed at Protecting Children from Inappropriate Email

In recent months, two state laws became effective that aim to protect children from receiving various types of adult content, including pornographic email. The Michigan Children's Protection Registry Act[159] and the Utah Child Protection

---

154. Consumers appear to be taking advantage of whitelisting. A survey conducted by Bigfoot Interactive, an email marketing company, reported that over half of those surveyed always added legitimate senders to their address books. *Email and Spam: Consumer Attitudes and Behaviors*, Bigfoot Interactive, Feb. 2005. Similarly, DoubleClick reported that 85 percent of respondents have utilized the "Add to Address Book" function in email programs. DoubleClick 2005 Consumer Email Study, PowerPoint presentation, June 27, 2005 (on file with the FTC).

155. *See, e.g.,* http://join.msn.com/?pgmarket=en-us&page=features/parental; http://discover.aol.com/product/parental.adp and *Earthlink Premieres Parental Controls Software*, Sept. 30, 2003, Earthlink press release available at http://www.earthlink.net/about/press/pr_parentalcontrols/. *See also* Columbia: Bellovin, 49 (noting that whitelisting is the "simplest and best solution" for young children).

156. *See* http://www.consumerreports.org/main/content/display_report.jsp?FOLDER%3C%3Efolder_id=597365.

157. Pew: Fallows, 54; Digital Impact: Jalli, 63.

158. Amanda Lenhart, *Protecting Teens Online*, Pew Internet & Am. Life Project, Mar. 17, 2005.

159. Mich. Comp. Laws §§ 752.1061 - 752.1068.

Registry Law[160] establish child protection registries on which minors can register their electronic contact information.[161] The laws make it illegal to send prohibited adult content to children whose information is listed on the registries.[162] Similar legislation was considered in Illinois.[163]

The Commission generally supports initiatives that protect children from inappropriate content, but state registries that maintain sensitive information belonging to children raise troubling issues. The Commission has serious concerns about the security and privacy risks inherent in any type of do-not-email registry. In its report to Congress on the feasability of a national do-not-email registry, the FTC detailed these risks at length. Indeed, that report concluded that any registry "that earmarked particular email addresses as belonging to or used by children would raise very grave concerns. . . [and] the possibility that such a list could fall into the hands of the Internet's most dangerous users, including pedophiles, is truly chilling."[164] Although difficult to quantify, the risk of pedophiles or other dangerous persons misusing the registry data to discover the email address of a minor is certainly real. First, such a list could be misused by registry personnel. Second, such a list is subject to direct hacking by technologically sophisticated persons. Third, the operator of such a registry is unlikely to be able to screen every single individual who might seek, or to whom it might provide, registry access. Several sources with whom the Commission consulted on this Report raised similar security and privacy concerns.[165] Others

---

160. Utah Code Ann. §§ 13-39-102 - 13-39-304.

161. Under the laws, such information can include email addresses, telephone numbers, fax numbers, and instant messaging ("IM") identities.

162. The Michigan statute prohibits the sending of messages if the "primary purpose of the message is to, directly or indirectly, advertise or otherwise link to a message that advertises a product or service that a minor is prohibited by law from purchasing, viewing, possessing, participating in, or otherwise receiving." Mich. Comp. Laws § 752.1065(1). The Utah statute prohibits sending a communication that "(a) advertises a product or service that a minor is prohibited by law from purchasing; or (b) contains or advertises material that is harmful to children, as defined in Section 76-10-1201 [i.e., pornography]." Utah Code Ann. § 13-39-202.

163. H.B. 572, 94th Gen. Assem. (Ill. 2005). *See also* FTC Staff Comment to the Honorable Angelo "Skip" Saviano Concerning Illinois H.B. 0572 to Create a Child Protection Registry, available at http://www.ftc.gov/os/2005/11/051101cmtbill0572.pdf.

164. *See* http://www.ftc.gov/reports/dneregistry/report.pdf. In the year and a half since the Commission issued that report, there have been no technological advances that would alleviate the risk that pedophiles and spammers would misuse registry data. Bishop Report, 20-21.

165. ESPC: Hughes, 58; DMA: Cerasale, 59; and EFF: Newitz, 51-52.

suggested that these laws, if not expressly preempted by CAN-SPAM, certainly undermine the intent of CAN-SPAM's preemptive powers.[166]

5. Recommendations

Overall, since the enactment of CAN-SPAM, the email landscape has improved with regard to pornographic spam. Statistics show a decline in the amount of such spam that is being sent, and consumers report receiving less in their inboxes, likely due in part to improved blocking and filtering technology and vigorous enforcement of the ALR. Despite these improvements, the Commission recommends continued vigilance to ensure that consumers, especially children, are protected from pornographic spam. Specifically, the Commission has three recommendations, which, if adopted, will provide continued or increased protection for consumers from receipt and viewing of pornographic spam:

- continued vigorous enforcement of the civil and criminal provisions of CAN-SPAM and the ALR;
- passage of the US SAFE WEB Act[167] to strengthen the Commission's ability to pursue pornographic spammers who exploit international borders to evade prosecution; and
- redoubled efforts to educate consumers about available technologies to protect children from viewing sexually explicit spam.

In addition, the Commission would caution against legislative action on the state level to adopt registry-style laws in the hope they may effectuate improved protections for children in the online environment. The Commission believes that grave security and privacy concerns argue decisively against such measures.

---

166. EFF: Newitz, 51; Experian: Goodman, 59-60 (noting that CAN-SPAM preempted many disparate state laws and the implications of complying with multiple laws is impractical for legitimate senders). *See also* Appendix 1.E.2 for a complete discussion of the preemption provision.

167. The need for this legislation is discussed in detail in section III.B.3.a *supra*. We reiterate this recommendation here with respect to this specific type of spam.

IV. Conclusion: Summary of Findings and Recommendations

The CAN-SPAM Act has been effective in providing a roadmap for legitimate marketers to use in crafting their email campaigns. Compliance by legitimate online marketers is high, as discussed in detail in Appendix 1, and consumers and businesses benefit from having a set of best practices, articulated within the Act, adopted by legitimate emailers. The Act has also increased the ease or efficiency of enforcement against spammers. Yet, while recent trends indicate a decrease in the amount of spam reaching consumers' inboxes, spam is increasingly becoming a vehicle for identity theft (through phishing) and for the delivery of viruses and other forms of malware, such as spyware. As Congress found when enacting CAN-SPAM, the spam problem cannot be solved by legislation alone; technological approaches and international cooperation are key. The Commission has actively prodded industry to deploy domain-level authentication, and it should be in place in the near future. Finally, passage of the US SAFE WEB Act would enhance the ability of the FTC to combat illegal spam sent internationally.

Appendix 1: Analyses of CAN-SPAM's Substantive Provisions

Table of Contents

This Appendix contains the Commission's analyses of the substantive provisions of the CAN-SPAM Act, as mandated by Section 7709(a).[1] In preparing these analyses, FTC staff conferred with all of the federal and state entities granted enforcement authority under the Act. Staff also consulted with several major ISPs, which also are authorized to bring CAN-SPAM cases, as well as other interested parties.[2] The Commission finds that most of the substantive provisions of CAN-SPAM are being used in enforcement actions against unlawful spammers. Perhaps equally importantly, CAN-SPAM is serving an invaluable role in defining best practices for commercial emailers.

A. 15 U.S.C. § 7703 – Criminal Provisions of CAN-SPAM

15 U.S.C. § 7703 criminalizes five types of activities in connection with email, sets forth the maximum penalties for each type, and calls for the U.S. Sentencing Commission to consider new sentencing guidelines.[3] Because the Commission possesses only civil law enforcement authority, responsibility for enforcing CAN-SPAM's criminal provisions lies with the Department of Justice ("DOJ").[4] Therefore, much of the information in this section was provided by the Computer Crime and Intellectual Property Section within the Criminal Division of DOJ.[5]

---

1. In addition to the substantive provisions analyzed in this Appendix, the Act contains several sections which are either procedural in nature or the subject of other extensive reports to Congress by the FTC. These sections, not discussed in this Appendix, include: Section 1 – Short Title; Section 2 – Congressional Findings and Policy; Section 3 – Definitions; Section 9 – Do-Not-Email-Registry (a separate report to Congress was submitted addressing this section on June 16, 2004; *see* http://www.ftc.gov/reports/dneregistry/report.pdf); Section 11 – Improving Enforcement by Providing Rewards for Information about Violations; Labeling (the FTC has submitted two separate reports to Congress addressing this section: one on September 16, 2004, *see* http://www.ftc.gov/reports/rewardsys/040916rewardsysrpt.pdf; and one on June 16, 2005, *see* http://www.ftc.gov/reports/canspam05/050616canspamrpt.pdf); Section 13 – Regulations; Section 15 – Separability; and Section 16 – Effective Date.

2. For a detailed description of the parties and sources consulted in the preparation of the Report overall, *see* Report section II and Appendix 2.

3. 15 U.S.C. § 7704(d) contains the only other criminal provision in the Act, providing up to five years in prison for unlawful transmission of sexually-oriented spam. *See* Report section III.C.2.

4. DOJ has authority to enforce all of CAN-SPAM's criminal and civil provisions, except 15 U.S.C. § 7705 (civil seller liability).

5. The Commission also contacted the Federal Bureau of Investigation ("FBI") to consult on the drafting of this Report. FBI personnel did not respond with input before press time, due to demands associated with Hurricanes Katrina and Rita.

During the early months of CAN-SPAM, DOJ focused on two goals as it would with any new statute instituting criminal prohibitions: (1) ensuring that prosecutors and agents were well informed of the Act; and (2) initiating investigations into prohibited conduct. Having met these goals, DOJ now has brought four criminal prosecutions under 15 U.S.C. § 7703, and defendants in each of those cases have pled guilty.[6] Numerous other non-public investigations are ongoing.

1. 18 U.S.C. § 1037(a) – Substantive Criminalization

15 U.S.C. § 7703(a) criminalizes five activities that spammers have used to evade ISPs' anti-spam filters and avoid detection by law enforcement. Each of the following five activities constitutes a new crime under 18 U.S.C. § 1037(a).

a. 18 U.S.C. § 1037(a)(1) – Accessing a Protected Computer without Authorization to Send Multiple Commercial Email Messages

This provision criminalizes hacking into computers to send spam, including through the use of zombie drones.[7] To date, DOJ has completed three prosecutions under Section 1037(a)(1). First, in September 2004, Nicholas Tombros pled guilty in the Central District of California to a violation of this section, after admitting to sending spam through wireless home networks that had not been properly secured.[8] Second, in February 2005, in the District of Arizona, Andrew Ellifson pled guilty to a violation of this section, in addition to a conspiracy count, in connection with sending obscene spam.[9] Third, in June 2005 in the Northern District of Georgia, Peter Moshou also pled guilty to a violation of this section, after admitting accessing an ISP's computers without authorization in order to send spam promoting vacation timeshare services.[10]

---

6. As discussed in more detail below, guilty pleas have been obtained from Jason Smathers in the "AOL spammer" case, Nicholas Tombros in the "wi-fi spammer" case, and Peter Moshou in the "timeshare spammer" case. A fourth criminal prosecution in Arizona involving obscene spam and four individuals, one of whom has pled guilty to a CAN-SPAM count, is discussed in section III.C.2 of the Report.

7. *See* section III.A.2 of the Report and Appendix 3 for more information about zombie drones.

8. *See* http://www.usdoj.gov/usao/cac/pr2004/131.html. Tombros' sentencing has been postponed.

9. *See* Report section III.C.2. Ellifson's sentencing has been postponed.

10. Bill Montgomery, *Guilty Plea a Win for Spam Act,* Atlanta Journal-Constitution, July 1, 2005, at 4E. On November 17, 2005, Moshou was sentenced to 12 months in prison and was ordered to pay $120,000 in restitution.

DOJ believes that the three-year maximum penalty for violations of Section 1037(a)(1) has made Section 1037(a)(1) the most effective CAN-SPAM criminal provision to date.

b. 18 U.S.C. § 1037(a)(2) – Using Open Relays with Intent to Deceive in Sending Multiple Commercial Email Messages

This provision was primarily designed to protect consumers against spammers who use open relays and open proxies to disguise their identities.[11] DOJ has completed one prosecution under this paragraph of Section 1037. In February 2005, Jason Smathers, a former America Online ("AOL") employee, entered a plea of guilty to conspiracy to commit a violation of 18 U.S.C. § 1037(a)(2). Smathers admitted stealing a proprietary AOL database containing screen names and offering those screen names for sale to another individual who intended to send email through open relays and open proxies. Smathers was sentenced to 15 months imprisonment in August 2005.[12]

c. 18 U.S.C. § 1037(a)(3) – Using Materially False Header Information in Sending Multiple Commercial Email Messages

This paragraph criminalizes the insertion of materially false information into email headers,[13] which makes it more difficult for recipients and ISPs to distinguish legitimate email from spam. To date, there has been no prosecution solely under Section 1037(a)(3), although the prosecutions under Sections 1037(a)(1) and 1037(a)(2) have also involved instances of header falsification.

d. 18 U.S.C. § 1037(a)(4) – Falsely Registering Email Accounts or Domain Names in Connection with Sending Multiple Commercial Email Messages

This provision criminalizes email account "churning," a technique by which spammers send large quantities of spam from numerous email accounts or domains. By registering a large number of email accounts or domain names using false information, a spammer can

---

11. *See* Appendix 3 for more information about open relays and proxies.

12. *See* http://www.usdoj.gov/usao/nys/Press%20Releases/August%2005/Smathers%20Sentencing%20PR.pdf.

13. "Header information" is defined by the Act as "the source, destination, and routing information attached to an electronic mail message, including the domain name and originating electronic mail address, and any other information that appears in the line identifying, or purporting to identify, a person initiating the message." 15 U.S.C. § 7702(8).

send messages from one account after another, hiding the true source, size, and scope of the spammer's collective mailings. There has been no prosecution under Section 1037(a)(4) to date.

e. 18 U.S.C. § 1037(a)(5) – Falsely Claiming to be the Registrant of Internet Protocol Addresses for Sending Spam

This provision criminalizes a fraudulent technique used by spammers to obtain IP addresses not listed on spam "blacklists."[14] Using this technique, a spammer would identify blocks of IP addresses that had not been assigned, that had been assigned to a defunct company, or that belonged to an existing company (not affiliated with the spammer). The spammer would then contact the relevant IP registration authority to trick the registration authority into reassigning the address to the spammer. For example, the spammer might represent himself to be the entity actually assigned to the IP block, or a successor to that entity. By such false pretenses, the spammer gains control over IP addresses assigned to others. When the spammer sends messages from such an IP address, ISPs' filters might treat the spam as legitimate email. There has been no prosecution under Section 1037(a)(5) to date.

2. 18 U.S.C. § 1037(b) – Statutory Penalties

18 U.S.C. § 1037(b) contains statutory maximum penalties for violations of Section 1037's new criminal provisions. The penalties fall into three tiers.

First, a five-year statutory maximum applies when the CAN-SPAM violation is in furtherance of any felony under state or federal law, or when the defendant has been previously convicted of an offense under 18 U.S.C. § 1037.[15] This top penalty tier has not yet been applied in a case. Second, a three-year statutory maximum applies for convictions under either Section 1037(a)(1) or for convictions under Section 1037(a)(2)-(5) when one of several additional

---

14. *See* Judge Report, 6-8; Bishop Report 20-21. Blacklists are "lists of known spammers, their IP addresses, and/or their ISP (Internet service provider). Using this information, spam filters can block all messages coming from known spammers and/or their ISPs. ISPs that fail to discipline spammers may find all email from their legitimate customers blocked by large numbers of recipients. This tactic forces the ISP to take action against spammers using their systems because legitimate users do not want to be inconvenienced by having their email blocked." *See* CipherTrust glossary available at http://www.ciphertrust.com/resources/glossary/index.php?term=B.

15. A prior conviction under 18 U.S.C. § 1030 – a similar criminal section concerning fraud and related activity in connection with computers – may also lead to the five-year statutory maximum. 18 U.S.C. § 1037(b)(1)(B).

conditions applies. The conditions relate to measures of the economic gain or loss, the volume of email sent, the number of false registrations used, or whether the defendant had a leadership role in the offense. This has been the penalty tier applied in CAN-SPAM prosecutions completed to date. Finally, a one-year statutory maximum applies for any other violation of Section 1037. At this time, DOJ has not acquired sufficient experience with the application of these penalties to conclude that the penalties are either too lenient or too harsh.

3. 18 U.S.C. § 1037(c) – Asset Forfeiture

18 U.S.C. § 1037(c) enables DOJ to seek the criminal forfeiture of both property obtained from spamming profits and the computers used to send the spam. This provision protects consumers by helping to disgorge the ill-gotten gains of spamming. Forfeiture has not yet been litigated in criminal prosecutions under CAN-SPAM. DOJ believes that the ability to obtain the proceeds and instrumentalities of violations of Section 1037 is important; yet, it does not have enough data at this time to render a considered opinion on the long-term efficacy of the forfeiture provision of the statute.

4. 28 U.S.C. § 994 (note) – Sentencing Guidelines

15 U.S.C. § 7703(b) directs the U.S. Sentencing Commission to review and amend, as appropriate, the federal sentencing guidelines to provide proper penalties for violations of 18 U.S.C. § 1037. In particular, 15 U.S.C. § 7703(b)(2)(A)(i) proposes sentencing enhancements for address harvesting and dictionary attacks.

The Sentencing Guidelines revision applicable on November 1, 2004 implements this provision of CAN-SPAM. Defendants convicted under 18 U.S.C. § 1037 will have their sentences calculated under the main Fraud/Theft guideline section (USSG § 2B1.1) which increases penalties based upon the amount of loss suffered by the victim(s) of the offense. The Fraud/Theft section of the Guidelines recommends that individuals convicted under Section 1037 be given an increase in the base offense level for engaging in "mass-marketing." It also provides an additional enhancement to the recommended sentence if the Section 1037 offense involved "obtaining electronic mail addresses through improper means," which is defined as including

"the unauthorized harvesting of electronic mail addresses of users of a website, proprietary service, or other online public forum." Other sentencing enhancements (such as for using sophisticated means in the commission of the offense) may also apply depending on the facts of the particular case.

As with CAN-SPAM's statutory maximum penalties, DOJ does not yet have enough information to conclude that the Sentencing Guidelines are either too lenient or too harsh. DOJ does believe that the Sentencing Commission acted appropriately in treating CAN-SPAM under the Fraud/Theft guideline, and believes that the enhancements for particular conduct are appropriate. Finally, DOJ is still examining the effects of the Supreme Court's decision in *United States v. Booker*, which has given courts greater latitude to sentence defendants within the statutory range without mandatory application of the Sentencing Guidelines.[16]

5. 15 U.S.C. § 7703(c) – Sense of Congress to Use All Law Enforcement Tools

DOJ continues to use a number of its tools to address the problem of spam. Two recent cases provide illustrations. First, in March 2005, DOJ obtained a conviction of Anthony Greco in federal court in Los Angeles on one count of threatening to damage computers with the intent to extort.[17] Greco was charged with that violation, plus two others – including a violation of CAN-SPAM's criminal provision against unauthorized computer access, 18 U.S.C. § 1037(a)(1) – for sending waves of spam to an online messaging service. Greco had contacted the messaging service and sought employment, stating that if he were not hired he would share his instant message spam ("spim") techniques with other spammers; as a result, he indicated, the flood of spam might shut down the messaging service. Greco's sentencing has been postponed. While not a conviction strictly under CAN-SPAM, this case demonstrates DOJ's aggressive willingness to take on evolving spam threats, including the act of "spimming."

Second, in August 2005, a jury in Little Rock, Arkansas convicted Scott Levine of numerous federal law violations, including 120 counts of unauthorized access to computers. During 2002

16. ___ U.S. ___, 125 S. Ct. 738, 160 L. Ed. 2d 621 (2005).

17. *See* http://www.usdoj.gov/usao/cac/pr2005/050.html.

and 2003, acting with others, Levine, an officer of a company that sent commercial email on behalf of advertisers, hacked into the computer system of a major data management company. Together they stole over one billion records containing consumers' personal information, physical addresses, and email addresses in order to enhance his company's email and direct mail marketing lists. Although the criminal activity in this case preceded the enactment of CAN-SPAM, Levine's conviction demonstrates DOJ's continued commitment to protect against the theft and illegal use of consumers' personal information, including email addresses.

B. 15 U.S.C. § 7704 – Major Civil Provisions of CAN-SPAM

15 U.S.C. § 7704 contains numerous substantive civil provisions that can be enforced in federal court through lawsuits brought by certain federal agencies, including the FTC and DOJ, the state Attorneys General, and ISPs.[18] Sections B through E of this Appendix assess the effectiveness of each of the substantive civil provisions of the Act according to two factors: (1) whether the provision has served as a "best practices" model adopted by legitimate senders; and (2) whether the provision has increased the ease or efficiency of enforcement against spammers. Where either of these criteria is met, the Commission believes that a given substantive civil provision of CAN-SPAM is effective. These sections also summarize the significant enforcement actions taken by the FTC and other plaintiffs pursuant to 15 U.S.C. § 7704.

The Commission does not believe that CAN-SPAM's effectiveness can be determined by measuring changes in the amount or types of spam since the Act's passage because numerous variables, such as changes in anti-spam technologies and spammers' tactics, are predominantly responsible for such changes.[19]

---

18. Such plaintiffs have filed dozens of suits under 15 U.S.C. § 7704 against hundreds of known and "John Doe" defendants – both spammers who actually send email messages and those who hire them (sellers). Initial results of these cases are positive, as discussed in sections A through D of this Appendix.

19. *See* Bishop Report, 4.

1. 15 U.S.C. § 7704(a)(1) – Prohibition of False or Misleading Transmission Information

Section 7704(a)(1) prohibits false or misleading transmission information in email messages.[20] The prohibition on false or misleading header information is the only provision that applies equally to "commercial electronic mail messages" and to those messages deemed "transactional or relationship" under the Act.[21] Because this section outlaws a practice commonly used by spammers to conceal the true source of their messages, it is one of the most useful provisions in CAN-SPAM. Falsified headers make it difficult for recipients and law enforcers to identify the actual sender of a message and can impede ISPs' efforts to filter out such a message. It is not surprising, then, that violations of the false header provision have been alleged in the majority of civil CAN-SPAM enforcement actions brought to date. Twelve of the Commission's 20 CAN-SPAM cases have alleged the use of false or misleading headers.[22] Additionally, ten cases brought by various ISPs and two cases filed by state Attorneys General have alleged violations of this provision.[23] Enforcement actions alleging violations of the false header provision have targeted practices commonly used by spammers, including: (1) sending email messages with non-existent email addresses in the "from" lines;[24] (2) routing or relaying email messages through a third-party's computer;[25] and (3) "spoofing" or transmitting email messages that falsely indicate that the message originates from a third-party's server or email address.[26]

Most sources with whom the Commission consulted strongly supported the false or misleading header provision. One individual referred to it as "one of the most important

---

20. 15 U.S.C. § 7704(a)(1).

21. *Id.*

22. *See* Appendix 5.

23. *See* Appendices 6 and 7.

24. *See, e.g., FTC and State of California v. Optin Global,* No. C-05-1502 SC (N.D. Cal. filed Apr. 12, 2005).

25. *See, e.g., FTC v. Cleverlink Trading*, No. 05C 2889 (N.D. Ill. filed May 16, 2005).

26. *See, e.g., FTC v. Phoenix Avatar*, No. 04C 2897 (N.D. Ill. filed Apr. 23, 2004); *FTC v. Creaghan Harry*, No. 04C 4790 (N.D. Ill. filed July 21, 2004).

[provisions] in the Act" and another commented that it was a "wonderful, very simple hook to hang legal action on."[27] Similarly, two representatives from state Attorneys General offices noted that the false header provision has been extremely effective in law enforcement actions, and a provision that judges have clearly understood.[28]

Looking to the Commission's criteria for assessing the effectiveness of a provision,[29] the Commission finds that the false or misleading header provision has been effective. While Section 7704(a)(1) likely has had no effect on legitimate senders because they were not falsifying headers prior to CAN-SPAM, it has likely codified a best practice for legitimate marketers. Equally important, the false header provision created an express law violation for use by law enforcement where one did not previously exist. Falsified transmission information is often the calling card of spam that violates other provisions of CAN-SPAM or deceptively promotes a product or service.[30] Because legitimate senders have no reason to conceal their identities, it is generally only the truly bad actors that falsify headers. The new enforcement hook enables law enforcement easily to prove a law violation against a spammer who can be identified. Measures making it more difficult, or ideally, impossible, for senders to hide behind false or misleading headers would bolster the effectiveness of this provision. For instance, developing authentication technology and increasing awareness about computer vulnerabilities would contribute to the effectiveness and enforceability of the false or misleading header provision.

2. 15 U.S.C. § 7704 (a)(2) – Prohibition of Deceptive Subject Lines

Section 7704(a)(2) prohibits commercial email messages that contain deceptive or misleading subject lines.[31] Legitimate email marketers are complying with the deceptive

---

27. Bigfoot: Cohen, 66; Word to the Wise: Adkins, 65.

28. Massachusetts Office of Attorney General ("MAOAG"): Schafer, 41; California Office of Attorney General ("CAOAG"): Sweedler, 42.

29. *See supra* Section B (introduction).

30. IETF: Levine, 65.

31. 15 U.S.C. § 7704(a)(2).

subject line provision, as they are with other provisions of the Act.[32] Some sources with whom the Commission consulted noted that this provision is helpful to consumers because it outlaws a practice commonly used by spammers, and it provides a clear cause of action for law enforcement.[33] One interview participant noted that the deceptive subject line prohibition was a "fantastic provision" because it puts spammers in a "catch-22:" spammers can either use a non-deceptive subject line and risk having their messages remain unopened, or use a deceptive subject line and risk prosecution.[34]

Eight of the Commission's 20 CAN-SPAM cases have alleged violations of the deceptive subject header provision. Additionally, the vast majority of CAN-SPAM cases brought by state Attorneys General and ISPs have alleged violations of this provision. This provision has been charged in instances where the subject lines: (1) indicated, falsely, that the recipient had a prior relationship with the sender;[35] (2) indicated, falsely, that the message was from the recipient's ISP or contained time-sensitive information;[36] or (3) contained information that was in no way related to the message's content.[37]

Using the two measures of effectiveness noted above, the Commission finds that the deceptive subject line provision has been effective. This provision establishes a best practice by sending a clear signal to legitimate marketers that they must ensure that their subject lines are accurate and do not mislead recipients as to the content of their messages. As to improving anti-spam law enforcement, prior to CAN-SPAM's passage, the FTC attacked deceptive subject

---

32. Although not the focus of the published study by the FTC, a review of data gathered for the FTC Staff's Top Etailer study found that compliance with this provision among top etailers was nearly 100 percent.

33. *See, e.g.,* ESPC: Hughes, 66-67; CAOAG: Sweedler, 44-45; MAOAG: Schafer, 45; Texas Office of Attorney General: Schuelke, 45; TRUSTe: O'Malley, 24-25.

34. Microsoft: Goodman, 48. Others noted that this provision has not been effective. One academic commented that some subject lines may not be considered "deceptive" under the Act, but still confuse, confound, or obfuscate the intent of the message. Oregon: St Sauver, 67. Others noted that a violation of this provision was difficult to define because there is a fine line between what is simply a marketing tactic and what is considered misleading. Columbia: Bellovin, 68. *See also* Word to the Wise: Adkins, 67.

35. *See FTC and State of California v. Optin Global,* No. C-05-1502 SC (N.D. Cal. filed Apr. 12, 2005).

36. *See*, *e.g., FTC v. Global Web Promotions,* No. 04C 3022. (N.D. Ill. filed April 28, 2004).

37. *See*, *e.g., FTC v. Gregory Bryant,* No. 3:04-cv-897-J-32MMH (N.D. Ill. filed July 21, 2004).

lines under Section 5 of the FTC Act.[38] In this respect, the deceptive subject line provision has not provided the Commission with a new cause of action. The CAN-SPAM provision does, however, expose violators to civil penalties (or in state and ISP actions, to statutory damages) which provides a deterrent to illegitimate marketers.[39]

3. 15 U.S.C. §§ 7704(a)(3), 7704(a)(4), and 7704(a)(5)(A)(ii) – Opt-out Provisions

Three inter-related provisions in the Act provide consumers the right to opt out of receiving future commercial email from a particular sender. Section 7704(a)(5)(A)(ii) mandates that all commercial email messages include a notice of the recipient's opportunity to opt out of future commercial email messages from the sender. This provision ensures that recipients, regardless of whether they are otherwise aware of their opt-out rights under the CAN-SPAM Act, are informed of them in every commercial email message.

Second, Section 7704(a)(3) requires that commercial email messages contain a functioning return email address or other Internet-based mechanism that allows a recipient to submit a request not to receive future commercial email messages – in other words, to contain an opt-out mechanism.[40] The Act also specifies that an initiator of commercial email may comply with this

---

38. Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), prohibits deceptive acts in commerce. Deception occurs if there is a material representation, omission, or practice that is likely to mislead consumers acting reasonably under the circumstances. *See FTC v. Cliffdale Assocs.*, 103 F.T.C. 110, 165, *appeal dismissed sub nom., Koven v. FTC*, No. 84-5337 (11th Cir. 1984). *See, e.g., FTC v. Patrick Cella*, No. 03-3202 (C.D. Cal. filed May 7, 2003) (alleging that subject lines containing statements such as, "All members must read. Do not delete." were deceptive); *FTC v. Westby, et al.*, Case No. 03 C 2540 (N.D. Ill. filed Sept. 16, 2003) (alleging that subject lines containing statements such as "Fwd: You may want to reboot your computer" and "Did you hear the news?" were deceptive).

39. In an action alleging deception pursuant to Section 5(a) of the FTC Act, a federal court can use its equitable powers to order restitution or disgorgement. CAN-SPAM has added civil penalties to the Commission's arsenal in spam cases. 15 U.S.C. § 7706(a) (citing to Section 18(a)(1)(B) of the FTC Act, 15 U.S.C. § 57a(a)(1)(B), consequently treating CAN-SPAM violations as if they were violations of an FTC trade rule). Courts may award up to $11,000 per violation in civil penalty matters, regardless of consumers' economic losses. 15 U.S.C. § 45(m)(1)(A), as modified by 28 U.S.C. § 2461, as amended and as implemented by 16 C.F.R. § 1.98(d).

40. Section 7704(a)(3)(A) provides that: "It is unlawful for any person to initiate the transmission to a protected computer of a commercial electronic mail message that does not contain a functioning return electronic mail address or other Internet-based mechanism, clearly and conspicuously displayed that – (i) a recipient may use to submit, in a manner specified in the message, a reply electronic mail message or other form of Internet-based communication requesting not to receive future commercial electronic mail messages from the sender at the electronic mail address where the message was received; and (ii) remains capable of receiving such messages or communications for no less than 30 days after the transmission of the original message."

opt-out requirement by providing the recipient a list or menu from which to choose the specific types of messages the recipient does not wish to receive, provided such list or menu includes an option to allow the recipient to opt out of all future commercial email.[41] Section 5(a)(3)(C) provides a safe harbor for instances when a return email address or other mechanism is not working due to a technical problem beyond the control of the sender, provided that the sender corrects the problem within a reasonable period of time.[42] The purpose of this opt-out provision is to ensure that recipients actually have a means of effecting their choice not to receive future commercial email from any particular sender.

Third, Section 7704(a)(4) of the Act prohibits any person from initiating a commercial email message to a recipient who has previously opted out.[43] A sender, or one assisting a sender, has 10 business days to process an opt-out request; sending subsequent commercial email to one who has opted out after this grace period is unlawful.[44]

The FTC's recent study of top etailers' compliance with the opt-out provisions shows very high rates of compliance by such legitimate businesses.[45] One hundred percent of the etailers

---

41. Section 7704(a)(3)(B) provides that: "The person initiating a commercial electronic mail message may comply with subparagraph (A)(i) by providing the recipient a list or menu from which the recipient may choose the specific types of commercial electronic mail messages the recipient wants to receive or does not want to receive from the sender, if the list or menu includes an option under which the recipient may choose not to receive any commercial electronic mail from the sender."

42. Section 7704(a)(3)(C) provides that: "A return electronic mail address or other mechanism does not fail to satisfy the requirements of subparagraph (A) if it is unexpectedly and temporarily unable to receive messages or process requests due to a technical problem beyond the control of the sender if the problem is corrected within a reasonable time period."

43. 15 U.S.C. § 7704(a)(4)(i)-(iv) (prohibiting senders and persons acting on their behalf from initiating commercial email messages to those who have opted out, and prohibiting the sender or any other person who knows that the recipient has opted out from selling, leasing, exchanging, or otherwise transferring opt-out email addresses for any purpose other than compliance with the law).

44. The Act's 10-day time period for senders to honor a recipient's opt-out request is currently under review by the Commission, which has sought comments on a proposal to reduce the amount of time allowed to honor an opt-out request to 3 days. *See* 70 FR 25426 (May 12, 2005) available at http://www.ftc.gov/os/2005/05/05canspamregformfrn.pdf.

45. This is consistent with other reports of top etailer compliance since the passage of the Act. One study by EmailLabs published in January 2004 showed that compliance with this provision, even during the first month after CAN-SPAM was enacted, was 95 percent. Press release, "Confusion Reigns as Permission-Based Email Marketers Comply With Some Requirements of CAN-SPAM but Not Others," EmailLabs (Jan. 27, 2004), available at http://www.emaillabs.com/articles/news/CAN_SPAM_Compliance_audit.html.

surveyed included in their commercial email messages a notice of the recipient's opportunity to opt out of receiving such messages in the future, as well as a working opt-out mechanism.[46]

Regarding the final opt-out provision – the requirement that senders honor recipients' requests not to receive future commercial email – the FTC's Top Etailers study showed that 89 percent of etailers surveyed honored requests not to receive further email. Similarly high rates of compliance have been found by others studying this provision.[47]

On the other hand, reports since the passage of the Act suggest that, apart from the top etailers, overall compliance with all three opt-out provisions may be low. According to studies by MX Logic, an email defense solution provider that has tracked compliance since the passage of the Act, compliance with all provisions of the Act studied, including the inclusion of an opt-out mechanism, has fluctuated between a low of 0.54 percent in January 2004 and a high of seven percent in December 2004, with an average of three percent compliance overall.[48]

The Commission sought data regarding the percentage of recipients that avail themselves of the right to opt out. Data from before the passage of the Act showed that the great majority of consumers simply deleted or ignored unsolicited email from an unknown sender.[49] These

---

46. *See* Top Etailers' Compliance with CAN-SPAM's Opt-Out Provisions, a report by the FTC's Division of Marketing Practices, at 3 (July 2005), available at http://www.ftc.gov/reports/optout05/050801optoutetailersrpt.pdf. As noted in that study, a small percentage of top etailers' messages contained a very abbreviated notice of the right to opt-out, such as "Unsubscribe" or "Remove Me," which, in the view of FTC staff, would be minimally acceptable to provide adequate notice. Depending on the circumstances, the mere use of the terms "Remove Me," or "Unsubscribe," may not satisfy the clear and conspicuous notice requirements of sections 7704(a)(3)(A)(i) and (5)(A)(ii) of the Act. The better practice, in the view of staff, is to include a more complete explanation of the right to opt-out, such as "This email was sent to [email address of recipient]. If you would like not to receive further information about specials, please send us an email with the word 'Unsubscribe' in the subject line or click here [hyperlink to Internet-based opt-out mechanism] if you wish to unsubscribe." This compliance guidance was included in the Top Etailers study.

47. 2004 CAN-SPAM B2C Compliance Audit, Arial Software, 2004 at 3 (finding that only 1.8 percent of the more than 1000 top etailers studied ignored opt-out requests).

48. MX Logic reports data on CAN-SPAM compliance monthly. Data for the studies is culled from 10,000 randomly selected email messages reviewed each week. Compliance with individual provisions is not tracked, and the reported compliance rates indicate messages that complied with all of tracked provisions (valid physical postal address, opt out mechanism, non-deceptive subject line, and adult label). *See* http://www.mxlogic.com.

49. *Email and Spam: Consumer Attitudes and Behaviors,* Bigfoot Interactive, Nov. 2003, at 12 (showing that in a survey of adult computer users conducted in October 2003, 83 percent said that they would delete or ignore unsolicited email from an unknown sender, while only 4 percent would either use an unsubscribe link or reply feature).

data are borne out by some of those consulted for this Report, who expressed skepticism about recipients' willingness to use opt-out mechanisms, given the commonly-held belief that opting out merely signals to spammers that they have found a "live" address, and could therefore result in more spam.[50] None of those interviewed were able to provide any evidence that this is, in fact, the case, but clearly the perception persists that opting out leads to more spam. This perception remains despite previous FTC research suggesting that opting out does not result in the receipt of increased amounts of spam,[51] and the conclusion of experts that it is unlikely that tracking opt-out requests is an especially effective means for spammers to gather "live" addresses.[52]

One potentially troubling concern regarding the safety of opting out has come to light. Some reports in the media in late 2004 suggested that clicking on an opt-out link in an email may have even more dire consequences than receipt of more spam, such as the introduction of malware onto the computer of the individual opting out.[53] The Commission has sought data regarding such opt-out exploits from those it consulted with in preparation of this Report, as well as from the experts retained in preparation of this Report. In the view of those experts, while there is a risk of harm when using a web-based opt out link, there is little evidence to suggest any pattern of such abuse.[54]

---

50. *See, e.g.,* CAOAG: Sweedler, 50-51; MAOAG: Schafer, 51-52.

51. As part of its 2002 International Netforce initiative, the FTC and its law enforcement partners tested opt-out links in over 200 spam messages. The results showed that the vast majority of these mechanisms were inoperable, and that opting out did not lead to an increase in the amount of spam received. *See* http://www.ftc.gov/opa/2002/04/spam.htm.

52. *See* Judge Report, 7.

53. *See, e.g.,* Oregon: St Sauver, 14. Some reports of these opt-out exploits have been reported in the media. *See* "Can-Spam Mandated Opt-Out Link Can Lead to Infestation," Sept. 22, 2004, available at http://arstechnica.com/news.ars/post/20040922-4217.html ("According to Alex Shipp of security firm MessageLabs, clicking on the opt-out link in certain e-mails will forward the user to a website presumably set up by the authors of the e-mail bugaboo. Unpatched Internet Explorer users who scroll down to the bottom of the page looking for the unsubscribe link will instead be hit with the drag-and-drop exploit described in [a Microsoft Security Bulletin]); "Click Here to Become Infected," Sept. 22, 2004, available at http://www.theregister.co.uk/2004/09/22/opt-out_exploit/print.html ("MessageLabs is blocking spam linking to the domains www. xcelent.biz (space deliberately inserted) which, if users click on the remove link and scroll down the page triggers a DragDrop JavaScript exploit. This uses an IE bug to download and run an EXE file, currently being analyzed by MessageLabs."). FTC staff contacted MessageLabs in October 2005 and learned that the company has no further evidence of such opt-out exploits.

54. *See* Judge Report, 17-18.

The Commission has actively enforced the opt-out provisions of the Act. In 15 of the 20 cases brought to date by the FTC, the Commission has charged defendants with failing to include the required opt-out notice and failing to include a functional opt-out mechanism in their messages. The FTC has alleged violations for failure to honor opt-out requests as well, in two of the 20 cases.[55] States and ISPs have also enforced these provisions.[56]

Applying the effectiveness criteria described above, the Commission finds that the opt-out provisions have been effective. These provisions codify pre-existing "best practices" used by legitimate etailers and require their universal application. Studies of top etailers' compliance show that the vast majority provide notice to consumers of their right to opt-out, include an unsubscribe mechanism, and honor requests not to receive future commercial email messages. There remains a significant gap, however, between the practices of legitimate etailers and spammers. In instances where spammers do not comply, the opt-out provisions provide the FTC and others who enforce the Act with a method of penalizing spammers that is not present in other existing statutes.[57] Thus, the Commission believes that the opt-out provisions of CAN-SPAM have been effective.

4. 15 U.S.C. § 7704(a)(5)(A)(i) – Notice of Advertisement or Solicitation

Section 7704(a)(5)(A)(i) of the Act mandates that every commercial email message contain "clear and conspicuous identification that the message is an advertisement or solicitation."[58] The purpose of this requirement is to provide notice that a message is an advertisement or

---

55. *See* Appendix 5.

56. *See Massachusetts v. DC Enterprises* (Suffolk Superior Court filed June 30, 2004); *Massachusetts v. Kuvayev, et al.* (Suffolk Superior Court filed May 11, 2005); *FTC and State of California v. Optin Global,* No. C-05-1502 SC (N.D. Cal. filed Apr. 12, 2005). ISPs have also alleged violations of this provision. *See, e.g., Microsoft Corp. v. Lin, et al.*, (W.D. Wash. filed Mar. 9, 2004).

57. It is unlikely that the FTC could require that senders include an opt-out mechanism pursuant to the FTC Act. Prior to CAN-SPAM, the Commission had alleged violations of the FTC Act not for failure to include an opt-out, but in instances where a defendant made an opt-out representation, and then failed to honor it. *See, e.g., FTC v. G.M. Funding*, No. SACV 02-1026 DOC (C.D. Cal. filed Nov. 6, 2002). The Commission is not aware of any other law enforcement agencies that could require inclusion of an opt-out mechanism.

58. 15 U.S.C. § 7704(a)(5)(A)(i). This provision does not apply to messages sent to recipients who have given affirmative consent to receive email messages. 15 U.S.C. § 7704(a)(5)(B).

solicitation, which will signal to recipients that a message is commercial, presumably enabling them to determine quickly if they wish to read it or delete it.

The FTC has found little data about compliance with this provision by legitimate marketers. Tracking compliance with this provision is complicated by the fact that etailers who send email messages to recipients who have provided affirmative consent to receive such messages need not comply.[59] Thus, data – such as that from the FTC's Top Etailer study – based on email messages sent pursuant to such affirmative consent given by FTC staff in opting in to receive them – are not useful in providing statistics on mandatory compliance. A review of messages received in the Top Etailer study, though, shows that 97 percent of the messages surveyed included notice that the message was an advertisement.[60] Because these etailers are providing notice even where it is not required, the Commission believes that it may be fair to infer that where the notice is required, top etailers' compliance rates would be as high or higher.

Three of the Commission's 20 cases brought to date included allegations that defendants failed to include clear and conspicuous notice that their email messages were advertisements or solicitations.[61] In one of these cases, the defendants' email falsely represented that recipients had inquired about mortgage services, or had a prior relationship with the defendants, and failed to identify the email as an advertisement or solicitation.[62] In another case, the Commission charged defendants with several counts, including violation of this provision for sending email messages falsely informing consumers that their computers had been "scanned" and found to contain spyware, and directing them to websites for purportedly free software to fix the problem.[63] The

---

59. 15 U.S.C. § 7704(a)(5)(B).

60. A review of the messages shows that 19 percent of the messages contained an explicit notice stating that the message was an advertisement or solicitation; 78 percent clearly contained advertisements or contained language that mentioned an offer, sale, promotion or some other advertising language; and three percent did not include clear and conspicuous identification that the message was an advertisement. The Commission staff believes that the best practice is for advertisers to include an explicit notice, clearly and conspicuously displayed, that their email messages are advertisements or solicitations, when such is the case.

61. It is worth noting, however, that in each of the three cases alleging violations of this provision the Commission also alleged violations of 15 U.S.C. § 7704 (a)(1), the prohibition on false or misleading transmission information.

62. *See FTC and State of California v. Optin Global,* No. C-05-1502 SC (N.D. Cal. filed Apr. 12, 2005).

63. *See FTC v. Trustsoft,* No. H 05 1905 (S.D. Tex. filed May 31, 2005).

third case in which defendants were charged with violating this provision involved the deceptive sale of dietary supplements marketed through spam that failed to include the required advertising notice.[64] State Attorneys General and ISPs have also enforced this provision.[65]

Applying the effectiveness criteria, the Commission finds that this provision has been somewhat effective in codifying a "best practice" for legitimate email marketers.[66] To the extent commercial mail messages clearly announce themselves as such, recipients can more efficiently determine which messages they choose to spend time reviewing, and which they may choose to delete, thereby reducing wasted time and frustration. Thus, commercial email messages that clearly and conspicuously[67] are identified as advertisements or solicitations provide some value; however, spammers whose messages purport not to be advertisements are highly unlikely to disclose that their emails are advertising.

The identification of advertisement provision has been minimally helpful to the FTC and other enforcers in prosecuting spammers efficiently. In some cases, proving that the required identification is missing is relatively easy compared to proving that the claims made in the email are false or misleading. Thus, the Commission finds that this provision has also been somewhat effective in increasing the ease and efficiency of enforcement against spammers.

---

64. *See FTC v. Pacific Herbal Sciences,* No. CV05-7247 RSWL (C.D. Cal. filed Oct. 6, 2005).

65. In addition to the Optin Global case, brought jointly by the FTC and California, *see supra* note 62, Massachusetts has alleged violations of this provision in two actions brought in state court. *See Massachusetts v. DC Enterprises* (Suffolk Super. Ct. filed June 30, 2004) and *Massachusetts v. Kuvayev, et al.* (Suffolk Super. Ct. filed May 11, 2005). ISPs have also alleged violations of this provision. *See, e.g., EarthLink v. John Does 1 -25 (mortgage lead spammers) and EarthLink v. John Does 26 - 50 (prescription drug spammers)* (N.D. Ga. filed Oct. 27, 2004).

66. Some of those consulted in preparation for this Report expressed skepticism about the effectiveness of these provisions as applied to criminal spammers, who were unlikely to comply, but noted that even as applied to criminal spammers, the provision would allow for law enforcers to exact penalties for non-compliance. *See* Oregon: St Sauver, 73; Columbia: Bellovin, 73.

67. Information about how to make a "clear and conspicuous" disclosure on the Internet or in email is set forth in the Commission's publication "Dot Com Disclosures: Information About Online Advertising," available at http://www.ftc.gov/bcp/conline/pubs/buspubs/dotcom/index.html. While the disclosure must be evaluated in the context of the advertisement as a whole, factors to consider in determining whether the disclosure is "clear and conspicuous" include placement, prominence, and repetition.

5. 15 U.S.C. § 7704(a)(5)(A)(iii) – Valid Physical Postal Address

Section 7704(a)(5)(A)(iii) of the Act requires that every commercial email message include the valid physical postal address of the sender.[68] In theory, this provision should provide law enforcement with vital information – a ready means of contacting the sender of an email message. Because of the difficulty in identifying and locating defendants in spam cases, inclusion of this information theoretically would be a boon to law enforcement.[69]

Enforcement of this provision has been vigorous. Nearly all of the defendants against whom the FTC has brought suit under CAN-SPAM have failed to comply with this provision. In fact, in 18 of the 20 FTC cases brought to date, we have charged defendants with failing to list any address or listing bogus addresses.[70] States have also brought CAN-SPAM cases alleging violations of this provision, as have ISPs.[71]

---

68. 15 U.S.C. § 7704(a)(5)(A)(iii). This provision of the Act is currently under review in the extant NPRM in the Discretionary rulemaking. *See* Proposed Rule, § 316.2(p), 70 Fed. Reg. 25426, 25438 (May 12, 2005) (discussing the valid physical postal address provision). The Commission proposed an amended definition of the term "valid physical postal address," which clarifies that a sender may comply with this section of the Act by including in a commercial email message any of the following: (1) the sender's current street address; (2) a Post Office box the sender has registered with the United States Postal Service; or (3) a private mailbox the sender has registered with a commercial mail receiving agency ("CMRA") that is established pursuant to United States Postal Service regulations.

69. According to some, inclusion of a valid physical postal address of the sender may also serve as an indicator of legitimacy, demonstrating to recipients that the sender is complying with the law. Word to the Wise: Adkins, 81 (noting that whether a sender includes a valid physical postal address in a commercial email message is really a measure of "how closely they're paying attention to the CAN-SPAM requirement"). Concomitantly, when spammers fail to include a valid physical postal address in their messages, they flag their messages as unlawful and risk law enforcement action. DMA: Cerasale, 72-73. Some of those consulted in preparation for this Report suggest that the required valid physical postal address is also to be used as a means of notifying a sender that a recipient does not wish to receive future commercial email messages. Oregon: St Sauver, 71-72. The Act, however, does not permit this method of signaling the desire to opt out. Rather, the Act requires that each commercial email message contain a "functioning return electronic mail address or other Internet-based mechanism . . . that a recipient may use to submit, in a manner specified by the message, a reply electronic mail message or other form of Internet-based communication requesting not to receive future commercial electronic mail messages from that sender. . ." 15 U.S.C. § 7704(a)(3)(A)(i) (emphasis added).

70. *See* Appendices 5, 6, and 7 for a list of cases alleging a violation of this section. *E.g., FTC v. Global Net Solutions* (no address at all). The FTC cases alleging violations of this provision also allege other violations of CAN-SPAM.

71. State cases include: *FTC and State of California v. Optin Global,* No. C-05-1502 SC (N.D. Cal. filed Apr. 12, 2005) (no address for some messages; false address for others, determined with cooperation of US and Canadian authorities); and *Texas v. Ryan Pitylak* (W.D. Tex. filed Jan. 13, 2005) (address included is the valid physical postal address of a non-related entity). ISP cases include: *EarthLink v. Gregory Lars Alsing d/b/a Parcelship.com and Impression Media* (N.D. Ga. filed Jan. 18, 2005).

In the case of the valid physical postal address provision, as with the other substantive provisions of CAN-SPAM, there is a clear distinction between the Act as applied to legitimate actors and as applied to spammers. The wide disparity in compliance rates illustrates this point. A review of data collected by the FTC in conjunction with its Top Etailer study, published in August 2005, showed that 94 percent of messages sent by top etailers complied with the valid physical postal address provision.[72] Earlier surveys conducted by private organizations found lower rates of compliance by leading email marketers, but still found that a majority of those surveyed included their valid physical postal address in commercial email messages.[73]

The Commission found no reliable data on overall compliance rates – for all senders, not just top etailers – with the address requirement. The Commission notes, however, that spammers who seek to evade filters and law enforcement are highly unlikely to provide their true addresses in their spam.[74] Further efforts making it harder for spammers to operate anonymously, such as the development of authentication protocols, provide the greatest promise in enhancing overall compliance with this provision.

---

72. A sampling of the messages received from the 100 etailers studied shows that 94 percent included an address purporting to be that of the sender. The validity of the address was not tested for this purpose, so the compliance rate shows the rate at which senders included an address, not necessarily the rate at which they included a valid address.

73. *See supra* note 45 (citing to a survey by EmailLabs of top etailers' compliance with this provision in January 2004 which found that 56 percent of emails were compliant. It is not clear, however, from the published methodology that this survey distinguished between messages that would be deemed "commercial" under the Act and those that would be considered "transactional or relationship" messages. Because transactional messages are exempt from this provision, counting them for the study would mean that the compliance rate is artificially low. A surprising finding from the same study showed that, in contrast to the address provision figures, 87 percent of the messages studied offered an unsubscribe link, which, presumably, is a more burdensome provision with which to comply.) Also, in April 2004, JupiterResearch reported that 64 percent of leading email marketers complied with this provision; however, it is also difficult to assess the methodology used in this study. Press release, *JupiterResearch Finds Legitimate E-Mail Marketers Struggling With Federal CAN-SPAM Compliance* (Apr. 20, 2004), available at http://www.jupitermedia.com/corporate/releases/04.04.20-newjupresearch.html.

74. *See* "Impact of CAN-SPAM? Brightmail Finds Spam is Still Flowing," Feb. 2, 2004 ("There are certain provisions of the law – noting the sender's physical address in the message and including an opt-out mechanism – that Brightmail has seen in spam messages for years. Spammers include this information only to evade less sophisticated filters – the addresses they use are non-existent and their opt-outs are not legitimate.").

Applying the effectiveness criteria, the Commission finds that this provision likely has helped to codify a "best practice."[75] The valid physical postal address provision also may have a positive effect from the point of view of improved law enforcement.

6. 15 U.S.C. § 7704(b) – Aggravated Violations

15 U.S.C. § 7704(b) designates certain practices commonly used by spammers as aggravated violations. These practices, which include address "harvesting," "dictionary attacks," automated creation of multiple sender accounts, and computer hijacking, allow spammers to increase the volume of messages they can send. While the Act does not make engaging in one of these practices a *per se* law violation, 15 U.S.C. § 7704(b) does provide that any such activity becomes an additional law violation when committed in conjunction with an unlawful act or practice proscribed by 15 U.S.C. § 7704.

This provision has not yet been alleged by a federal or state plaintiff in federal court; however, ISPs have invoked it in at least a dozen private suits.[76] A court may award states or ISPs up to three times the damage award otherwise available if a spammer willfully violates this provision.[77] Applying the effectiveness criteria, however, the Commission finds that this provision has limited value.[78] First, legitimate marketers eschewed these practices even before CAN-SPAM. However, this provision may possibly serve to reign in those otherwise legitimate marketers who might have gravitated toward these aggressive tactics in the absence of legislative guidance to the contrary. Second, the trebling of damages has little, if any, effect on law

---

75. According to Trevor Hughes of the ESPC, this provision has not "caused undue pain or concern in the legitimate sending community," which views the inclusion of this information as a best practice. ESPC: Hughes, 72.

76. *See* Appendix 6.

77. 15 U.S.C. §§ 7706(f)(3)(C) and (g)(3)(c), respectively. CAN-SPAM does not permit treble damages for other enforcers, including the FTC. However, because Section 7704(d) creates an additional law violation that can be alleged by the FTC, it can, in effect, result in a doubling of the civil penalty sought by the FTC.

78. The improved effectiveness of some ISPs' anti-spam filters may be substantially lessening the impact of harvesting and dictionary attacks. The FTC staff's recent harvesting study noted that two major ISPs effectively filtered over 86 percent of spam sent to harvested addresses. *See* Report section III.A.2. To help reduce the incidence of harvesting and dictionary attacks, the Commission has consistently urged consumers to avoid displaying their email addresses in public places and to choose a unique address that is less susceptible to simple dictionary attacks. *See, e.g.,* FTC*, Putting a Lid on Deceptive Spam* at 2-3 (2002) (consumer education brochure), available at http://www.ftc.gov/bcp/conline/features/spam.pdf.

enforcement's or ISPs' ability to bring cases. The typical spam case involves thousands, and in some cases, millions, of violations of CAN-SPAM. Tripling an already astronomical potential monetary judgment has little value when most, if not all, defendants who would engage in these practices would not have the resources to pay the damage award even before it was tripled.

7. 15 U.S.C. § 7704(d) – Requirement to Place Warning Labels on Sexually-Explicit Commercial Email

15 U.S.C. § 7704(d) specifically addresses commercial email that contains sexually oriented material. Under this section, sexually oriented commercial email must: (1) contain a mark or notice in the message's subject line that alerts the recipient to the message's content;[79] (2) exclude from the initially-viewable area of the message any sexually oriented material; and (3) include in the initially-viewable area of the message only the required mark or notice, the sender's valid physical postal address, an opt-out mechanism, and instructions on how to access the sexually oriented material.[80]

Looking to the Commission's criteria for assessing the effectiveness of a provision, the Commission finds that this provision has been effective. First, this provision established a set of best practices for legitimate marketers to follow. Second, this provision created a new tool for law enforcement to pursue senders of sexually-explicit commercial email without having to show that the email message or underlying content constitutes a deceptive act or practice.

C. 15 U.S.C. § 7705 – Seller Liability

15 U.S.C. § 7705 makes it illegal for a seller to permit a spammer to promote the seller's goods or services through spam containing false headers if the seller: (1) knows or should have known in the ordinary course of business that the goods or services were being promoted through spam containing false headers; (2) received or expected to receive an economic benefit from

---

79. Pursuant to its mandate under Section 5(d)(3) of the CAN-SPAM Act, the Commission engaged in a rulemaking proceeding to establish the required mark or notice. The Commission prescribed the phrase "SEXUALLY-EXPLICIT: " to be included in the subject line and initially-viewable area of any commercial email containing sexually oriented material. The resulting rule, the "Adult Labeling Rule," ("ALR") took effect on May 19, 2004. 16 C.F.R. § 316.4. *See* Report section III.C.1 for a discussion of the enforcement of the ALR.

80. 15 U.S.C. § 7704(d)(1). These requirements do not apply if the recipient has given the sender "prior affirmative consent" for the receipt of such a message. *Id.* § 7704(d)(2).

such spam; and (3) took no reasonable action either to prevent the transmission of the spam or to detect the transmission and report it to the Commission. A third party who provides goods or services to such a seller, however, is not liable for violating this provision unless the third party: (1) owns or has a greater than 50 percent ownership or economic interest in the seller; (2) has actual knowledge that the goods or services are promoted by spam containing false headers; and (3) receives or expects to receive an economic benefit from such promotion. This provision may only be enforced by the FTC, and not by state Attorneys General or ISPs.

The goal of the provision was to permit the Commission to pursue sellers who received an economic benefit from spam containing false headers. According to CAN-SPAM's primary sponsors in the Senate, Senators Burns and Wyden, "[15 U.S.C. § 7705] does not require any showing that the merchant actually hired or induced the spammer to send spam. . . [I]f the spammer is hard to find and his contractual relationship with the merchant has been obscured by under-the-table dealings, the FTC doesn't have to spend time and effort trying to prove the relationship."[81]

Applying the Commission's criteria for assessing the effectiveness of a CAN-SPAM provision, the Commission sees little evidence that the provision has established a set of best practices for sellers. The Commission reaches this conclusion because the provision only imposes liability on those sellers who knew or should have known that their products were being promoted by spam with false headers and who "took no reasonable action" to prevent the transmission of the spam or to detect it and report it to the Commission. This is problematic in two respects: first, sellers who know that their products are being promoted by spam violating other provisions of the law (such as spam containing no opt-out mechanism or a false or misleading subject line) remain unaffected by this provision. Second, the parameters of what might constitute "reasonable action to prevent the transmission" sufficient to exonerate a seller remain untested. It is worth noting, however, that, in the two years since CAN-SPAM's

81. 149 Cong. Rec. S15945 (daily ed. Nov. 25, 2003).

enactment, we are unaware of even a single seller informing the Commission that it has detected spam with false headers advertising its products or services.

Applying the second effectiveness criteria, the Commission has not brought any cases alleging a violation of this section because it would come into play in a very narrow set of circumstances, none of which have presented themselves in the two years since CAN-SPAM's enactment. First, the provision would apply when the Commission could prove that the seller knew or should have known that its goods or services were being promoted by spam containing false headers. This knowledge requirement creates a significant evidentiary burden. A spammer is unlikely to inform a seller that it will be using spam containing false headers to promote the seller's goods or services. Second, this provision requires the Commission to prove that the seller received or expected to receive an economic benefit from spam containing false headers. And, third, in many instances, the Commission may have difficulty in proving that the seller took no reasonable action to prevent the transmission of the spam.[82]

Nonetheless, the Commission has vigorously pursued sellers of products being promoted by illegal spam pursuant to 15 U.S.C. § 7704 by charging the sellers as "initiators" of the spam. Under 18 U.S.C. § 7704(a), an initiator – a person who originates or transmits the spam or procures its initiation or transmission – is liable for illegal spam. In most instances, CAN-SPAM's broad definition of "initiate" enables the Commission to pursue sellers who have caused spam to be sent to consumers.

D. 15 U.S.C. § 7706 – Civil Enforcement

15 U.S.C. § 7706 empowers the FTC and various other federal agencies, state law enforcement agencies, and ISPs, to bring suit in federal court against spammers who violate the

82. The section's exemption from liability for third parties who provide goods or services to a seller imposes additional evidentiary burdens on the Commission. If a seller were to create a straw middleman through which it entered into contracts with the spammer, the Commission would need to demonstrate that the seller owned more than 50 percent of the straw middleman or had actual knowledge that the spammer would be sending spam containing false headers.

civil provisions of the Act.[83] The FTC has brought 20 civil cases against a total of 64 known defendants, including ten cases against defendants responsible for sexually-explicit spam.[84] In its actions under CAN-SPAM, the Commission may seek civil penalties and equitable relief, such as injunctions, disgorgement, and consumer redress.[85]

In four of the FTC's CAN-SPAM cases involving sexually-explicit email, the Commission has obtained settlements totaling $1.159 million in civil penalties, barring defendants from violating the Act, and requiring defendants to monitor their affiliates to ensure they are not violating the law.[86] To date, the Commission also has successfully concluded four other CAN-SPAM matters, obtaining permanent injunctions and redress.[87]

At the state level, three Attorneys General have filed a total of three actions – one with the FTC as co-plaintiff – in federal court naming 15 defendants pursuant to the Act.[88] State

---

83. In addition to the FTC and DOJ, federal entities with enforcement authority under the Act are the FCC, the Office of the Comptroller of the Currency, the Federal Reserve Board, the Federal Deposit Insurance Commission, the Office of Thrift Supervision, the National Credit Union Administration, the Securities and Exchange Commission, the Department of Transportation, the Department of Agriculture, and the Farm Credit Administration. 15 U.S.C. § 7706(b). CAN-SPAM also grants enforcement authority to ISPs, state Attorneys General, and state insurance commissioners. 15 U.S.C. §§ 7706(g), (f), and (b)(6), respectively.

84. *See* Appendix 5. In seven of those 20 cases, the Commission sought civil penalties in addition to other equitable relief for CAN-SPAM violations. The Office of Consumer Litigation, working with the U.S. Attorney's Offices in the various districts, filed the cases pursuant to DOJ's authority to seek civil penalties as a remedy on behalf of the Commission. 15 U.S.C. § 56(a). The Commission is aware of no federal entity, other than the FTC and DOJ, that has initiated a civil action under CAN-SPAM.

85. 15 U.S.C. §§ 7706(a) and (d). The other federal agencies with civil enforcement authority under the Act may seek remedies provided by their own statutory grants. 15 U.S.C. § 7706(c). Senate Comm. on Commerce, Science. and Transp., Rep. on the CAN-SPAM Act of 2003, S. Rep. No. 108-102, at 20-21 (2003).

86. *See* http://www.ftc.gov/opa/2005/07/alrsweep.htm.

87. *FTC v. Phoenix Avatar,* No. 04C 2897 (N.D. Ill. judgment entered Mar. 29, 2005) (settlement of $15,000 and suspended judgment of $230,000); *FTC v. Global Web Promotions*, No. 04C 3022 (N.D. Ill. judgment entered June 16, 2005) (default judgment including $2.2 million in consumer redress); *FTC v. Creaghan Harry,* No. 04C 4790 (N.D. Ill. judgment entered May 5, 2005) (settlement of $485,000, with $215,000 payable immediately, and suspended judgment of $5.9 million in consumer redress); *FTC v. Global Net Solutions*, No. CV-S-05-0002 (D. Nev. orders of Aug. 4 and Sept. 8, 2005) (judgments totaling $700,018 in disgorgement).

88. *See* Appendix 7. The Commission is not aware of any action under the Act filed by a state insurance commissioner.

enforcement entities and ISPs may seek injunctions and damages, including statutory damages, for violations of the Act.[89] The state cases remain in litigation.

ISPs have also filed CAN-SPAM suits initially against more than 100 known defendants and more than 580 unknown (John Doe) defendants.[90] Most of these cases are still in litigation, but some have settled.[91]

In assessing the effectiveness of this section of the Act, the Commission notes the inapplicability of the first effectiveness criterion. This section imposes no obligations on email marketers. Turning to the second criterion, the Commission finds that this section has been effective because it has provided the FTC and other federal agencies, state Attorneys General, and ISPs with useful new tools in the fight against spam.

E. 15 U.S.C. § 7707 – Preemption

Section 7707 of CAN-SPAM deals with the effect of the Act on other federal and state laws, as well as on the policies of Internet access service providers.[92] These provisions are discussed in turn, below.

1. Federal Law

Section 7707(a)(1) of the Act clarifies that CAN-SPAM does not limit the ability of the FCC to enforce certain sections of the Communications Act or of DOJ to enforce a variety of

89. The maximum per-violation statutory damage figures are $250 for state Attorneys General and $100 for ISPs; however, where certain techniques were used to send the spam, such as address harvesting, dictionary attacks and hacking, the statutory damages may be tripled. 15 U.S.C. §§ 7706(f)(3) (for states) and (g)(3) (for ISPs) (both referencing the aggravated violations of 15 U.S.C. § 7704(b)). One commenter with the State of California told the Commission that CAN-SPAM could be improved for state enforcers by changing the legal remedy of "damages" to "penalties." CAOAG: Sweedler, 62 ("[the mere] receipt of spam doesn't cause substantial economic damage to the individual consumer") (emphasis added).

90. *See* Appendix 6. The FTC conducted an extensive literature review and contacted major ISPs in compiling these data. These figures represent collective litigation data as of September 1, 2005.

91. For example, Microsoft obtained a $7 million settlement against defendant Scott Richter, and AOL received a $13 million judgment against Braden Bourneval and Davis Wolfgang Hawke. *See* Elizabeth M. Gillespie, *Microsoft Receives $7M in Spam Settlement,* Associated Press, Aug. 9, 2005, and Mike Musgrove, *AOL Wins Judgment Against Spammers,* The Washington Post, Aug. 11, 2005, at D5.

92. *See* Report note 2.

criminal laws.[93] In our consultations with the FCC and DOJ, neither raised concerns regarding this provision, nor did any other sources the Commission consulted with in preparation for this Report.

Section 7707(a)(2) of the Act clarifies that the FTC may continue to bring spam cases under the FTC Act.[94] Of the 20 cases that the Commission has brought against spammers since the passage of the CAN-SPAM Act, nine have alleged violations of both the FTC Act and the CAN-SPAM Act. The Commission determines on a case-by-case basis whether to plead violations of the CAN-SPAM Act, the FTC Act, or both.

In assessing the effectiveness of this provision, the Commission notes the inapplicability of the first criterion. As to the second factor, the Commission views this provision as effective because it preserves the ability of federal agencies to determine the most efficient means of pursuing spammers.

2. State Law

Pursuant to Section 7707(b) of the Act, state laws that expressly regulate commercial email messages are preempted by CAN-SPAM, except "to the extent that any such statute, regulation, or rule prohibits falsity or deception in any portion of a commercial email message or information attached thereto."[95] The Act does not, however, preempt state laws that are not specific to email such as trespass, contract or tort law, or other state laws to the extent those laws relate to acts of fraud or computer crime.

This provision was the subject of considerable discussion by the parties consulted in preparation for this Report. Some parties criticized the preemption provision as unnecessarily

---

93. "Nothing in this Act shall be construed to impair the enforcement of section 223 or 231 of the Communications Act of 1934 (47 U.S.C. 223 or 21, respectively), chapter 71 (relating to obscenity) or 110 (relating to sexual exploitation of children) of title 18, United States Code, or any other Federal criminal statute." *Id.* § 7707(a)(1).

94. "Nothing in this Act shall be construed to affect in any way the Commission's authority to bring enforcement actions under the FTC Act for materially false or deceptive representations or unfair practices in commercial electronic mail messages." *Id.* § 7707(a)(2).

95. In full, the section states: "This Act supersedes any statute, regulation, or rule of a State or political subdivision of a State that expressly regulates the use of electronic mail to send commercial messages, except to the extent that any such statute, regulation, or rule prohibits falsity or deception in any portion of a commercial electronic mail message or information attached thereto." 15 U.S.C. § 7707(b).

limiting the avenues that states might use in pursuing spammers. For example, a representative of the California Attorney General's Office expressed the view that preemption of state laws that were consistent with CAN-SPAM harmed state law enforcement efforts because it prevented states from seeking additional remedies that would be available under state law.[96] Privacy advocates also spoke out against the provision, noting the states "have been faster to react to new consumer protection problems than the federal government has."[97] Other interview participants, though, supported the preemption provision, noting the importance of having a single federal standard for legitimate companies to follow in executing their email campaigns.[98] According to the Email Service Provider Coalition, the preemption provision is "one of the most important things that the CAN-SPAM Act did," because it "created a common platform for legitimate businesses to understand what was onside and what was offside with regards to commercial email."[99]

---

96. CAOAG: Sweedler, 69-70 (noting that state penalty remedies "are more reasonably obtainable through prosecution . . ."). The representative further noted that state laws often contain a right of private action, as well, which would enable individual recipients to enforce the laws. CAOAG: Sweedler, 70-71. Some of those consulted in preparation of this Report agreed that a private right of action would increase enforcement of the Act and benefit recipients who would aggressively pursue their legal rights. *See, e.g.,* Oregon: St Sauver, 74. Still others disagree. *See, e.g.*, Columbia: Bellovin, 74 (agreeing that a private right of action would be of little practical use because individuals would not have the resources, in most instances, to identify and track spammers). In addition, at hearings held on the operation of the CAN-SPAM Act in May 2004, Senator McCain expressed skepticism about the value of a private right of action. *See* CAN-SPAM Act: Hearing Before the Senate Comm. on Commerce, Science and Transp., 108th Cong., 2d Sess. (2004) ("I do not believe, however, that authorizing broad private rights of action will improve enforcement efforts. If industry and government authorities spending vast resources in this effort can only muster enough evidence to bring a grand total of 8 spam cases over the past 5 months, then private rights of action will produce little more than expenses for legitimate businesses to fend off opportunistic trial lawyers. Spammers will remain at large.").

97. EPIC: Hoofnagle, 64. *See also* Oregon: St Sauver, 83-84 (questioning whether uniformity in a domestic legal scheme regulating email is necessary given the international nature of the medium and the multitude of international laws and regulations with which marketers already must be comply).

98. Columbia: Bellovin, 83 ("[T]o the extent that there is legitimate email advertising going on, and there certainly is some of that by reputable companies, that's where preemption is good because then they only have to comply with one set of rules."). Professor Bellovin went on to suggest that, ideally, state laws would only be preempted with regard to those legitimate firms in compliance with CAN-SPAM, as a sort of safe harbor, leaving states free to pursue bad actors under their own laws as well as CAN-SPAM. *Id.*

99. ESPC: Hughes, 75. *See also* DMA: Cerasale, 78-79. *But see* EPIC: Hoofnagle, 65 (expressing skepticism that companies that can use "sophisticated profiling systems, that can in fact profile people down to the ZIP+4 level" cannot use similarly sophisticated technology to comply with a myriad of state email marketing laws).

One interview participant not only praised the preemption provision, but argued that it may need to be strengthened to prevent attempts, such as the child do-not-email registries adopted by the legislatures of Utah and Michigan[100] to "create criminal violations as a means to try to get around the CAN-SPAM Act."[101] Another noted that, within the bounds of the preemption exception set forth in CAN-SPAM, state laws aimed at fraud and deception are welcome as an additional means of spam enforcement.[102]

The Commission believes that the preemption provision has been effective in creating a single regulatory scheme for businesses to adhere to when conducting national email marketing campaigns.

3. Internet Access Service Providers

Section 7707(c) of the Act states that: "[n]othing in th[e] Act shall be construed to have any effect on the lawfulness or unlawfulness, under any other provision of law, of the adoption, implementation, or enforcement by a provider of Internet access service of a policy of declining to transmit, route, relay, handle, or store certain types of electronic mail messages." No one interviewed for this Report raised concerns regarding this section. Nor was it a topic raised by ISPs in response to the Commission's Section 6(b) orders. This provision, however, was the focus of recent litigation. In an August 2005 ruling, the United States Court of Appeals for the Fifth Circuit held that the University of Texas ("UT") lawfully filtered email messages from an online dating service sent to recipients on the UT servers. According to the Court, although UT was a state entity, it was acting as an Internet access provider. UT's filtering of email therefore was permissible under § 7707(c), which provides that CAN-SPAM does not affect an Internet

100. *See* Report section III.C.4.

101. *See* DMA: Cerasale, 77-79.

102. *See* ESPC: Hughes, 75-76 (noting that the Virginia anti-spam statute, in particular, has been a positive example of a state law that supplements CAN-SPAM).

access provider's anti-spam policies.[103] Turning to the effectiveness criteria, the Commission believes that this provision is effective in enabling those who provide Internet access service to set their own filtering policies independently, without interference from the operation of the Act.

F. 15 U.S.C. § 7712 – Application to Wireless

15 U.S.C. § 7712 directs the FCC to promulgate a rule to protect consumers from unwanted mobile service commercial messages. After a public comment period, the FCC's final rule was announced in September 2004,[104] and it became fully effective in March 2005. This rule has two primary effects: (1) the creation of a publicly-available list of Internet domain names exclusively associated with wireless services; and (2) a general prohibition on sending spam to an address at any such domain.[105]

Consulting with the FCC during the preparation of this Report, the FTC learned that the FCC has conducted outreach to wireless carriers to ensure that the list of domain names is as accurate as possible. The FCC has also endeavored to educate consumers about the new rule through speeches, press releases, and a wireless-spam fact sheet available on its website. The FCC reports that, since the beginning of enforcement in March 2005, it has not received significant numbers of consumer complaints alleging violations of the rule. As a result, the

---

103. 15 U.S.C. § 7707(c). *See White Buffalo Ventures, LLC v. University of Tex. at Austin*, m 04-50362 (Aug. 2, 2005) (finding that while UT was a state subdivision, and thus arguably subject to the Act's preemption provision, § 7707(b)(1), the university also clearly met the Act's definition of a provider of "Internet access service," and was thus entitled to set its own filtering policies).

104. FCC Order 04-194, adopted Aug. 4, 2004, available at http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-04-194A1.pdf, published at 69 Fed. Reg. 55765 (Sept. 16, 2004).

105. The first posting of the wireless domain names list on the FCC website occurred on February 7, 2005, thirty days before the start of enforcement. FCC Notice DA05-331, available at http://hraunfoss.fcc.gov/edocs_public/attachmatch/DA-05-331A1.pdf. The list may be viewed at http://www.fcc.gov/cgb/policy/DomainNameDownload.html.

agency has taken no enforcement action thus far, but it stands ready to take action against any entity once its violations become apparent.[106]

106. The FCC's unique statutory enforcement scheme – involving notice of unlawful conduct – could impact the agency's ability to enforce violations of this new rule effectively. Under the Communications Act, if a violator is not an FCC licensee, the agency must first issue a warning citation before it can issue a monetary forfeiture penalty. 47 U.S.C. § 503(b)(5). CAN-SPAM violators typically are not FCC license holders; thus, the statutory citation requirement is likely to be triggered in many FCC CAN-SPAM enforcement cases.

Appendix 2: List of Interviews

Name (Last, First)	Organization	Date of Interview
Addicott, Kimberly	Verizon	7/27/2005
Adkins, Steve	Word to the Wise	7/26/2005
Alonzo, Mercedes	Connecticut Office of Attorney General	7/14/2005
Archie, Jennifer	AOL	7/27/2005
Baer, Josh	SKYLIST and UnsubCentral LLC	7/27/2005
Barszcz, Jim	AT&T	7/27/2005
Bays, Julie	Oklahoma Office of Attorney General	7/14/2005
Bellovin, Steve	Columbia University	7/21/2005
Berkower, Elise	DoubleClick	7/27/2005
Bolton, Barbara	Federal Trade Commission	7/14/2005
Borenstein, Nathaniel	IBM	7/28/2005
Bowles, Elizabeth	Aristotle.net	7/27/2005
Brady, Betsy	Microsoft Corporation	7/27/2005
Castelli, Eric	LashBack LLC	7/26/2005
Cerasale, Jerry	Direct Marketing Association (DMA)	7/27/2005
Chavez, Esther	Texas Office of Attorney General	7/14/2005
Clocker, Kimberly	Verizon	7/27/2005
Cohen, Jordan	Bigfoot Interactive	7/26/2005
Cohen, Stephen	Federal Trade Commission	7/14/2005
Colclasure, Sheila	Acxiom Corporation	7/28/2005
Coleman, Sana	Federal Trade Commission	7/14/2005
Collier, Lloyd	Federal Communications Commission	7/14/2005
Dailey, Thomas	Verizon	7/27/2005
DeGraff, Kenneth	Consumers Union	7/26/2005
Della Penna, Michael	Bigfoot Interactive	7/26/2005
Devlin, Brian	Michigan Office of Attorney General	7/14/2005
Edelman, Ben	Harvard University	7/21/2005
Everett-Church, Ray	PrivacyClue LLC	7/20/2005
Fallows, Deborah	Pew Internet & American Life Project	7/20/2005
Fisher, Ashley	Arkansas Office of Attorney General	7/14/2005
Fox, Jean Ann	Consumer Federation of America	7/26/2005
Free, Peter	Wyoming Office of Attorney General	7/14/2005
Gasster, Liz	AT&T	7/27/2005

Name (Last, First)	Organization	Date of Interview
Gerdes, Michael	Pennsylvania Office of Attorney General	7/14/2005
Goodman, Joshua	Microsoft Corporation	7/27/2005
Grant, Susan	National Consumers League	7/26/2005
Hadeishi, Hajime	Federal Trade Commission	7/26/05; 7/27/05
Hadley, Tony	Experian	7/27/2005
Hagan, Deborah	Illinois Office of Attorney General	7/14/2005
Halpert, Jim	Internet Commerce Coalition	7/27/2005
Hawes, Gary	Connecticut Office of Attorney General	7/14/2005
Hedges, Chris	West Virginia Office of Attorney General	7/14/2005
Hochberg, Jane	Idaho Office of Attorney General	7/14/2005
Hodapp, Larry	Federal Trade Commission	7/14/2005
Hoofnagle, Chris	Electronic Privacy Information Coalition (EPIC)	7/20/2005
Hughes, Trevor	Email Service Provider Coalition (ESPC)	7/27/2005
Ingis, Stuart (Stu)	AOL Time Warner (Piper Rudnick for)	7/27/2005
Ingles, Sherry	Wisconsin Office of Attorney General	7/14/2005
Isaacson, Ben	Experian	7/27/2005
Jacobsen, Jennifer	AOL Time Warner	7/27/2005
Jaglowski, Mary	State of Connecticut	7/14/2005
Jalli, Quinn	Digital Impact	7/27/2005
Jansen, Mark	Montana Department of Justice	7/14/2005
Kornblum, Aaron	Microsoft Corporation	7/27/2005
Leuer, Jennifer	Experian	7/27/2005
Levine, John	Internet Engineering Task Force (IETF), Anti-Spam Research Group (ASRG)	7/26/2005
Levy, Leslie	Nebraska Office of Attorney General	7/14/2005
Lewis, Chris	Nortel Networks	7/26/2005
Lieb, Rebecca	ClickZ Network	7/26/2005
Litwin, Hedda	National Association of Attorneys General	7/14/2005
Malmerg, Kristin	Federal Trade Commission	7/14/2005
Mansourkia, Magnolia (Maggie)	MCI	7/27/2005
Matties, Deborah	Federal Trade Commission	7/14/2005
McClellan, Bill	Electronic Retailing Association	7/28/2005
McDonald, Susan	Federal Trade Commission	7/14/2005
McEldowney, Ken	Consumer Action	7/26/2005

Name (Last, First)	Organization	Date of Interview
Meyer, Jennifer	Illinois Office of Attorney General	7/14/2005
Miller, Jay	Federal Trade Commission	7/14/2005
Moriyama, Michael	Hawaii Department of Commerce and Consumer Affairs	7/14/2005
Neumon, John	Connecticut Office of Attorney General	7/14/2005
Newitz, Annalee	Electronic Frontier Foundation (EFF)	7/20/2005
O'Malley, Colin	TRUSTe	7/28/2005
Osburn, Alice	General Motors	7/28/2005
Petroff, Jim	Ohio Office of Attorney General	7/14/2005
Roberts, Lee Ann	Tennessee Office of Attorney General	7/14/2005
Rohlich, Nelle	Wisconsin Office of Attorney General	7/14/2005
Saulnier, Julie	Federal Communications Commission	7/14/2005
Schafer, Scott	Massachusetts Office of Attorney General	7/14/2005
Schuelke, Brad	Texas Office of Attorney General	7/14/2005
Selis, Paula	Washington Office of Attorney General	7/14/2005
Sherry, Linda	Consumer Action	7/26/2005
Shull, Andrew	Oregon Department of Justice	7/14/2005
Silversin, Louis	Federal Trade Commission	7/26/05; 7/28/05
Singh, Tony	Department of Justice	7/14/2005
St Sauver, Joe	University of Oregon	7/21/2005
St. Clair, John	MCI	7/27/2005
Stansell, Maxine	Federal Trade Commission	7/14/2005
Stratton, Connie	New Hampshire Office of Attorney General	7/14/2005
Swanson, Jodi	South Dakota Office of Attorney General	7/14/2005
Sweedler, Ian	California Office of Attorney General	7/14/2005
Taff, Thomas	National Association of Attorneys General	7/14/2005
Teeluckingh, Anthony	Department of Justice	7/14/2005
Teter, Carolyn	Wyoming Office of Attorney General	7/14/2005
Weintraub, Ann	Federal Trade Commission	7/14/2005
Welch, Susan	Procter & Gamble	7/28/2005
Williams, Bridgette	Mississippi Office of Attorney General	7/14/2005
Winterrowd, Dana	California Department of Consumer Affairs	7/14/2005
Worley, Harriet	North Carolina Department of Justice	7/14/2005

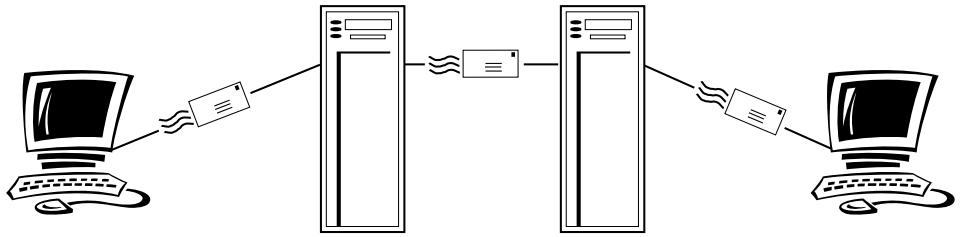
Appendix 3: Part III of the Commission's National Do Not Email Registry Report

III. The Email System and the Resulting Spam Problem

The email system is open, allowing information to travel freely with relative anonymity and ease. This structure facilitates the proliferation of spam by making it possible and cost-efficient for illegitimate marketers to send spam to billions of email accounts worldwide, while allowing them to hide

Federal Trade Commission

Graphic 1



their identities and the origins of their email messages. ISPs have responded to the spam problem by using blocking and filtering software. Currently, ISPs are attempting to combat this fundamental problem with spam – anonymity – by developing authentication technologies that would provide a method for identifying the true origin of an email.

A. How the Email System Works[14]

Email is a complex system that includes the sequential interactions of at least four computers[15] that engage in a five-part dialogue. (*See* Graphic 1). Each step in the email process is recorded within the email's "headers," so that an email's path through each computer can be tracked. Unfortunately, the system that makes email work, "Simple Mail Transfer Protocol" or "SMTP,"[16] does not require the transmission of accurate information. As explained below, the only piece of information that must be accurate is the recipient's address appearing in an SMTP command known as "RCPT TO."

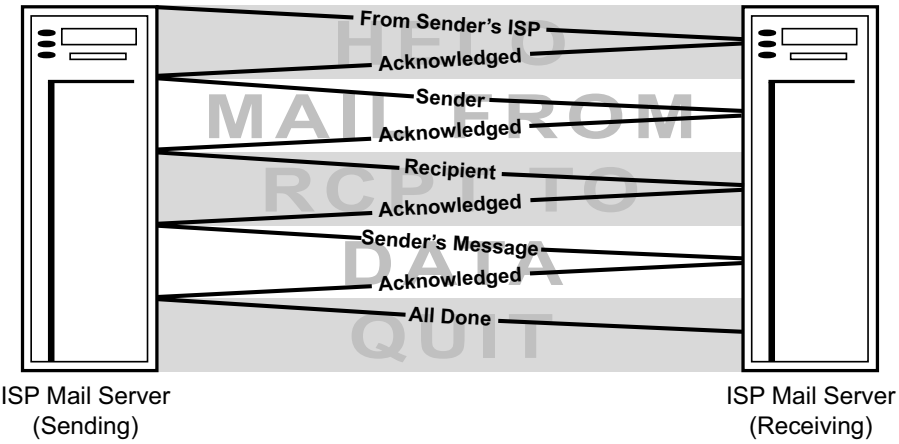
1. The five-part dialogue

Anyone who has ever used email knows what a "user-friendly" medium it is. To send a message, a person only needs to open an email program, type a recipient's address in the "To:" line, perhaps include a subject in the "Subject:" line, type the body of the message, maybe add an attachment, and select "send." A recipient has a similarly easy time. To read a message, a recipient only needs to open an email program, select the message listed in the inbox, and, if an attachment is included with the message, download or read the attachment.

The technical process of how email functions is, of course, much more complex. From the time that a person clicks "send" until the message arrives in a recipient's inbox, many processes occur involving – when reduced to the most basic form – at least four computers:

14. Don Blumenthal, the FTC's Internet Lab Coordinator, provided much of the material for this Section.
15. In reality, if a message is sent within an organization, only three computers may be involved because the sending mail server and the receiving mail server may be the same.
16. SMTP is defined in a "request for comments" posted by the Internet Engineering Task Force ("IETF") and known as RFC 2821. The IETF is an Internet-standards setting body.

Graphic 2



(1) the sender's computer; (2) a mail server owned by an ISP or other entity that provides the sender with an email account; (3) a mail server owned by an ISP or other entity that provides the recipient with an email account; and (4) the recipient's computer.

Clicking the "send" button transmits the email message from the sender's computer to the sender's outbound mail server. This sending server locates and begins a dialogue with the recipient's inbound mail server using SMTP. Under SMTP, the sending and receiving mail servers engage in a five-part dialogue. (*See* Graphic 2).

In the first part, the sending server initiates the exchange with the receiving server using a command known as "HELO," followed by the name of the sending mail server. If translated into English, the sending server would be saying "Hello, I'm <servername>." The receiving server responds with an acknowledgment back to the sending server. It is important to note that the receiving server uses this "HELO" command only to ensure that it is receiving a valid transmission.[17] The receiving server does not verify whether the servername listed after the "HELO" command is the sending server's actual, accurate name. This aspect of SMTP – the fact that the receiving server does not demand authentication that the sending server is what it purports to be – significantly impedes effective anti-spam solutions, including robust enforcement of the CAN-SPAM Act and the effective use of anti-spam filters by ISPs and other domain operators.[18]

After the receiving server has sent an acknowledgment, the sending server begins the second part of the dialogue, using a command called "MAIL FROM." The sending server, in effect, tells the receiving server, "I have mail to deliver from <sender>." The "MAIL FROM"

17. The receiving computer only validates whether the dialogue started properly. The "HELO" command is the first command allowed under the SMTP system. If there is no "HELO" command when using SMTP, then the transmission is invalid.

18. *See infra* Section III.B.1.

is followed by an email address, known as the "envelope from." The "envelope from" is analogous to the return address appearing on an envelope sent through the postal system. As with a return address on an envelope, nothing requires the "envelope from" to be accurate. Moreover, just as the return address on a letter need not match the return address on the envelope containing the letter, the "envelope from" does not have to match the "From:" line that a recipient sees when reading an email message.[19]

In the third part of the dialogue, the sending server, using the "RCPT TO" command, tells the receiving server the email address to which the message should be delivered, and the receiving server sends an acknowledgment back to the sending server. If the message is for more than one recipient, the sending server issues separate "RCPT TOs" for each one. As with the "MAIL FROM," nothing requires that the "RCPT TO" address match the address that appears in the "To:" line of the email. Spammers often exploit this feature to make it appear that their messages are personal. For example, a message's "To:" line may state "Bob," "Account Holder," or any other term designed to trick recipients into believing that they have a relationship with the spammer. In contrast, the email address in the "RCPT TO" command must be valid or the message cannot be delivered.[20]

In the fourth part of the dialogue, after the receiving server has acknowledged the "RCPT TO," the sending server, using the "DATA" command, transmits the actual message. While not required, the first line of the message usually begins with "Subject:," followed by the sender's desired subject. Other headers, such as "Reply-To:,"[21] "cc:," and "bcc:" also may be specified here.[22] The text of the message and any attachments then follow. A blank line with a period signals the end of the "DATA" section. This part of the dialogue concludes when the receiving mail server acknowledges receipt of the email.

In the fifth and final part of the dialogue, the sending server uses the "QUIT" command to terminate the process. The recipient then can view the message through a web interface or email program.

2. Email headers

In theory, the above-described email path is memorialized in "headers" that the recipient can view. Headers are added at three points in the basic four-computer model: (1) message creation; (2) transmission to the sender's server; and (3) transmission to the recipient's

19. Indeed, the Commission staff's April 2003 False Claims in Spam Study reported that 1/3 of the spam analyzed contained false information in the "From:" line. False Claims in Spam, 3.

20. *See infra* Section III.B.1.

21. "Reply-To:" may vary from the address in the "From:" line. This header has legitimate uses; for example, a sender with two addresses may want replies to go to only one address. Spammers, however, can use this header to deflect hostile responses. For instance, the "Reply-To:" address may identify a non-existent email address, in which case opt-out demands will disappear into the ether. Or, the spammer may identify a valid but innocent email address, thereby causing the maligned addressee to receive an avalanche of opt-out requests and complaints. *See infra* Section III.B.1.

22. The headers discussed in this section are only a subset of those available. They are, however the most commonly used and the most important for understanding email transmission and how spammers use the current system to hide their identities.

#	Header	Header's Source
1	Received: from server.sender.com (server.sender.com [123.45.67.90]) by server.recipient.com (8.8.5/8.7.2) with ESMTP id ABC12345 for <pan@recipient.com>; Tue, Mar 30 2004 20:06:22 EST -0500 (EST)	Receiving Mail Server
2	Received: from client.sender.com (client.sender.com [123.45.67.89]) by server.sender.com (8.8.5) id 003A23; Tue, Mar 30 2004 20:06:17 EST -0500 (EST)	Sending Mail Server
3	From: dmb@sender.com (D.M. Bloom)	Sender
4	To: pan@recipient.com	Sender
5	Date: Tue, Mar 30 2004 20:06:15 EST	Sending Mail Server
6	Message-Id: <dmb061346790416-00012487@sender.com>	Sending Mail Server
7	X-Mailer: Eudora v.6.0.3.0	Sender's Computer
8	Subject: How Email Works	Sender

server. Headers contain lines of information that provide details about the message and its transmission. Understanding headers is critical to understanding how email works and how spammers exploit the email system.

When an email is received, the recipient usually views only a few of the header lines, including the "To:" line, the "From:" line, the "Subject:" line, and the "Date:" line. Most email programs, though, enable recipients to view all of the headers for each message. A recipient who chooses to view all headers will see the information appearing in the second column of the table above, showing an illustrative email header, presented in the order in which it appears in the email.[23]

As a message travels from computer to computer, a new header is added to the top of the list of headers. Headers therefore should be read in reverse order. In the example above, the sender creates Line 8, the "Subject:" header. The sender's computer also creates Line 7, "X-Mailer," a header that denotes the sender's email program. The sender's mail server adds Line 6, the "Message-Id," a unique number that stays with the message from beginning to end. (Other "Ids" are created as the message passes through different servers). The "Message-Id" does not always have the email format shown here; it may be just a series of characters without the sender's domain information.[24] The sender's mail server adds Line 5, "Date:." This header shows the date and time the sender's mail server processes the message. Line 4, "To:," shows the intended recipient, and line 3, "From:," shows the sender's email address. The sender creates both Lines 4 and 3. "From:" also may show a name in brackets or parentheses.

Headers that begin with "Received:" are called "routing headers," and each mail server that a message passes through as it travels from sender to recipient adds such a routing header. These headers should be read from bottom to top. In the example above, the first "Received:" header (Line 2) indicates that the sending mail server (server.sender.com) received the message from the sender's computer (client.sender.com), which had the IP number, or Internet address, 123.45.67.89, on March 30, 2004, at 8:06 pm. The "8.8.5" shows

23. In reality, each line of an email header is not numbered, although for convenience of explanation, the table provides ordinal numbers in the first column.

24. The sender's domain information – where on the Internet the sender purports to come from – appears after the @ symbol in line 6.

the version of Sendmail, a mail server program, used on the sender's server. The second "Received:" header (Line 1) shows receipt of the message by the recipient's mail server from the sender's mail server. This header is similar to the previous one except for the format of the "ID" assigned at this step and the fact that it shows the intended recipient. The routing is now complete; the recipient's email program does not add a header when the message is retrieved.

The four-computer model is the simplest depiction of the core processes in sending an email message. Email routing is rarely that simple, however. There are almost always a number of additional intervening stops on the path from sender to recipient. This is because the sender's mail server must find the proper IP address for the recipient's mail server. If the sending server does not have a complete database of email servers and their corresponding IP addresses, it must route the message through intervening servers, or "relays," that narrow the destination down to the proper receiving server. Each server in the relay process adds a "Received from:" line to the headers.[25] When relays are secured properly, the system works well and a message can be traced to its origin.

B. How Spammers Exploit the Email System

Spammers are technologically adept at hiding their identities. Their concealment techniques make it extremely difficult to track them. In addition, spammers continually engage in a game of technological cat-and-mouse with the ISPs that try to block their messages.

1. Spammers exploit SMTP's anonymity

Spammers use many techniques to hide, including: spoofing, open relays, open proxies, and zombie drones. As explained below, each of these techniques makes it difficult, if not impossible, to identify spammers through email headers and significantly impedes law enforcement.[26]

First, spammers use "spoofing" to falsify header information and hide their identities. This technique disguises an email to make it appear to come from an address other than the one from which it actually comes.[27] A spammer can falsify portions of the header or the entire header. A spammer can even spoof the originating IP address.[28] The SMTP system facilitates this practice because it does not require accurate routing information except for the intended recipient of the email.[29] By failing to require accurate sender identification, SMTP allows spammers to send email without accountability, often disguised as personal email.[30] A spammer can send out millions of spoofed messages, but any bounced messages – messages returned

25. As part of the Data dialogue in part 4 of the SMTP dialogue described above, spammers also can add spurious "Received:" headers manually before sending a message.

26. *See infra* Section III.C.

27. Felten Report, 2. Spoofing requires virtually no technical sophistication and can be accomplished by simply changing the preferences in a computer user's email software. AOL: Koschier – Spam Forum (April 30, 2003), 175-82.

28. Bishop Report, 12 n.6.

29. *See supra* Section III.A.1.

30. An attorney representing AOL testified before the Pennsylvania State Senate Communications and Technology Committee that as much as 90 percent of spam messages contain falsified header or routing information (September 23, 2003).

as undeliverable – or complaints stemming from the spoofed emails will only go to the person whose address was spoofed. The spammer never has to deal with them. As a result, an innocent email user's inbox may become flooded with undeliverable messages and angry, reactive email, and the innocent user's Internet service may be shut off due to the volume of complaints.[31]

Second, spammers use open relays to disguise the origin of their email. The difference between an open relay and a "secure" one is critical. A computer must be connected to a mail server to send or receive mail. When someone sends an email message using an email server that is "secure," the mail server's particular software checks to make sure that the sender's computer and email account are authorized to use that server. If this authorization is in order, then the server sends the mail. If the computer and email account are *not* listed as authorized, the server refuses to accept the email message. On the other hand, if a mail server is *not* secure, i.e., some of its settings allow it to stay open, it will forward email even though the senders are not authorized users of that server. An open server is called an open relay because it will accept and transfer email on behalf of any user anywhere.[32]

Spammers who use open relays effectively bypass the email servers to which their computers are connected. Once the spam passes through an open relay, a routing header from that server is added to the email. Thus, the email will appear as if it originated from the relay mail server. This allows spammers to obscure their tracks, making it difficult to trace the path their message takes from sender to recipient.

Third, many spammers use "open proxies." They began doing this after ISPs and other mail server operators realized the negative impact of open relays and made efforts to identify and close them.[33] Again, a word of explanation is in order. Most organizations have multiple computers on their networks, but have a smaller number of proxy servers that are the only machines on the network that directly interact with the Internet.[34] This system provides more efficient web browsing for the users within that organization and secures the organization's network against unauthorized Internet users from outside the organization. If the proxy is not configured properly, it is considered to be "open," and may allow an unauthorized Internet user to connect through it to other hosts (computers that control communications in a network or administer databases) on the Internet. "[P]roxy misconfiguration is common and results in general purpose forwarding that is utilized by hackers and spammers."[35] For example, a spammer can use an open proxy to connect to another mail server and use that mail server to

31. The Commission has charged spoofing as a violation of Section 5 of the FTC Act, 15 U.S.C. § 45. *See e.g., FTC v. GM Funding*, No. SAVC 02-1026 (C.D. Cal. filed Nov. 6, 2002) (one victim of spoofing received 40,000 rejected messages in his inbox); *FTC v. Westby*, No. 032-3030 (N.D. Ill. filed Apr. 15, 2003). Moreover, spoofing violates Sections 4 and 5(a) of the CAN-SPAM Act, 18 U.S.C. § 1037 and 15 U.S.C. § 7704(a).
32. Rubin Report, 13.
33. Nonetheless, "open relays continue to exist in abundance." Rubin Report, 14.
34. A proxy server is so named because, when interacting with the Internet, it serves as a substitute or proxy for other computers on its network.
35. Rubin Report, 14.

send spam. The headers for messages that pass through an open proxy indicate the proxy's IP address in the "Received:from" line, and not the true originating IP address. In this way, open proxies provide another means for spammers to hide their tracks. MessageLabs, an email security company, believes that spammers sent more than two-thirds of all their email in 2003 through open proxies.[36]

Fourth, the most recent escalation in this cat-and-mouse game involves the exploitation of millions of home computers, using malicious viruses, worms, or "Trojans."[37] These infections, often sent via spam, turn any computer into an open or compromised proxy called a "zombie drone."[38] Once a computer is infected with one of these programs, a spammer can remotely hijack and send spam from it. Spammers target home computers with high speed Internet connections, such as DSL or cable modem lines, that are poorly secured. Spam sent via zombie drones will appear to originate (and actually will originate) from these infected computers.[39] This practice is all the more pernicious because users often do not know that their home computers are infected. The outgoing spam does not show up in their outbox. Once an ISP realizes spam is coming from one of its customer's machines, the ISP must shut off the customer's Internet service even though the customer had no knowledge that the spammer was using his or her machine.[40]

Although it is difficult to estimate the prevalence of zombie drones, Microsoft's Anti-Spam Manager has indicated that zombie drones presently account for somewhere between 15 and 60 percent of spam, and opined that the percentage is rising.[41] One major ISP reported a 41% increase in customer complaints regarding spam coming from other ISPs between October 2003 and February 2004.[42] This ISP believes that the shift is due to the increased use of zombie drones to transmit email messages from those other ISPs.[43] Another ISP reported that during 2003 it discovered over 600,000 open proxies or zombie drones.[44] Most recently, ISPs have observed compromised proxies shifting overseas, which means that the spam looks like it is coming from overseas, yet the virus author and spammer using the drones may be located in the United States.[45] If the past is an indication

36. MessageLabs states its conclusion, but does not explain how the company reached it. MessageLabs, "Spam and Viruses Hit All Time Highs in 2003," December 8, 2003 at http://www.messagelabs.com/news/pressreleases/detail/default.asp?contentItemId=613&region=. A background paper prepared by the Organization for Economic Cooperation and Development ("OECD") in January 2004, similarly states that 50 percent of spam flows through open relays and proxies, but does not explain the basis for this assertion. http://www.olis.oecd.org/olis/2003doc.nsf/43bb6130e5e86e5fc12569fa005d004c/edfc2255d6a8a51ac1256e240030f5b6/$FILE/JT00157096.PDF. The OECD's paper does not indicate the time frame for this statistic.
37. Rubin Report, 14-15.
38. Felten Report, 2.
39. Rubin Report, 14.
40. CNN, "Your Computer Could be a 'Spam Zombie,'" February 18, 2004, at http://www.cnn.com/2004/TECH/ptech/02/17/spam.zombies.ap/.
41. March 10, 2004 briefing of FTC staff by Microsoft Anti-Spam Manager.
42. Confidential 6(b) Order Response.
43. *Id*.
44. Confidential 6(b) Order Response.
45. One ISP reports that in January and February of 2004, 56% of all spam that made it to its subscribers' inboxes was routed through a server or proxy located outside the United States. Confidential 6(b) Order Response.

of the future, within the next several months spammers will have found an as-yet unknown new technique for masking their identities.

2. ISPs' response to spammers' email exploitation

The ISP industry's standard practice is to prohibit unsolicited bulk email.[46] ISPs and email filtering companies attempt to enforce this rule mainly through the use of blocking and filtering software.[47] ISPs initially block email based on volume ("volume filtering") and not based on content because their filters cannot make a distinction between commercial and non-commercial email. Many ISPs first attempt to block email at the point of the attempted connection to the ISPs' networks (the first part of the five-part SMTP dialogue).[48] For example, an ISP may initially block a message based on an IP address it has determined is used by spammers as an open relay or open proxy, or because an IP address or domain is associated with sending high volumes of spam. Anti-spam organizations compile "blacklists" of reported open relays and proxies that ISPs and other operators of mail servers can use to support their filtering efforts.[49]

Although the first line of defense against spam is volume filtering, most ISPs add an additional layer by filtering based upon their own customers' complaints. ISPs use complaint data in a variety of ways, including Bayesian filtering – filtering based upon the concept that some words occur more frequently in known spam. By analyzing email that customers report as spam, ISPs generate a mathematical "spam-indicative probability" for each word.[50] Many email filtering companies combine this type of filtering with filtering based upon different components of the message headers.

ISPs and email filtering companies are concerned about potentially blocking legitimate messages. These "false positives" can be a serious side effect of combating spam. According to Assurance Systems, a spam solutions provider, ISPs block or filter 17% of permission-based email.[51] To reduce false

46. United Online ("UOL"): Popek, 30-31; Junkbusters: Catlett, 15; *See also* the acceptable use policies of MCI (http://global.mci.com/legal/usepolicy; http://privacy.msn.com/anti-spam), Earthlink (http://www.earthlink.net/about/policies/use; http://docs.yahoo.com/info/guidelines/spam.html), Comcast (http://www.comcast.net/terms/abuse.jsp), AOL (http://postmaster.aol.com/guidelines/bulk_email.html), Microsoft (http://privacy.msn.com/anti-spam), and UOL (http://www.netzero.net/legal/terms.html, http://www.juno.com/legal/accept-use.html, and http://www.mybluelight.com/legal/terms-bluelight.html).
47. Email blocking occurs at the point of attempted connection to the ISP's network. Email filtering occurs once an email enters the ISP's network, but before it reaches a recipient's inbox.
48. *See supra* Section III.A.1.
49. SpamCop: Haight – Spam Forum (May 1, 2003), 118.
50. Mertz, David. "Spam Filtering Techniques: Comparing a Half-Dozen Approaches to Eliminating Unwanted Email," Gnosis Software, Inc., August 2002 at http://www.gnosis.cx/publish/programming/filtering-spam.html.
51. http://www.returnpath.biz/pdf/Blocking_Filtering_Report.pdf. Assurance Systems determined the percentage of permission-based messages that were incorrectly filtered by ISPs by tracking the delivery, blocking, and filtering rates of over nine thousand email campaigns. High false positive rates undermine consumer confidence in the email system. In an October 2003 study of 483 randomly selected consumers with home Internet access, RoperASW found that 40 percent of consumers who subscribe to or receive email from their credit card issuer expressed concern about not receiving email from the issuer due to their ISPs' anti-spam filters. *Email and Spam: Attitudes and Behaviors Among Financial Services Consumers*, Study commissioned and submitted to the Commission by Bigfoot Interactive.

positive rates, ISPs compile "white lists" of marketers who agree to adhere to an ISP's policies and procedures regarding bulk email. Once a marketer is on an ISP's white list, the ISP does not filter that marketer's messages. A certain number of complaints regarding a particular marketer who is on the ISP's white list, however, will trigger removal of that marketer from the white list.[52] The threat of false positives is a significant barrier to more effective filtering by ISPs.

C. Email's Lack of Authentication Enables Spammers to Exploit the Email System

Obfuscatory techniques such as spoofing, open relays, open proxies, and zombie drones make it more difficult for ISPs to locate spammers. When ISPs and domain holders implement technologies designed to stop one exploitative technique, spammers quickly adapt, finding new methods to avoid detection. If the cloak of anonymity were removed, however, spammers could not operate with impunity.[53] ISPs and domain holders could filter spam more effectively, and the government and ISPs could more effectively identify and prosecute spammers who violate the CAN-SPAM Act or other statutes.

The marketplace is already moving toward creating systems for authenticating a message's originating second-level domain,[54] with major ISPs backing various approaches.[55] AOL champions the adoption of SPF ("sender policy framework"),[56] an authentication standard developed by Meng Weng Wong ("Wong") that verifies the "envelope from"[57] of an email message. Microsoft has proposed "Caller ID for Email,"[58] a protocol that would verify the "From:" line that appears in an email message.[59] Recently, Microsoft and Wong announced plans to merge SPF and Caller ID for Email into one technical specification.[60] Yahoo! has advocated the implementation of "Domain Keys," a standard that would involve the use of public/private key cryptography.[61] The IETF has also established a working group to develop an authentication standard.[62] The IETF working group intends to propose an authentication standard during the Summer of 2004.[63]

52. Briefing of FTC staff by an ISP concerning its Confidential 6(b) Order responses.
53. Comcast: Lutner, 42; Edelman, 28; Savicom: Bernard, 23; UOL: Skopp, 61.
54. A second-level domain is the name in an email address that appears between the "@" symbol and the dot. For instance, "ftc" is the second-level domain in the address "abc@ftc.gov."
55. U.S. Internet Service Provider Association ("USISPA")-Comment, 2 (stating that "several of its members and other technology vendors are in the process of developing solutions to spam based on identifying the origin or identity of email senders"). Digital Impact: Brondmo, 17-18; ESPC: Hughes, 11; Internet Commerce Coalition ("ICC"): Halpert, 25; NetCreations: Mayor, 24; Roving Software: Olson, 20-21.
56. http://www.ietf.org/internet-drafts/draft-mengwong-spf-01.txt.
57. *See supra* Section III.A.1.
58. http://download.microsoft.com/download/2/e/2/2e2850b8-2747-4394-a5a9-d06b5b9b1a4c/callerid_email.pdf.
59. March 10, 2004 briefing of FTC staff by Microsoft Anti-Spam Manager.
60. http://www.microsoft.com/presspass/press/2004/may04/05-25SPFCallerIDPR.asp.
61. http://antispam.yahoo.com/domainkeys.
62. http://www.nwfusion.com/news/2004/0412marid.html.
63. *Id.*

None of these standards has been widely tested, and each is still in development. Estimates differ on how soon the market will test and widely deploy the competing authentication standards. Some believe that all email will be authenticated within a year.[64] Others are less sanguine. According to a technologist with Comcast, "[i]t might be even two years or more before any one solution is solid enough that it can be deployed even in smaller systems where it's not going to crush them."[65] Small ISPs are especially concerned that the multiple authentication standards will prove too costly to implement.[66]

It should be noted that these private market proposals do not authenticate the identity of the person sending an email. In other words, if a message claimed to be from abc@ftc.gov, the private market proposals would authenticate that the message came from the domain "ftc.gov," but would not authenticate that the message came from the particular email address "abc" at this domain. Nonetheless, domain-level authentication would confound spammers' ability to engage in spoofing and to send messages via open relays and open proxies, enable ISPs to deploy more effective filters, and provide law enforcement with an improved ability to track down and prosecute spammers.

64. Digital Impact: Brondmo, 24 (12 months); Roving Software: Olson, 23 (6 to 9 months).
65. Comcast: Lutner, 46.
66. Aritstotle: Bowles, 75.

Appendix 4: Summary of the US SAFE WEB Act

Background: The Internet and electronic commerce know no boundaries, and cross-border fraud and deception is a growing problem for consumers and businesses in the U.S. and abroad. **The US SAFE WEB Act provisions are needed to** help the FTC to protect consumers from cross-border fraud and deception, and particularly to fight spam, spyware, and Internet fraud and deception. The key provisions are summarized below:

- **Broadening Reciprocal Information Sharing.** (US SAFE WEB Act §§ 4(a), 6(a)) Allows the FTC to share confidential information in its files in consumer protection matters with foreign law enforcers, subject to appropriate confidentiality assurances. **Similar to** longstanding SEC, CFTC, and federal banking agency authority. **Needed to** allow the FTC to share information with foreign agencies to help them halt fraud, deception, spam, spyware and other consumer protection law violations targeting U.S. consumers. Also **needed** for the FTC to obtain, in return, foreign information required to halt such illegal practices.

- **Expanding Investigative Cooperation.** (US SAFE WEB Act § 4(b) (adding FTC Act § 6(j))) Allows the FTC to conduct investigations and discovery to help foreign law enforcers in appropriate cases. **Similar to** longstanding SEC, CFTC, and federal banking agency authority. **Needed to** allow the FTC to obtain information for foreign agencies' actions to halt fraud, deception, spam, spyware, and other consumer protection law violations targeting U.S. consumers. Also **needed** to help the FTC to obtain, in return, foreign investigative assistance in FTC cases.

- **Obtaining More Information from Foreign Sources.** (US SAFE WEB Act § 6(b)) Protects information provided by foreign enforcers from public disclosure if confidentiality is a condition of providing it. **Similar to** longstanding SEC and CFTC authority. **Needed** because, without it, some foreign law enforcers will not give the FTC information needed to halt fraud, deception, spam, and spyware.

- **Protecting the Confidentiality of FTC Investigations.** (US SAFE WEB Act § 7) Safeguards FTC investigations in a defined range of cases by (1) generally protecting recipients of Commission CIDs from possible liability for keeping those CIDs confidential; (2) authorizing the Commission to seek a court order in appropriate cases to preclude notice by the CID recipient to the investigative target for a limited time; and (3) tailoring the mechanisms available to the Commission to seek delay of notification currently required by the Right to Financial Privacy Act ("RFPA") or the Electronic Communications Privacy Act ("ECPA"), to better fit FTC cases. **Similar to** longstanding RFPA, ECPA, and securities law provisions. **Needed to** prevent notice to investigative targets that are likely to destroy evidence or to move assets offshore or otherwise conceal them, precluding redress to consumer victims.

- **Protecting Certain Entities Reporting Suspected Violations of Law.** (US SAFE WEB Act § 8) Protects a limited category of appropriate entities from liability for voluntary disclosures to the FTC about suspected fraud or deception, or about recovery of assets for consumer redress. **Similar to** longstanding protections for financial institutions making disclosures of suspected wrongdoing to federal agencies. **Needed because** liability concerns discourage third-party businesses from alerting the FTC to suspected law violations or recoverable assets.
- **Allowing Information Sharing with Federal Financial and Market Regulators.** (US SAFE WEB Act § 10) Adds the FTC to RFPA's list of financial and market regulators allowed to readily share appropriate information. The list already includes the SEC and the CFTC. **Needed to** help the FTC track proceeds of fraud, deception, or other illegal practices sent through U.S. banks to foreign jurisdictions, so they can be recovered and returned to consumer victims.
- **Confirming the FTC's Remedial Authority in Cross-Border Cases.** (US SAFE WEB Act § 3) Expressly confirms: 1) the FTC's authority to redress harm in the United States caused by foreign wrongdoers and harm abroad caused by U.S. wrongdoers; and 2) the availability in cross-border cases of all remedies available to the FTC, including restitution. **Needed to** avoid spurious challenges to jurisdiction in FTC cases and to encourage the full range of remedies for U.S. consumer victims in foreign courts.
- **Enhancing Cooperation Between the FTC and DOJ in Foreign Litigation.** (US SAFE WEB Act § 5) Permits the FTC to cooperate with DOJ in using additional staff and financial resources for foreign litigation of FTC matters. **Needed because**, without additional resources to freeze foreign assets and enforce U.S. court judgments abroad, fraudsters targeting U.S. consumers can more readily use the border as a shield against law enforcement.
- **Clarifying FTC Authority to Make Criminal Referrals.** (US SAFE WEB Act § 4(b) (adding FTC Act § 6(k))) Expressly authorizes the FTC to make criminal referrals for prosecution when violations of FTC law also violate U.S. criminal laws. **Similar to** existing FTC authority to provide information to criminal authorities, a narrow express criminal referral provision in the FTC Act, and an SEC provision. **Needed because** foreign agencies that address consumer fraud and deception as a criminal (not civil) law enforcement issue would be more willing to share information if FTC has express authority to share information with criminal authorities.
- **Providing for Foreign Staff Exchange Programs.** (US SAFE WEB Act § 9) Provides for foreign staff exchange arrangements between the FTC and foreign government authorities, and permits the FTC to accept reimbursement for its costs in these arrangements. **Needed to** improve international law enforcement cooperation in crossborder matters.

- **Authorizing Expenditure of Funds on Joint Projects.** (US SAFE WEB Act § 4(b) (adding FTC Act § 6(l)), 4(c)) Authorizes the FTC to expend appropriated funds, not to exceed $100,000 annually, toward operating expenses and other costs of cooperative cross-border law enforcement projects and bilateral and multilateral meetings. **Similar to** SEC authority. **Needed to** allow the FTC to help support valuable international cooperative organizations and projects such as the website or consumer education programs of the International Consumer Protection and Enforcement Network (ICPEN) that foster the FTC's mission.

- **Leveraging FTC's Resources Through Reimbursement, Gift Acceptance, and Voluntary and Uncompensated Services.** (US SAFE WEB Act § 11) Authorizes the FTC to accept reimbursement for providing assistance to law enforcement agencies in the U.S. or abroad, and to accept gifts and voluntary services in aid of the agency's mission and consistent with ethical constraints. **Similar to** the authority of numerous regulatory agencies, including the SEC and the CFTC, and of the FTC and DOJ in the antitrust context, to accept reimbursements from foreign counterparts. **Needed to** assure that in appropriate circumstances a foreign agency bears the costs of FTC efforts on their behalf, and to enable the FTC to employ volunteers as our Canadian counterparts have done successfully for years.

- **Requiring Report to Congress.** (US SAFE WEB Act § 13) Requires the FTC to report to Congress within three years after the enactment of this Act, describing the FTC's use of its new authority and recounting the number and types of requests for informationsharing and investigative assistance, the disposition of such requests, the foreign law enforcement agencies involved, and the nature of the information provided and received. Provides for the report to include recommendations for additional legislation as appropriate. **Needed to** provide important information to Congress on FTC accountability and cross-border trends and needs.

Appendix 5: FTC's CAN-SPAM Cases

January 1, 2004 through December 1, 2005

Listed chronologically by date filed

Caption	Goods or Services	CAN-SPAM or Adult Labeling Rule Violations Alleged	Status
FTC v. Phoenix Avatar, LLC; DJL, LLC; Daniel J. Lin; Mark M. Sadek; James Lin; and Christopher Chung, No. 04C 2897. (N.D. Ill. filed Apr. 23, 2004)	Diet patch	15 U.S.C. § 7704(a)(1) 15 U.S.C. § 7704(a)(5)	Settlement.
FTC v. Global Web Promotions PTY LTD.; Michael John Anthony Van Essen; and Lance Thomas Atkinson, No. 04C 3022. (N.D. Ill. filed Apr. 28, 2004)	Diet patch and human growth hormone supplement	15 U.S.C. § 7704(a)(1) 15 U.S.C. § 7704(a)(5)	Default judgment.
FTC v. Creaghan A. Harry, No. 04C 4790. (N.D. Ill. filed July 21, 2004)	Human growth hormone products	15 U.S.C. § 7704(a)(1) 15 U.S.C. § 7704(a)(5)	Settlement.
FTC v. Gregory Bryant, Jr. and Nadira Bryant, No. 3:04-CV-897. (M.D. Fla. filed Sept. 15, 2004)	Envelope-stuffing opportunity	15 U.S.C. § 7704(a)(1) 15 U.S.C. § 7704(a)(5)	Settlement.
FTC v. International Research and Development Corp.; Anthony Renda; Net Marketing Group, LLC; Floyd J. Tassin, Jr.; Marcia Tassin; Diverse Marketing Group, Inc.; Diverse Marketing Group, LLC; and Mark C. Ayoub, No. 04C 690. (N.D. Ill. filed Oct. 27, 2004)	"Automotive fuel saver"	15 U.S.C. § 7704(a)(1) 15 U.S.C. § 7704(a)(5)(A)	Discovery.
FTC v. Global Net Solutions, Inc.; Global Net Ventures, Ltd, a United Kingdom Co.; Wedlake Ltd.; Open Space Enterprises, Inc.; Southlake Group, Inc.; WTFRC, Inc.; Dustin Hamilton; Gregory Hamilton; Philip Doroff; and Paul Rose, No. S-05-0002. (D. Nev. filed Jan. 3, 2005)	Sexually-oriented content	15 U.S.C. § 7704(a)(1) 15 U.S.C. § 7704(a)(2) 15 U.S.C. § 7704(a)(4)(A)(i) 15 U.S.C. § 7704(a)(5)(A)(ii) or 15 U.S.C. § 7704(a)(3) 15 U.S.C. § 7704(a)(5)(A)(iii) 15 U.S.C. § 7704(d); 16 C.F.R. § 316.1(a)(1)	Settlement.

Caption	Goods or Services	CAN-SPAM or Adult Labeling Rule Violations Alleged	Status
FTC v. Sun Ray Trading, Inc.; SR & Associates, Inc.; Rolando Galvez-Garcia; Anneelises Flores Adino; and Kostadin Osvaldo Marte Tavarez, No. 05-20402. (S.D. Fla. filed Feb. 10, 2005)	Envelope-stuffing opportunity	15 U.S.C. § 7704(a)(2)	Discovery.
FTC and State of California v. Optin Global Inc.; Vision Media Limited Corp.; Rick Yang; and Peonie Pui Ting Chen, No. C 05 1502. (N.D. Cal. filed Apr. 12, 2005)	Mortgage loans and other products	15 U.S.C. § 7704(a)(1) 15 U.S.C. § 7704(a)(2) 15 U.S.C. § 7704(a)(4)(A)(i) 15 U.S.C. § 7704(a)(5)(A)(i) 15 U.S.C. § 7704(a)(5)(A)(ii) or 15 U.S.C. § 7704(a)(3) 15 U.S.C. § 7704(a)(5)(A)(iii)	Discovery.
FTC v. Cleverlink Trading Limited, a Cyprus LLC; Real World Media, LLC; Brian D. Muir; Jesse Goldberg; and Caleb Wolf Wickman, No. 05C 2889. (N.D. Ill. filed May 16, 2005)	Sexually-oriented content	15 U.S.C. § 7704(a)(1) 15 U.S.C. § 7704(a)(2) 15 U.S.C. § 7704(a)(5)(A)(ii) or 15 U.S.C. § 7704(a)(3) 15 U.S.C. § 7704(a)(5)(A)(iii) 15 U.S.C. § 7704(d); 16 C.F.R. § 316.4	Discovery.
FTC v. Trustsoft Inc. and Danilo Ladendorf, No. H 05 1905. (S.D. Tex. filed May 31, 2005)	"Spyware removal" software	15 U.S.C. § 7704(a)(1) 15 U.S.C. § 7704(a)(3) 15 U.S.C. § 7704(a)(5)(A)(i-iii)	Discovery.
U.S. v. Cyberheat, Inc., No. 05-cv-00475. (D. Ariz. filed July 20, 2005)	Sexually-oriented content	15 U.S.C. § 7704(a)(5)(A)(ii) or 15 U.S.C. § 7704(a)(3) 15 U.S.C. § 7704(a)(5)(A)(iii) 15 U.S.C. § 7704(d); 16 C.F.R. § 316.4(a)	Discovery.
U.S. v. Pure Marketing Solutions, LLC and Internet Matrix Technology, Inc., No. 05 cv-01353. (M.D. Fla. filed July 20, 2005)	Sexually-oriented content	15 U.S.C. § 7704(a)(5)(A)(ii) or 15 U.S.C. § 7704(a)(3) 15 U.S.C. § 7704(a)(5)(A)(iii) 15 U.S.C. § 7704(d); 16 C.F.R. § 316.4(a)	Settlement.
U.S. v. APC Entertainment, Inc., No. 05-cv-61194. (S.D. Fla. filed July 20, 2005)	Sexually-oriented content	15 U.S.C. § 7704(a)(5)(A)(ii) or 15 U.S.C. § 7704(a)(3) 15 U.S.C. § 7704(a)(5)(A)(iii) 15 U.S.C. § 7704(d); 16 C.F.R. § 316.4(a)	Settlement.
U.S. v. Bangbros.com, Inc.; RK Netmedia, Inc.; and Ox Ideas, Inc., No. 05-cv-21964. (S.D. Fla. filed July 20, 2005)	Sexually-oriented content	15 U.S.C. § 7704(a)(5)(A)(ii) or 15 U.S.C. § 7704(a)(3) 15 U.S.C. § 7704(a)(5)(A)(iii) 15 U.S.C. § 7704(d); 16 C.F.R. § 316.4(a)	Settlement.

Caption	Goods or Services	CAN-SPAM or Adult Labeling Rule Violations Alleged	Status
U.S. v. MD Media, Inc., No. 05-cv-72836. (E.D. Mich. filed July 20, 2005)	Sexually-oriented content	15 U.S.C. § 7704(a)(5)(A)(ii) or 15 U.S.C. § 7704(a)(3) 15 U.S.C. § 7704(a)(5)(A)(iii) 15 U.S.C. § 7704(d); 16 C.F.R. § 316.4(a)	Settlement.
U.S. v. TJ Web Productions, LLC, No. 05-cv-00882. (D. Nev. filed July 20, 2005)	Sexually-oriented content	15 U.S.C. § 7704(a)(5)(A)(ii) or 15 U.S.C. § 7704(a)(3) 15 U.S.C. § 7704(a)(5)(A)(iii) 15 U.S.C. § 7704(d); 16 C.F.R. § 316.4(a)	Discovery.
U.S. v. Impulse Media Group, Inc., No. 05-cv-01285. (W.D. Wash. filed July 20, 2005)	Sexually-oriented content	15 U.S.C. § 7704(a)(5)(A)(ii) or 15 U.S.C. § 7704(a)(3) 15 U.S.C. § 7704(a)(5)(A)(iii) 15 U.S.C. § 7704(d); 16 C.F.R. § 316.4(a)	Discovery.
FTC v. Pacific Herbal Sciences, Inc.; Natural Health Product, Inc.; New Star Marketing Group, Inc.; John A. Brackett, Jr.; and Lei Lu, No. 05 7247. (C.D. Cal. Oct. 6, 2005)	Oral sprays with human growth hormone	15 U.S.C. § 7704(a)(1) 15 U.S.C. § 7704(a)(2) 15 U.S.C. § 7704(a)(5)(A)(ii) or 15 U.S.C. § 7704(a)(3) 15 U.S.C. § 7704(a)(5)(A) (i) and (iii)	Discovery.
FTC v. Zachary Kinion, No. 05C 6737. (N.D. Ill. filed Nov. 29, 2005)	Mortgage loans and sexually-oriented content	15 U.S.C. § 7704(a)(1) 15 U.S.C. § 7704(a)(2) 15 U.S.C. § 7704(a)(5)(A)(ii) or 15 U.S.C. § 7704(a)(3) 15 U.S.C. § 7704(a)(5)(A)(iii)	Pre-discovery.
FTC v. Matthew Olson and Jennifer LeRoy, No. C05-1979. (W.D. Wash. filed Nov. 29, 2005)	Fuel efficiency enhancing devices and mortgage loans	15 U.S.C. § 7704(a)(1) 15 U.S.C. § 7704(a)(2) 15 U.S.C. § 7704(a)(5)(A)(ii) or 15 U.S.C. § 7704(a)(3) 15 U.S.C. § 7704(a)(5)(A)(iii)	Pre-discovery.

Appendix 6: ISPs' CAN-SPAM Cases

January 1, 2004 through September 1, 2005

Listed chronologically by date filed[1]

Caption	Goods or Services	CAN-SPAM Violations Alleged	Status
Hypertouch, Inc. v. BVWebTies, LLC; BlueStream Media; and Does 3 to 10. (N.D. Cal. filed Mar. 4, 2004)	BobVila.com and other websites	15 U.S.C. § 7704(a)(1) 15 U.S.C. § 7704(a)(4) 15 U.S.C. § 7704(a)(5)(A)(iii) 15 U.S.C. § 7704(b)(1)(A)(i) 15 U.S.C. § 7704(b)(1)(A)(ii)	Settlement.
America Online, Inc. v. Davis Hawke; Braden Bournival; Jacob Brown; Mauricio Ruiz; Amazing Internet Products LLC; and John Does 3-50. (E.D. Va. filed Mar. 9, 2004)	Sexual enhancement products, "banned CD," and ephedra pills	15 U.S.C. § 7704(a)(1) 15 U.S.C. § 7704(a)(2) 15 U.S.C. § 7704(a)(3) 15 U.S.C. § 7704(a)(5)	Settlement. Final judgment.
America Online, Inc. v. Richard Hicks; Alicia Colella; GW Consulting LLC; Amy Devoe; and John Does 5-40. (E.D. Va. filed Mar. 9, 2004)	Vacation timeshares and get-rich-quick offers	15 U.S.C. § 7704(a)(1) 15 U.S.C. § 7704(a)(2) 15 U.S.C. § 7704(a)(3) 15 U.S.C. § 7704(a)(5)	Settlement. Final judgment.
EarthLink, Inc. v. John Does 1 - 25 (the prescription drug spammers); John Does 26 - 35 (the mortgage lead spammers); John Does 36 - 45 (the cable descrambler spammers); John Does 46 - 55 (the university diploma spammers); John Does 56 - 65 (the get rich quick spammers); and John Does 66 - 75. (N.D. Ga. filed Mar. 9, 2004)	Various goods, includubg prescription drugs, mortgage services, cable descramblers, college diplomas, and get-rich-quick schemes	15 U.S.C. § 7704(a)(1) 15 U.S.C. § 7704(a)(2) 15 U.S.C. § 7704(a)(3)(A)(i) 15 U.S.C. § 7704(a)(3)(A)(ii) 15 U.S.C. § 7704(a)(4)(A) 15 U.S.C. § 7704(a)(5)(A) 15 U.S.C. § 7704(b)(1)(A)(i) 15 U.S.C. § 7704(b)(1)(A)(ii) 15 U.S.C. § 7704(b)(2) 15 U.S.C. § 7704(b)(3)	Dismissed.

1. FTC staff compiled this Appendix from information provided by top ISPs and from publicly available sources. Other federal court cases may have been filed by other ISPs. Additionally, ISPs have filed dozens of CAN-SPAM cases in state court, but these cases are not summarized in this Appendix.

Caption	Goods or Services	CAN-SPAM Violations Alleged	Status
Microsoft Corp. v. JDO Media, Inc.; Tony Lampert; Timothy Roland; Erik Summers; John McLeod; and John Does 5 - 50. (W.D. Wash. filed Mar. 9, 2004)	Automated multi-level marketing program	15 U.S.C. § 7704(a)(1) 15 U.S.C. § 7704(a)(2) 15 U.S.C. § 7704(a)(3) 15 U.S.C. § 7704(a)(5)	Settlement. Default judgment. Summary judgment.
Microsoft Corp. v. Daniel J. Lin; Mark M. Sadek; James Lin; Christopher M. Chung; Phoenix Avatar, LLC; DJL, LLC; and John Does 7 - 50 d/b/a Super Viagra Group. (W.D. Wash. filed Mar. 9, 2004)	"Super viagra" or weight loss patches	15 U.S.C. § 7704(a)(1) 15 U.S.C. § 7704(a)(2) 15 U.S.C. § 7704(a)(3) 15 U.S.C. § 7704(a)(5)	Default judgment.
Yahoo! Inc. v. Eric Head; Matthew Head; Barry Head; Gold Disk Canada, Inc.; Head Programming, Inc.; Infinite Technologies Worldwide, Inc.; and John Does 1 - 5. (N.D. Cal. filed Mar. 9, 2004)	Life insurance, mortgage and debt consolidation, and travel services	15 U.S.C. § 7704(a)(1) 15 U.S.C. § 7704(a)(2) 15 U.S.C. § 7704(a)(3) 15 U.S.C. § 7704(a)(5) 15 U.S.C. § 7704(b)(1)	Settlement.
Microsoft Corp. v. Leonid Radvinsky; Cyberpower Pty, Ltd; Cybertania, Inc.; Activsoft, Inc; and John Does 1 - 20. (W.D. Wash. filed Sept. 27, 2004)	Free grants	15 U.S.C. § 7704(a)(1) 15 U.S.C. § 7704(a)(2) 15 U.S.C. § 7704(a)(3) 15 U.S.C. § 7704(a)(5)	Settlement.
EarthLink, Inc. v. Christina Reese; YamboCS, Inc.; Angela M. Nickerson d/b/a YambosCS.com; and John Does 1 - 25 (the ASMTP spammers). (N.D. Ga. filed Oct. 14, 2004)	Sexually-oriented content	15 U.S.C. § 7704(a)(1) 15 U.S.C. § 7704(a)(2) 15 U.S.C. § 7704(a)(3)(A)(i) 15 U.S.C. § 7704(a)(3)(A)(ii) 15 U.S.C. § 7704(a)(4)(A) 15 U.S.C. § 7704(a)(5)(A) 15 U.S.C. § 7704(b)(1)(A)(i) 15 U.S.C. § 7704(b)(1)(A)(ii) 15 U.S.C. § 7704(b)(2) 15 U.S.C. § 7704(b)(3)	Discovery.
America Online, Inc. v. James Bragg; Timothy Bragg; Josefina Perez; and Global Internet Services, LLC. (E.D. Va. filed Oct. 27, 2004)	Prescription drugs	15 U.S.C. § 7704(a)(1) 15 U.S.C. § 7704(a)(2) 15 U.S.C. § 7704(a)(3) 15 U.S.C. § 7704(a)(5)	Settlement.

Caption	Goods or Services	CAN-SPAM Violations Alleged	Status
America Online, Inc. v. John Baker; Stephen Herceg; Chad Hughes; Danny Krotzer; Jason Kupis; Yaniv Mindell; S.W., a minor; and Jesse Zimmerman. (E.D. Va. filed Oct. 27, 2004)	Dating websites and sexually-oriented websites	15 U.S.C. § 7704(a)(1) 15 U.S.C. § 7704(a)(2) 15 U.S.C. § 7704(a)(3) 15 U.S.C. § 7704(a)(5)	Settlement. Discovery.
EarthLink, Inc. v. John Does 1 -25 (the mortgage lead spammers) and John Does 26 - 50 (the drug spammers). (N.D. Ga. filed Oct. 27, 2004)	Low mortgage or loan rates and prescription drugs	15 U.S.C. § 7704(a)(1)(A) 15 U.S.C. § 7704(a)(1)(B) 15 U.S.C. § 7704(a)(1)(C) 15 U.S.C. § 7704(a)(2) 15 U.S.C. § 7704(a)(3)(A)(i) 15 U.S.C. § 7704(a)(3)(A)(ii) 15 U.S.C. § 7704(a)(4)(A)(i) 15 U.S.C. § 7704(a)(4)(A)(ii) 15 U.S.C. § 7704(a)(4)(A)(iii) 15 U.S.C. § 7704(a)(4)(A)(iv) 15 U.S.C. § 7704(a)(5)(A)(i) 15 U.S.C. § 7704(a)(5)(A)(ii) 15 U.S.C. § 7704(a)(5)(A)(iii) 15 U.S.C. § 7704(b)(1)(A)(i) 15 U.S.C. § 7704(b)(1)(A)(ii) 15 U.S.C. § 7704(b)(2) 15 U.S.C. § 7704(b)(3)	Discovery.
Microsoft Corp. v. Steven Blaier; Jane Doe Blaier; Herbal Technologies, LLC; and John Does 1 - 10. (W.D. Wash. filed Oct. 27, 2004)	Sexual enhancement products	15 U.S.C. § 7704(a)(1) 15 U.S.C. § 7704(a)(2) 15 U.S.C. § 7704(a)(3) 15 U.S.C. § 7704(a)(5)	Dismissed.
Microsoft Corp. v. Henry Fitzsimmons; Jane Doe Fitzsimmons; and John Does 3 - 50 d/b/a yourloanz.com. (W.D. Wash. filed Oct. 27, 2004)	Discounted mortgage services	15 U.S.C. § 7704(a)(1) 15 U.S.C. § 7704(a)(2) 15 U.S.C. § 7704(a)(3) 15 U.S.C. § 7704(a)(5)	Default judgment.
Microsoft Corp. v. Kevin Hertz and John Does 2 - 50 d/b/a myauctionbiz.biz. (W.D. Wash. filed Oct. 27, 2004)	Training to increase profits on eBay	15 U.S.C. § 7704(a)(1) 15 U.S.C. § 7704(a)(2) 15 U.S.C. § 7704(a)(3) 15 U.S.C. § 7704(a)(5)	Discovery.

Caption	Goods or Services	CAN-SPAM Violations Alleged	Status
Yahoo! Inc. v. East Coast Exotics Entertainment Group, Inc. and Epoth LLC. (N.D. Cal. filed Oct. 27, 2004)	Sexually-oriented content	15 U.S.C. § 7704(a)(1) 15 U.S.C. § 7704(a)(3) 15 U.S.C. § 7704(a)(5)	Settlement.
America Online, Inc. v. Ambro Enterprises, Inc.; American Refinance Group; Andrew Amend; Jeremy Brown; Joshua Ellis; Stephen Goudreault; Ernesto Haberli; Eric Johnson; Nancy Korchick; Leadplex LLC; Opt-In America Corp.; Payperaction LLC; Ryan Pitylak; Timothy Saunders; Larry Schulman; Brian Tillman; Trendy Solutions Inc.; Mark Trotter; Daniel Walls; and Maria Walls. (E.D. Va. Dec. 17, 2004)	Mortgage leads	15 U.S.C. § 7704(a)(1) 15 U.S.C. § 7704(a)(2) 15 U.S.C. § 7704(a)(3) 15 U.S.C. § 7704(a)(5)	Settlement. Discovery.
EarthLink, Inc. v. Peter Moshou; Alice Cain; and John Does 1 - 25 (the timeshare spammers). (N.D. Ga. filed Dec. 20, 2004)	Timeshare brokerage services	15 U.S.C. § 7704(a)(1) 15 U.S.C. § 7704(a)(2) 15 U.S.C. § 7704(a)(3)(A)(i) 15 U.S.C. § 7704(a)(3)(A)(ii) 15 U.S.C. § 7704(a)(4)(A) 15 U.S.C. § 7704(a)(5)(A) 15 U.S.C. § 7704(b)(1)(A)(i) 15 U.S.C. § 7704(b)(1)(A)(ii) 15 U.S.C. § 7704(b)(2) 15 U.S.C. § 7704(b)(3)	Discovery.
EarthLink, Inc. v. Gregory Lars Alsing. (N.D. Ga. filed Jan. 18, 2005)	Cable descramblers and college diplomas	15 U.S.C. § 7704(a)(1) 15 U.S.C. § 7704(a)(2) 15 U.S.C. § 7704(a)(3)(A)(i) 15 U.S.C. § 7704(a)(3)(A)(ii) 15 U.S.C. § 7704(a)(4)(A) 15 U.S.C. § 7704(a)(5)(A) 15 U.S.C. § 7704(b)(1)(A)(i) 15 U.S.C. § 7704(b)(1)(A)(ii) 15 U.S.C. § 7704(b)(2) 15 U.S.C. § 7704(b)(3)	Settlement.

Caption	Goods or Services	CAN-SPAM Violations Alleged	Status
EarthLink, Inc. v. BC Alliance, Inc. and Craig S. Brockwell. (N.D. Ga. filed Jan. 18, 2005)	Computer printer supplies	15 U.S.C. § 7704(a)(1) 15 U.S.C. § 7704(a)(2) 15 U.S.C. § 7704(a)(3)(A)(i) 15 U.S.C. § 7704(a)(3)(A)(ii) 15 U.S.C. § 7704(a)(4)(A) 15 U.S.C. § 7704(a)(5)(A) 15 U.S.C. § 7704(b)(1)(A)(i) 15 U.S.C. § 7704(b)(1)(A)(ii) 15 U.S.C. § 7704(b)(2) 15 U.S.C. § 7704(b)(3)	Default judgment.
EarthLink, Inc. v. Richard Nolan; Nolan Micro Systems, Inc.; Marcus Tovar; E-Comm Consulting, Inc.; and John Does 1-5. (N.D. Ga. filed Feb. 22, 2005)	Mortgage leads	15 U.S.C. § 7704(a)(1) 15 U.S.C. § 7704(a)(2) 15 U.S.C. § 7704(a)(3)(A)(i) 15 U.S.C. § 7704(a)(3)(A)(ii) 15 U.S.C. § 7704(a)(4)(A) 15 U.S.C. § 7704(a)(5)(A) 15 U.S.C. § 7704(b)(1)(A)(i) 15 U.S.C. § 7704(b)(1)(A)(ii) 15 U.S.C. § 7704(b)(2) 15 U.S.C. § 7704(b)(3)	Settlement. Discovery.
EarthLink, Inc. v. Omagus, Inc.; James McCalla; and John Does 1-5. (N.D. Ga. filed Feb. 22, 2005)	Mortgage leads	15 U.S.C. § 7704(a)(1) 15 U.S.C. § 7704(a)(2) 15 U.S.C. § 7704(a)(3)(A)(i) 15 U.S.C. § 7704(a)(3)(A)(ii) 15 U.S.C. § 7704(a)(4)(A) 15 U.S.C. § 7704(a)(5)(A) 15 U.S.C. § 7704(b)(1)(A)(i) 15 U.S.C. § 7704(b)(1)(A)(ii) 15 U.S.C. § 7704(b)(2) 15 U.S.C. § 7704(b)(3)	Default judgment. Discovery.
America Online, Inc. v. Christopher William Smith; Advistech, S.A.; and John Does 1-20. (E.D. Va. Mar. 29, 2005)	Cable descramblers and sexually-oriented content	15 U.S.C. § 7704(a)(1) 15 U.S.C. § 7704(a)(2) 15 U.S.C. § 7704(a)(3) 15 U.S.C. § 7704(a)(5)	Discovery.

Caption	Goods or Services	CAN-SPAM Violations Alleged	Status
Microsoft Corp. v. Felipe Garcia; Joan Doe Garcia; David Peterson; Judy Doe Peterson; Robert Smoley; Jane Doe Smoley; Global Group International, LLC; and John Does 1 - 20. (W.D. Wash. filed Mar. 31, 2005)	Prescription drugs	15 U.S.C. § 7704(a)(1) 15 U.S.C. § 7704(a)(2) 15 U.S.C. § 7704(a)(3) 15 U.S.C. § 7704(a)(5) 15 U.S.C. § 7704(b)(3)	Discovery.
America Online, Inc. v. Matthew Bagley and John Does 1-10. (E.D. Va. Apr. 21, 2005)	Prescription drugs	15 U.S.C. § 7704(a)(1) 15 U.S.C. § 7704(a)(3) 15 U.S.C. § 7704(a)(5)	Discovery.
Microsoft Corp. v. Ryan Pitylak; Mark Trotter; Leadplex, Inc.; Leadplex, LLC; Payperaction, LLC; and John Does 1 - 20. (W.D. Tex. filed May 23, 2005)	Mortgates, debt consolidation and online dating services	15 U.S.C. § 7704(a)(2) 15 U.S.C. § 7704(a)(3) 15 U.S.C. § 7704(a)(5)	Discovery.
Microsoft Corp. v. Jumpstart Technologies, LLC and John Does 1 - 20. (N.D. Cal. filed July 14, 2005)	Various goods, including mail-order coffee, vacations, loan consolidation, and credit gift cards	15 U.S.C. § 7704(a)(2) 15 U.S.C. § 7704(a)(5)	Discovery.

Appendix 7: States' CAN-SPAM Cases

January 1, 2004 through September 1, 2005

Listed chronologically by date filed[1]

Caption	Goods or Services	CAN-SPAM Violations Alleged	Status
Washington v. AvTech Direct d/b/a AvTech Computers and Educational Purchasing Services; Arlene Sediqzad; Gary Hunziker; MD&I Corporation; and Min Hui Zhao. (W.D. Wash. filed Oct. 26, 2004)	Desktop computer sales targeted to non-profit groups	15 U.S.C. § 7704(a)(1) 15 U.S.C. § 7704(a)(2) 15 U.S.C. § 7704(a)(4)(A)(i)	Discovery.
Texas v. Ryan Pitylak; Mark Trotter; Leadplex, Inc.; Leadplex, LLC; Payperaction, LLC; and Eastmark Technology Limited, LLC. (W.D. Tex. filed Jan. 13, 2005)	Numerous types of services, including mortgage services, debt counseling, and warranty services	15 U.S.C. § 7704(a)(2) 15 U.S.C. § 7704(a)(5)	Discovery.
FTC and California v. Optin Global, Inc.; Vision Medial Limited, Corp.; Rick Yang; and Peonie Pui Ting Chin. (N.D. Cal. filed Apr. 12, 2005)	Various products, including auto warranties, pharmaceutical products, online college degree programs, and mortgage services	15 U.S.C. § 7704(a)(1) 15 U.S.C. § 7704(a)(2) 15 U.S.C. § 7704(a)(3) 15 U.S.C. § 7704(a)(4)(A)(i) 15 U.S.C. § 7704(a)(5)(A)(i) 15 U.S.C. § 7704(a)(5)(A)(ii) 15 U.S.C. § 7704(a)(5)(A)(iii)	Discovery.

1. State cases filed in state court, rather than federal court, include:
   - *Massachusetts v. DC Enterprises and William Carson*. Suffolk superior court; filed June 30, 2004, alleging violations of 15 U.S.C. §§ 7704(a)(1), 7704(a)(3)(A)(i) and (ii), and 7704(a)(5)(A)(i) and (iii) for mortgage brokering services. Settlement announced Oct. 7, 2004 including $25,000 civil penalty and injunction;
   - *Florida v. Scott Filary and Donald Townsend*. Circuit court for 13th Judicial Circuit, Hillsborough County, Fla.; filed April 4, 2005, alleging violations of 15 U.S.C. §§ 7704(a)(1), 7704(a)(2), 7704(b)(1)(A)(ii), 7704(b)(3), and 7705 for various products, including prescription drugs, cigarettes, downloads, e-books, and cash advances; and
   - *Massachusetts v. Leo Kuvayev; Vladislav Khokholkov; Anna Orlova; Pavel Tkachuk; Michelle Marco; Dennis Nartikoev; Pavel Yashin; 2K Services, Ltd.; and Ecash Pay, Ltd.* Suffolk superior court; filed May 11, 2005, alleging violations of 15 U.S.C. §§ 7704(a)(1), 7704(a)(3)(A)(i) and (ii), 7704(a)(5)(A)(i) and (iii), and 7704(b)(1) for counterfeit drugs, pirated software, pornography, and mortgage loans.


sp@m.filter
dom@in.se
priv@cy.enforce@bility
rel@y.server
f@lse.positive
inbox.sp@m
cy.filter.com
bayesi@n.filter
zombie.proxy
children.inbox
dom@in.security
anonymous.em@il
he@ders.em@il.com
priv@cy.com
technic@l.authentic@tion
sp@m.dom@in
em@il.priv@cy.com
dom@in.security.com
practic@l.sp@m.c
pr@ctical.technic@l
security.e