Subject Line Labeling As A Weapon Against Spam

A Report To Congress

Federal Trade Commission
June 2005

Subject Line Labeling As a Weapon Against Spam

A CAN-SPAM Act Report to Congress

June 2005

Federal Trade Commission

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

Table of Contents

Executive Summary i

I. Introduction and Overview 1

II. Subject Line Labeling Laws in the States and in Other Countries 3

A. State Subject Line Labeling Laws 3

1. Objectives of State Subject Line Labeling Requirements 5
2. Enforcement of State Subject Line Labeling Requirements 5
3. Effectiveness of State Subject Line Labeling Requirements 6

B. Subject Line Labeling Laws in Other Countries 7

III. The Commission Recommends Against Mandatory Subject Line Labeling 9

A. Mandatory Subject Line Labeling Is Likely Not an Effective Tool For ISPs To Block and Filter Spam 10

1. Mandatory subject line labeling will not enhance ISPs' current techniques for combating spam 10
2. Mandatory subject line labeling is an ineffective tool for ISPs because spammers will not comply with a labeling requirement 13

B. Practical and Technological Concerns with Subject Line Labeling Requirements 15

C. Mandatory Subject Line Labeling Would Not Strengthen Anti-Spam Law Enforcement 17

IV. Conclusion 18

Appendix 1: List of Interviews

Appendix 2: Part III of the Commission's National Do Not Email Registry Report

Concurring Statement of Commissioner Pamela Jones Harbour

Dissenting Statement of Commissioner Jon Leibowitz

Executive Summary

The Federal Trade Commission (the "FTC" or "Commission") submits this Report pursuant to Section 11(2) of the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (the "CAN-SPAM Act"), 15 U.S.C. § 7710(2) (2003), which requires the Commission to submit "a report that sets forth a plan for requiring commercial electronic mail to be identifiable from its subject line . . . or an explanation of any concerns the Commission has that cause the Commission to recommend against the plan."

A subject line labeling requirement would compel senders of unsolicited commercial email ("UCE") to include specific characters, such as "ADV," in the subject lines of their messages. The idea is that subject line labeling could make it easier for Internet Service Providers ("ISPs") to identify and screen out unwanted UCE, and for consumers to block or segregate UCE, or to tell at a glance whether individual messages that reach their in-boxes are commercial. Thus, subject line labeling may appear to offer a simple legislative fix, theoretically making it easy to either completely block all unwanted commercial email or to segregate UCE from other email messages.

The Commission, however, strongly doubts that such an outcome would result. The Commission comes to this conclusion after examining the likely benefits of an ADV labeling requirement applicable to all UCE, including email messages sent by legitimate marketers. Experience with subject line labeling requirements in the states and in other countries does not support the notion that such requirements are an effective means of reducing spam through more efficient sorting or filtering. Indeed, spam filters widely available at little or no cost (through ISPs or commercial companies) more effectively empower consumers to set individualized email preferences to reduce unwanted UCE from both spammers and legitimate marketers. Mandatory subject line labeling, by comparison, would be an imprecise tool for filtering and sorting that, at best, might make it easier to segregate *labeled* UCE from *unlabeled* UCE. This is because it is extremely unlikely that outlaw spammers would comply with a requirement to label the email messages they send. By contrast, legitimate marketers likely *would* comply with a subject line labeling requirement. As a result, if ISPs were to filter based on the subject line label – or if consumers were to set their personal email programs to direct labeled email messages to their junk mail folders – then labeled UCE messages sent by law-abiding senders would be filtered out. Meanwhile, unlabeled UCE messages sent by outlaw spammers would still reach consumers' in-boxes.

Nor would noncompliance carry any negative consequences for a spammer, because subject line labeling would do nothing to enhance the ability of law enforcers to track down and exact a penalty from those who do not comply. Mandatory subject line labeling would merely add another "per se" violation that could be alleged against a spammer, if and when the spammer is found.

Ultimately, therefore, the Commission believes that although a labeling requirement may allow those individual consumers who wish to avoid UCE from law-abiding marketers to filter such UCE, consumers already have technological options to identify UCE sent by law-abiding marketers. In addition, a labeling requirement holds little promise as a means of ameliorating the spam problem. Therefore, the Commission continues to believe that emphasis should be placed on encouraging industry to develop alternatives, such as email authentication, in lieu of a requirement for subject line labeling.

I. Introduction and Overview

The Federal Trade Commission (the "FTC" or "Commission") submits this Report pursuant to Section 11(2) of the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (the "CAN-SPAM Act"), 15 U.S.C. § 7710(2) (2003), which requires the Commission to submit "a report that sets forth a plan for requiring commercial electronic mail to be identifiable from its subject line, by means of compliance with Internet Engineering Task Force Standards, the use of the characters 'ADV' in the subject line, or other comparable identifier, or an explanation of any concerns the Commission has that cause the Commission to recommend against the plan."

In preparing this Report, the Commission used a number of techniques to obtain information from numerous individuals and organizations. First, in January and February 2005, the Commission interviewed thirty individuals representing nineteen organizations, including consumer groups, privacy groups, email marketers, Internet Service Providers ("ISPs"), and technologists.[1] A court reporter transcribed these interviews.[2]

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.[3] The 6(b) Orders required the ISPs to provide detailed information regarding their anti-spam technologies, volume and types of spam reaching their mail servers, and email authentication testing data.[4]

[1] A complete list of interviewees has been attached to this Report as Appendix 1.

[2] Citations to these transcripts identify the organization, representative from the organization, and page number of the transcript. For instance, the citation "Microsoft: Katz, 16," would refer to a statement made by Microsoft employee Harry Katz on page 16 of the transcript. The Commission has posted the transcripts online at http://www.ftc.gov/reports/advlabeling/xscripts/index.html.

[3] The Commission issued 6(b) Orders to America Online ("AOL"), SBC, Road Runner, Bell South, Verizon, Cox, Earthlink, Microsoft, and United Online ("UOL"). The Commission, in preparation for its National Do Not Email Registry Report to Congress, previously issued 6(b) Orders to AOL, Comcast, Earthlink, Microsoft, MCI, UOL, and Yahoo!.

[4] To ensure that their anti-spam techniques do not become known to spammers, 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.

Third, the Commission solicited comments from the general public in a March 10, 2004, Advance Notice of Proposed Rulemaking concerning CAN-SPAM Act rules and mandatory reports to Congress (the "ANPR").[5] By the close of the comment period, the Commission had received 104 comments regarding subject line labeling.[6]

By a large majority, the industry sources consulted in preparing this Report urged that a subject line labeling requirement would not be an effective anti-spam measure. Representatives of several consumer organizations, however, expressed support for such a requirement, as did the majority of individual consumers who commented on the issue.[7] Some consumer representatives also acknowledged, however, that subject line labeling has potential drawbacks.[8]

Section II of this Report discusses the states' experiences with mandatory subject line labeling laws and similar laws in other countries. Section III presents three reasons not to impose subject line labeling. Such a requirement: (1) would not be an effective tool for ISPs to block and filter spam because it would not enhance ISPs' current anti-spam techniques; (2) has technological and

[5] Citations to these comments identify the organization or person submitting the comment and the page number of the comment. For instance, the citation "Wells Fargo-Comment, 3" refers to page 3 of the comment submitted by Wells Fargo. The Commission has posted the comments online at http://www.ftc.gov/os/comments/canspam/index.htm.

[6] Forty-seven comments were from various industry groups and trade associations, of which 40 opposed any type of subject line labeling. Of the remaining 57 comments from individuals, which varied in scope and substance, over half generally supported subject line labeling.

[7] Electronic Privacy Information Center ("EPIC"): Hoofnagle, 17, 20-21; Privacy Clue: Everett-Church, 23; Consumer Action: Sherry, 5-6; Consumer Federation of America ("CFA"): Fox, 6. Consumers wanted an "ADV" label in order to allow them to filter, delete, or decide whether to read unsolicited commercial email ("UCE") messages. *See, e.g.*, "It is important that every UCE message contain an identifier in the subject line (like the "ADV" that was common in many state laws prior to the CAN-SPAM Act) so that those who do not want spammers sending us messages which, like junk faxes, utilize our property and resources to deliver their unwanted messages, can exclude all UCE." Sutton, Jimmy- Comment, 1; "[R]equiring ADV in the subject line of a commercial message would give the recipients the ability to take full control of whether or not they wish to view the advertisements." McCoy, Daryl- Comment, 1; "I want to make a choice of what I read or watch on my computer the same [way] I cho[o]se what TV station or newspaper [to watch or read]. Hathaway, Tommy- Comment, 1.

[8] "Consumer Action realizes that many people are saying that ADV labeling, such a requirement won't help stop bad actors. It might legitimize spam and it may even be a violation of free speech, but we really feel that even if it does not stop all the bad actors, a labeling requirement will help e-mail users to identify many messages they would prefer not to receive. Consumers can choose to ignore the spam by filtering their e-mail with the subject line ADV, or whatever the requirement becomes." Consumer Action: Sherry, 5-6. "Our original preference was that commercial e-mail be set up on an opt-in basis, so that consumers had control over the e-mail coming in to their mail boxes. Having failed to win that, and having CAN-SPAM on the books as is, the least we can do is label commercial e-mail so the consumers have a bit more information to use, and, of course, the idea being if you can filter out messages based on something that's in the subject line, that will empower consumers to have a bit of control over this." CFA: Fox, 6.

practical implementation problems; and (3) would not strengthen anti-spam law enforcement. Section III also discusses technological alternatives to subject line labeling that hold better promise of reducing the burden of spam for consumers.

In order to distinguish between legitimate marketers' unsolicited commercial email ("UCE") messages – which some consumers may want to receive and others may not – and the deceptive, fraudulent, or misleading UCE messages typically containing falsified header information,[9] this report will use "spam" to refer only to the fraudulent, deceptive, or misleading email messages that clog so many in-boxes.

II. Subject Line Labeling Laws in the States and in Other Countries

A number of jurisdictions, both within the United States and abroad, have enacted subject line labeling laws as a tool to help combat spam. Experience in these jurisdictions indicates that labeling laws have had little impact on the fight against spam.

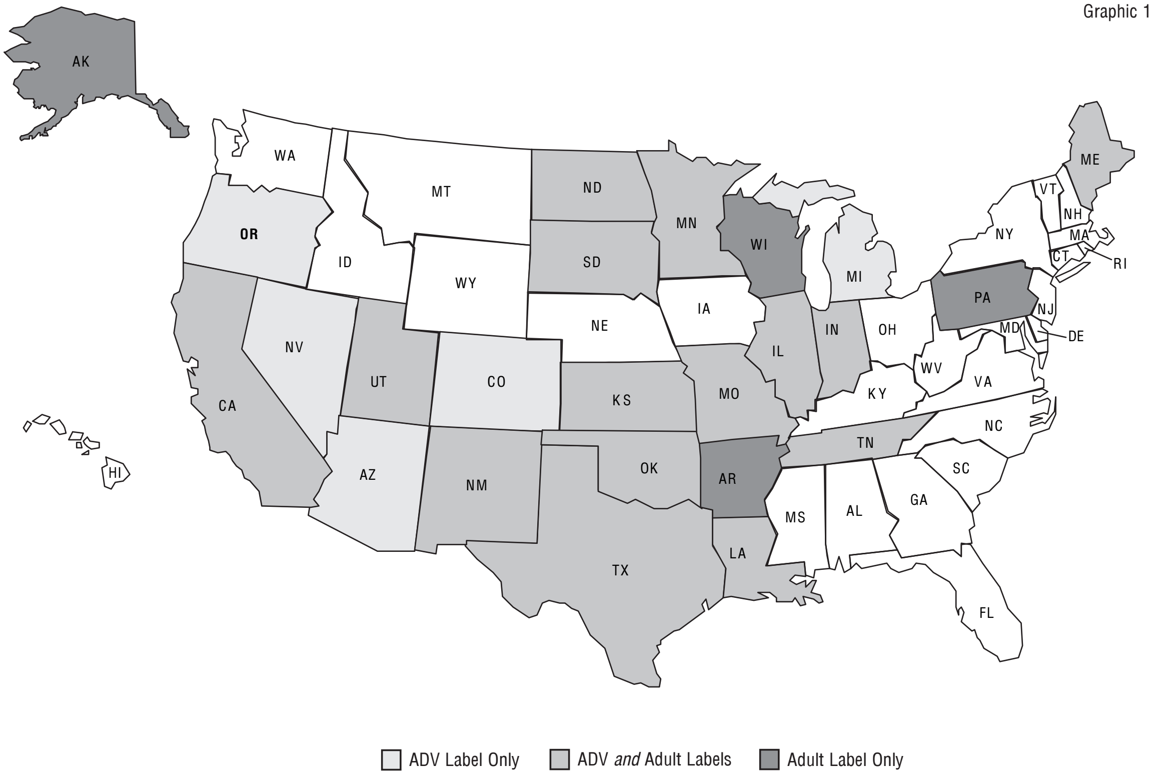
A. State Subject Line Labeling Laws

Thirty-seven states have statutes that directly or indirectly regulate commercial electronic mail. Of these, 20 required that commercial email be labeled in its subject line, typically with the characters "ADV:," prior to the passage of the CAN-SPAM Act, which preempted such requirements.[10] The majority of these labeling requirements applied to UCE. Other states had labeling requirements that applied only to sexually-explicit commercial email. These laws required such messages to carry the label "ADV:ADLT" or other similar variations.

[9] *See* Appendix 2. Appendix 2 contains Part III of the Commission's June 2004 Report to Congress on a National Do Not Email Registry, which discusses in great detail the many techniques that spammers use to bypass filters and reach consumers' in-boxes.

[10] Section 7707(b) of the CAN-SPAM Act preempts any state statute or regulation that "expressly regulates the use of electronic mail to send commercial messages" except to the extent that such statutes prohibit falsity or deception in a commercial email message. The Act does not preempt state laws to the extent that those laws relate to fraud or computer crime. 15 U.S.C. § 7707(b)(2)(B) (2003).

Graphic 1



The majority of the state commercial email labeling laws were not in effect for very long before they were preempted by the CAN-SPAM Act on January 1, 2004. The first state spam statute to include an ADV labeling requirement was enacted in 2000.[11] Four other states followed suit in 2002,[12] but the majority of the state labeling laws – in fourteen states – were not enacted until 2003,[13] with one state enacting a labeling law in 2004.[14] (*See* Graphic 1 for a summary of the various state labeling laws.)

[11] Colorado enacted a spam statute in 2000 that included a subject line labeling requirement. Colo. Rev. Stat. § 6-2.5-103 (2000).

[12] These states include: Kansas (Kan. Stat. Ann. § 50-6,107 (2002)); Minnesota (Minn. Stat. § 325F.694 (2002)); South Dakota (S.D. Codified Laws § 37-24-6 (2002) (expired 2004)); and Utah (Utah Code Ann. § 13-36-103 (2002) (repealed 2004)).

[13] These states include: Arizona (Ariz. Rev. Stat. § 44-1372.01 (2003)); California (Cal. Bus. & Prof. Code § 17538.4 (2003) (amending 1998 Law to require subject line labeling) (repealed 2003)); Indiana (Ind. Code § 24-5-22-8 (2003)); Louisiana (La. Rev. Stat. Ann. § 51:1741.1 (2003)); Maine (Me. Rev. Stat. Ann. tit. 10 § 1497 (2003)); Michigan (Mich. Comp. Laws § 445.2503 (2003)); Missouri (Mo. Rev. Stat. § 407.1138 (2003) (amending 2000 Law to require subject line labeling)); Nevada (Nev. Rev. Stat. § 41.730 (2003) (amending 1997 Law to require subject line labeling)); New Mexico (N.M. Stat. Ann. § 57-12-23 (2003)); North Dakota (N.D. Cent. Code § 51-27-04 (2003) (expired 2004)); Oklahoma (Okla. Stat. tit. 15 § 776.6 (2003) (amending 1999 Law to require subject line labeling)); Oregon (Or. Rev. Stat. § 646.607 *as amended by* Or. Laws Ch. 759 (2003)); Tennessee (Tenn. Code Ann. § 47-18-2501 (2003) (amending 1999 Law to require subject line labeling)); and Texas (Tex. Bus. & Comm. Code Ann. § 47-18-2501 (2003)).

[14] Illinois amended its existing spam statute to include a subject line labeling requirement in 2004. Ill. Comp. Stat. tit. 815 § 511/10 (2004) (amending 1999 Law to require subject line labeling).

1. Objectives of State Subject Line Labeling Requirements

Although legislative history discussing the rationale and basis underlying state labeling laws is scant, the legislative history in two states, Arizona and California, sheds some light on the objectives of state labeling requirements. Legislators in Arizona believed that an ADV labeling requirement would facilitate spam investigations because it would simplify the task of assessing whether a violation had occurred.[15] Some sources consulted in preparing this Report expressed the theme that subject line labeling could provide an additional "hook" for law enforcement in the form of an additional violation to charge.[16]

The California legislative history suggests that the State Assembly was fully aware of the likely limitations of subject line labeling. The report of the Committee on Consumer Protection, Governmental Efficiency, and Economic Development of the California Assembly noted that critics of the bill questioned whether the labeling provisions could be effectively enforced against spam that originates from outside California.[17] We believe that a national subject line labeling requirement raises the same concern because spam often originates overseas.

2. Enforcement of State Subject Line Labeling Requirements

Very few states were able to bring enforcement actions charging violations of their subject line labeling requirements under their state spam laws. Commission staff contacted the attorney general offices of all 20 states that had enacted subject line labeling laws; several of these offices noted that their statutes were preempted by the CAN-SPAM Act before they were able to file enforcement actions.[18]

Staff found that only one state with a labeling requirement, California, successfully brought an action under its general spam statute. The complaint alleged violations of virtually all provisions of the California statute, including

[15] *Fiscal Analysis of Arizona House Bill 2107*, 46th Legis. Sess. 1 (Ariz. 2003), *available at* http://www.azleg.state.az.us.

[16] Internet Engineering Task Force ("IETF"): Hardie, 12; EPIC: Hoofnagle, 20; CFA: Fox, 8.

[17] *Appropriations Committee Fiscal Summary of Assembly Bill 1676*, 1997-1998 Legis. (Cal. 1998), *available at* http://www.leginfo.ca.gov. Although the legislative history is limited with respect to the labeling provision of the anti-spam statute, the history shows that the California Internet Industry Alliance opposed California's ADV labeling requirement because labeling would be potentially damaging to Internet users, could be misunderstood by foreign Internet users, and would conflict with labeling requirements of other states. *Senate Comm. on Bus. and Professions Bill No. AB 1676*, 1997-1998 Legis. (Cal. 1998).

[18] These states include Illinois, Kansas, Oklahoma, Tennessee, Texas, and Utah.

ADV labeling violations. The Court entered a final judgment in that case and issued a permanent injunction ordering, among other relief, a $2 million civil penalty.[19] Although Missouri attempted to bring two enforcement actions under its general spam law – including violations of the labeling requirement – state authorities were unable to execute service on the defendants.[20] State attorney general offices emphasized the difficulty they experienced in seeking to enforce spam laws, chiefly because of the obstacles encountered in trying to identify and locate the spammers.[21]

3. Effectiveness of State Subject Line Labeling Requirements

The CAN-SPAM Act's findings specifically state:

> Many States have enacted legislation intended to regulate or reduce unsolicited commercial electronic mail, but these statutes impose different standards and requirements. As a result, they do not appear to have been successful in addressing the problems associated with unsolicited commercial electronic mail, in part because, since an electronic mail address does not specify a geographic location, it can be extremely difficult for law-abiding businesses to know with which of these disparate statutes they are required to comply.[22]

Although there do not appear to be any empirical studies or reports on the efficacy of the various state labeling requirements during the period when they were in effect, FTC staff found in its own April 2003 "False Claims in Spam" study that only two percent of email messages that the Commission reviewed contained an "ADV" label in their subject lines.[23] A representative from the Internet Commerce Coalition ("ICC") similarly stated in an interview that a relatively small percentage of email was in compliance with state labeling

[19] *People v. Willis*, No. 1-02-CV811428 (Cal. Super. Ct. 2002).

[20] *Missouri v. Nixon*, No. 034-02424 (Mo. Cir. Ct. 2003); *Missouri v. FunDetective.com*, No. 034-02428 (Mo. Cir. Ct. 2003).

[21] States raising this concern include Illinois, Kansas, and Maine. *See also* FTC's National Do Not Email Registry Report, at pp. 23-25, *available at* http://www.ftc.gov/reports/dneregistry/report.pdf.

[22] 15 U.S.C. § 7701(2)(a)(11) (2003).

[23] False Claims in Spam, 11. The Commission has posted the False Claims in Spam report online at http://www.ftc.gov/reports/spam/030429spamreport.pdf. At the time the Commission's report came out, there were five states that had labeling laws in effect: Kansas, Minnesota, South Dakota, Utah, and Colorado.

laws and that the labeling requirements were "highly ineffective."[24] Based on interviews conducted in preparation for this Report, the Commission discovered that many ISPs, both large and small, chose not to filter based on the states' ADV labeling requirements when they were in effect.[25] Therefore, the low number of labeled messages reviewed is probably not due to ISP subject line filtering.

B. Subject Line Labeling Laws in Other Countries

South Korea, Japan, and most member states of the European Union have implemented anti-spam regulations in recent years. Most European countries generally prohibit the sending of UCE to consumers unless the consumer has given prior consent to receiving such emails.[26] In addition, some European countries, such as the United Kingdom ("U.K."), Finland, Norway, and Poland, have enacted laws requiring a label in the subject line of a UCE.[27] Because UCE legally cannot be sent to consumers without their prior consent in these countries, however, the labeling requirement applies only in limited circumstances. For example, it may apply when an unsolicited commercial message is sent to a business.[28]

In any event, there appears to have been little compliance with such labeling requirements in Europe. For example, in a 2003 report, a U.K. parliamentary committee stated that:

> [m]ost unsolicited email sent within the UK, even that which is sent by organisations which otherwise regard themselves as acting within the law, fails to abide by [the requirement that] any unsolicited commercial communication must be 'identifiable clearly and unambiguously as soon

[24] ICC: Halpert, 8. *See also*, MCI: Mansourkia, 7; Email Service Provider Coalition ("ESPC"): Hughes, 13. Similarly, a representative from MCI stated that after examining a subset of emails about which MCI received complaints, some of them had an "ADV" label, but the majority did not. MCI: Mansourkia, 7. In addition, the executive director of the ESPC stated, "I think it's fair to say that during that time [when state labeling laws were in effect] we saw exponential growth in spam and at the same time we didn't see any ADV labels showing up in inboxes around the United States." ESPC: Hughes, 13.

[25] AOL: Jacobsen, 5; Telephone conversation with Aristotle: Bowles; Earthlink: Youngblood, 7. The representatives from AT&T and MCI were not sure if they filtered based on a subject line label. AT&T: Israel, 7; MCI: Mansourkia, 7. UOL is the only ISP that affirmatively stated that it used the "ADV" label as one basis for filtering. UOL: Squire, 8.

[26] *See* Background Paper for the OECD Workshop on Spam 19-20, Annex, DSTI/ICCP2003(10)/FINAL (Jan. 22, 2004), *available at* http://www.olis.oecd.org/olis/2003doc.nsf/LinkTo/dsti-iccp(2003)10-final.

[27] *Id.* at 22.

[28] *Id.* at 32.

> as it is received.' For example, an email could meet these requirements by the presence of an ADV: prefix on its subject line.[29]

Currently, we are aware of two countries – Japan and South Korea – that have enacted specific email labeling requirements applicable to a broad range of commercial email messages. In April 2002, Japan passed its "Law on Regulation of Transmission of Specified Electronic Mail." Among other things, it requires UCE to be labeled in its subject line with five Japanese characters and a star that translates into "unsolicited email advertisement."[30] In Japan, data suggests that spam did not decrease after its labeling requirements went into effect.[31]

Korea promulgated an anti-spam law in 2001 that requires that the term "ADV" in Korean characters be included in the subject line of UCE.[32] After finding that many spammers were labeling their messages using irregular characters, such as "A*D*V*," the Korean legislature passed new measures in 2002 that made such alterations illegal.[33] These measures also required that adult-oriented commercial email be labeled "ADLT" in Korean characters.[34]

Because the amount of spam did not decrease, the Korean National Assembly revised the law in late 2002, and mandated that the "@" symbol also be included in the subject line of commercial email messages.[35] Although Korean government officials acknowledged that spam continued to increase under the prior law, we

[29] Spam, A Report of the All Party Internet Group 9, *available at* http://www.apig.org.uk/spam_report.pdf.

[30] *Tokutei Denshi-Mail-no Soushin-no Tekisei-ka-tou-ni-kansuru Houritsu [Law on Regulation of Transmission of Specified Electronic Mail]*, Law No. 26, April 17, Year Heisei 14 (2002).

[31] *The Current Status and the Future Task Regarding SPAM Mail*, Ministry of Econ., Trade, and Indus. ("METI"), Dec. 6, 2004, at 9-10.

[32] *See* "The Act on Promotion of Information and Communication and Communications Network Utilization and Information Protection of 2001," Article 50, cited in http://www.spamcop.or.kr/eng/m_2.html and Chung, Hyu-Bong, *Anti-Spam Regulations in Korea*, Korea Info. Sec. Agency (KISA), Apr. 15, 2003, at 5, *available at* http://cauce.mail.daum.net/meeting/hbchung.doc.

[33] Chung, at 5.

[34] *Id*.

[35] "Because the methods or skills of the transmission of spam are increasingly becoming diversified technically, and since spammers typically disregard the seriousness of spam, the amount of spam did not decrease. For this reason, the National Assembly promulgated a revised Act . . . on December 18, 2002, to tighten control over spam." *See* Korea Spam Response Center, Anti-Spam Activities in Korea, *available at* http://www.spamcop.or.kr/eng/m_2.html. This revised Act also established criminal penalties and raised existing fines.

are not aware of any studies that have examined the effectiveness of this new requirement.[36]

III. The Commission Recommends Against Mandatory Subject Line Labeling

A statutory requirement that UCE bear a subject line label would sweep broadly. In the floor discussion preceding passage of the CAN-SPAM Act, Senator McCain contended that unsolicited email may be welcomed by some but condemned by others, making the task of email regulation a difficult one:

> [T]he word 'spam' means different things to different people. The Federal Trade Commission defines spam generally as 'unsolicited commercial email' and some Americans do not want any of it. Other consumers like to receive unsolicited offers by email; to these consumers, spam means only the unwanted fraudulent or pornographic email that also floods their inbox.
>
> Many American businesses view email over the Internet as a new medium through which to market or communicate more effectively with customers. To them, this type of communication is not spam, but commercial speech protected by the First Amendment. The Direct Marketing Association reports that 37 percent of consumers it surveyed have bought something as a result of receiving unsolicited email from marketers.
>
> Internet service providers are the businesses caught in the middle, forced every day to draw distinctions between what they perceive as legitimate email and what is spam. In this environment, the risk of ISPs blocking legitimate mail that consumers depend on, such as purchase receipts or healthcare communications, is as much a concern as the prospect of failing to block as much spam as possible in the face of consumer demand.[37]

[36] KISA: Chung – Spam Forum (May 2, 2003), 111-12. The Spam Forum was a three-day workshop held by the FTC in the spring of 2003. The Commission posted these transcripts online at http://www.ftc.gov/bcp/workshops/spam. Citations to the transcripts of the Spam Forum identify the speaker's organization and name, the date of the Forum, and the page number on which the statement can be found. For instance, the citation "KISA: Chung – Spam Forum (May 2, 2003), 167" would refer to a statement made by KISA employee Hyu-Bong Chung that can be found on page 167 of the May 2, 2003 Spam Forum transcript.

[37] 108th Congress, Cong. Rec. S13020 (daily ed. Oct. 22, 2003) (statement of Sen. McCain), *available at* http://thomas.loc.gov. In a 2003 study of online behaviors, 92 percent of email users believed that spam is UCE from a sender they do not know or cannot identify. Pew Internet and American Life, *Spam: How it is Hurting Email and Degrading Life on the Internet*, Oct. 22, 2003, 10, *available at* http://www.pewinternet.org/reports/pdfs/PIP_Spam_Report.pdf.

As noted previously, this Report uses the term "spam" to refer only to the fraudulent, deceptive, or misleading email messages that typically contain falsified header information and other core violations of CAN-SPAM. Thus, spam is distinguished from legitimate marketers' UCE messages – which some consumers may want to receive and others may not.

Theoretically, ISPs and consumers could easily filter out any email with a subject line label. As explained in this section, however, there are three important considerations that argue against imposition of mandatory subject line labeling.

First, subject line labeling is unlikely to enhance the sophisticated filtering strategies that ISPs use and are constantly improving. Further, subject line labeling likely would have little value for ISPs because there is no reason to expect that outlaw spammers, who are already violating the CAN-SPAM Act and possibly other laws as well, would obey a subject line labeling requirement. Second, there are other potential practical or technological problems with implementing a subject line labeling requirement. Third, and finally, mandatory subject line labeling would not contribute in any material way to the strengthening of anti-spam law enforcement.

A. Mandatory Subject Line Labeling Is Likely Not an Effective Tool For ISPs To Block and Filter Spam

1. Mandatory subject line labeling will not enhance ISPs' current techniques for combating spam

The ISP industry's standard practice is to prohibit unsolicited bulk email.[38] ISPs and email filtering companies attempt to enforce this prohibition mainly through a multi-layered approach that involves email blocking and filtering software.[39] Many ISPs' first layer of defense is email blocking.[40] 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 Internet Protocol ("IP")

[38] *See, e.g.*, acceptable use policies of 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).

[39] 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 in-box. Confidential 6(b) Order Responses. UOL: Squire, 8.

[40] Confidential 6(b) Order Responses.

address that the ISP has determined to be an open relay or open proxy used by spammers,[41] or because an IP address or domain is associated with the sending of 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 blocking efforts.[42]

Although ISPs generally have a policy that prohibits unsolicited bulk email, some use "whitelists" to ensure that email messages initially will not be blocked based on the IP address. A whitelist is a compilation of marketers' IP addresses that an ISP will allow into its networks. Because an ISP has no way of determining on its face whether an email is "solicited" or "unsolicited," whitelisting is a way to ensure that ISPs do not mistakenly filter out email from law-abiding bulk marketers that comply with the ISPs' policies. For example, AOL has a whitelisting program that allows bulk emailers to send a high volume of email messages, provided they adhere to several requirements, including: sending a minimum of 100 emails per month; sending only CAN-SPAM compliant email; and sending only "permission-based" email.[43]

Whitelisting enables legitimate bulk mailers to send their messages without encountering blocking. However, in addition to blocking email at the point of entry into an ISP's network, most ISPs filter email once it is in their networks based upon their own customers' complaints.[44] ISPs use complaint data in a variety of ways – for example, to support Bayesian filtering. Bayesian filtering is 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.[45] ISPs use customer complaint data to filter out email messages about which their customers are most concerned.[46]

[41] For a description of open relays and open proxies, *see* Appendix 2.

[42] SpamCop: Haight – Spam Forum (May 1, 2003), 118.

[43] AOL's whitelist program can be viewed at http://postmaster.info.aol.com/tools/whitelist_guides.html.

[44] Confidential 6(b) Order Response.

[45] David Mertz, *Spam Filtering Techniques: Comparing a Half-Dozen Approaches to Eliminating Unwanted Email*, Gnosis Software, Inc., Aug. 2002, *available at* http://www.gnosis.cx/publish/programming/filtering-spam.html. *See also,* Joshua Goodman, David Heckerman and Robert Rounthwaite, "Stopping Spam: What Can Be Done to Stanch the Flood of Junk E-mail Messages?" *Scientific American*, Apr. 2004, *available at* http://www.sciam.com/article.cfm?articleID=000F3A4B-BF70-1238-BF7083414B7FFE9F). Mr. Heckerman manages the Machine Learning and Applied Statistics group at Microsoft Research. Mr. Goodman and Mr. Rounthwaite helped to organize the Microsoft product team that delivers the anti-spam technologies deployed in Exchange, Outlook, MSN, and Hotmail.

[46] Confidential 6(b) Order Responses.

Spammers' latest ploy involves taking control of innocent users' computers and using them to generate and send spam[47] – a practice known as creating "zombie drones" or "bot networks." In order to thwart this practice, many ISPs are implementing controls on outbound email messages originating from within their own networks and sent to other ISPs. These controls include monitoring outgoing email and blocking specific accounts that exceed some hourly or daily threshold for sending email.[48]

Business representatives commented that this multi-layered approach, combined with advances in blocking and filtering technology, is proving effective at combating spam. A Microsoft representative stated, for example, "[w]e think we're catching the majority of spam" and that Microsoft's filters' effectiveness had "improved incredibly" in the last two years.[49] Similarly, AOL has announced that its customers reported 75 percent less spam in their in-boxes and received 60 percent less spam in their junk email folders in 2004.[50] In June 2004, Microsoft announced that its SmartScreen filtering technology was blocking 95 percent of all spam coming into its Hotmail network.[51]

In addition, a representative from AOL stated that:

> if there are complaints that come in about a legitimate marketer, there are a variety of tools on the technology side and even in the consumer's hands to fix those problems, so [subject line labeling is] not a necessary tool. . .[F]or legitimate marketers who may make mistakes or generate complaints, there are ways already of dealing with those issues.[52]

[47] *See* Appendix 2. *See also, The Difficulties of Tracing Spam Email*, a report prepared by Dr. Dan Boneh of Stanford University for FTC staff preparing the FTC's Report to Congress on A CAN-SPAM Informant Reward System. Boneh's report can be found online at http://www.ftc.gov/reports/rewardsys/expertrpt_boneh.pdf; the FTC's report can be found online at http://www.ftc.gov/reports/rewardsys/040916rewardsysrpt.pdf.

[48] Confidential 6(b) Order Responses; Anick Jesdanun, *Battle Against Spam Shifts to Containment*, Apr. 15, 2005, *available at* http://abcnews.go.com/Technology/wireStory?id=673399.

[49] Microsoft: Katz, 10. In fact, "Microsoft IT believes that a multi-layered approach to messaging hygiene is essential. A single method, no matter how satisfactory, is simply not adequate to encounter the variation of risks associated with Internet mail." *Messaging Hygiene at Microsoft: How Microsoft IT defends against spam, viruses, and e-mail attacks*, at 7 (October 2004), *available at* http://www.microsoft.com/technet/itsolutions/msit/security/messaginghygienewp.mspx#EHAA.

[50] This later figure reflects the reduction in email deemed to be spam and sent to AOL members' spam folders, rather than their in-boxes. *America Online Announces Breakthroughs in Fight Against Spam*, Bus. Wire, Dec. 27, 2004.

[51] Bill Gates, *Preserving and Enhancing the Benefits of Email – A Progress Report*, June 28, 2004, *available at* http://www.microsoft.com/mscorp/execmail/2004/06-28antispam.asp.

[52] AOL: Jacobsen, 11.

2. Mandatory subject line labeling is an ineffective tool for ISPs because spammers will not comply with a labeling requirement

Subject line labeling seems appealing because ISPs theoretically could preset their filters to screen out all email messages containing a particular label. However, subject line labeling is a rather crude way to filter and likely would not be very effective to combat spam because it would not distinguish spam from legitimate marketers' UCE that some consumers may want to receive.[53] Only law-abiding commercial emailers would label their UCE. Spammers would simply ignore such a requirement. A representative from AOL stated, for example, that:

> a large proportion of the spam . . . coming over our [AOL's] network is from spammers who engage in fraud and falsification [and] are not going to . . . follow an ADV requirement . . . [W]hile we [AOL] may be able to identify marketers sending legitimate emails, it doesn't help us filter out the spam that most people are complaining about.[54]

Further, a representative from PrivacyClue noted:

> The reality is that most spammers these days are still engaged in activities that range from marginally legal to quite illegal, and as a result, failure to comply with ADV is no great leap for them to make . . .[55]

Because spammers are unlikely to comply with a labeling requirement that might result in automatic filtering of their email, filtering by ISPs based on a mandatory subject line label may have the unintended consequence of filtering out labeled UCE from legitimate marketers while inadvertently allowing fraudulent spam to appear in consumers' in-boxes.[56] Thus, if ISPs filtered all UCE messages with an "ADV" label, two undesirable side effects could occur: (1) consumers would likely never see an email message with a subject line label, and would be confused as to whether the absence of a label means that the message is not

[53] UOL: Squire, 24-25; Earthlink: Youngblood, 11-12, 15; AT&T: Israel, 12; Telephone conversation with Aristotle: Bowles.

[54] AOL: Jacobsen, 9. Representatives from both MCI and Microsoft agreed. MCI: Mansourkia, 9; Microsoft: Katz, 9.

[55] PrivacyClue: Everett-Church, 19-20.

[56] UOL: Squire, 25, 29; AT&T: Israel, 28; SkyList: Baer, 27.

fraudulent spam;[57] and (2) legitimate marketers, whose labeled UCE messages would be filtered, likely would be penalized through loss of some potential customers who might want to receive these marketers' UCE.[58] Consequently, subject line labeling would not likely add in any material way to the spam-fighting tools that ISPs already employ.

Proponents of subject line labeling, however, believe that labeling could provide a means for consumers to sort the contents of their in-boxes and more efficiently discard unwanted email.[59] Representatives of some consumer groups argue that the use by legitimate marketers of the "ADV" label would not only help consumers filter their emails, but would also help identify law-abiding marketers for consumers. One representative opined that "this [subject label] will help people realize, will help separate legitimate marketers from really, really, bad actors."[60] In addition, consumers could conclude by looking at emails from companies that put "ADV" in their messages that these companies are more interested in following the rules.[61] Subject line labeling could make consumers feel more comfortable in either opening the emails or opting out of receiving further emails without fears that they would be spammed further by deciding to unsubscribe. One participant from Microsoft noted that he could "see a label empowering consumers to sort mail or to perhaps place it in buckets more efficiently based on a label."[62]

However, consumers currently may use highly calibrated, personalized spam filters to limit or separate emails that they receive, including UCE from legitimate

[57] Experian: Hadley, 23-24; Earthlink: Youngblood, 11; UOL: Squire, 24-25; Telephone conversation with Aristotle: Bowles. Consumers using personal filters would likely have an equally difficult time distinguishing legitimate marketers' UCE from fraudulent spam. Some consumers who might want to see UCE from legitimate marketers might end up filtering labeled UCE messages that they actually want to see and be forced to sift through those unlabeled fraudulent spam messages they do not want to see. Electronic Frontier Foundation ("EFF"): Newitz, 7-8; AT&T: Israel, 30; MCI: Mansourkia, 14-15; ASRG: Levine, 11; Wells Fargo-Comment, 10; Key Corp.-Comment, 2; Newsletter and Electronic Publishers Assoc.-Comment, 8-9; Consumers Bankers Assoc.-Comment, 16; MasterCard-Comment, 9.

[58] DoubleClick: Berkower, 29; Experian: Hadley, 28; AT&T: Israel, 12 & 28 ("imposing the requirement and using it as a basis for filtering would, in effect, drive email marketing underground or out of legitimate channels."); Telephone conversation with Aristotle: Bowles; Earthlink: Youngblood, 19; Discover Bank-Comment, 4; US Email Service-Comment, 1; American Business Media-Comment, 8; Courthouse News Service-Comment, 4; Magazine Publishers of America-Comment, 13; Electronic Retailing Association-Comment, 13; MBNA-Comment, 13; Mastercard-Comment, 9.

[59] Consumer Action: Sherry, 5-6; CFA: Fox, 6.

[60] Consumer Action: Sherry, 12

[61] *Id.* at 13.

[62] Microsoft: Kornblum, 13.

marketers.[63] In fact, consumers can either obtain their own filtering software allowing them to block or sort out messages they do not want to receive,[64] or obtain personalized filtering services provided by their ISPs.[65] Commercially available products and services provided by ISPs may include: blocklists of known spammers updated continuously; customized filters to block specific words, images, domains, or senders; whitelists of particular desired senders; personalized Bayesian filtering; and junk folders where spam is quarantined.[66] Some ISPs even allow consumers to block all email coming from sources outside of the consumer's address book.[67] Thus, consumers who want to block or filter UCE, even from legitimate marketers, already have a number of options available to them. Consumers are more significantly empowered by sophisticated spam filters than by a one-size-fits-all "ADV" label, which casts all email as either advertising or something else.

B. Practical and Technological Concerns with Subject Line Labeling Requirements

Commenters raised three possible technological and practical concerns with subject line labeling requirements. First, the representative from the Coalition Against Unsolicited Commercial Email explained how subject lines in emails work:

> [There are] a whole sequence of technical conversations . . . between sending and receiving servers, and the 'to' and the 'from' address are primarily the only useful pieces of information that are transmitted before the body of the message along with the remainder of the headers, including the subject line, are transmitted in delivery . . . . [thus], the costs of receiving and storing and processing an Email message on the

[63] Consumers can also use non-technical methods to prevent spam. Some examples include: creating multiple email addresses to use exclusively for personal and online activities; creating an email address that is tough to crack, and avoiding posting email addresses in newsgroups and web pages. These and other non-technical ways to avoid spam are described in the FTC's publication *You've Got Spam: How to "Can" Unwanted Email* (April 2002) *available at* http://www.ftc.gov/bcp/conline/pubs/online/inbox.htm.

[64] EPIC: Hoofnagle, 17; Privacy Clue: Everett-Church, 23. Some filtering software is available for free and some software costs a fee. *See* http://spam.getnetwise.org/tools for a description of various spam fighting tools which could be used to block or delete all UCE.

[65] UOL: Squire, 29; Telephone conversation with Aristotle: Bowles; Confidential 6(b) Order Responses. For example, AOL provides a description of the personal spam tools it offers its subscribers at http://www.aol.com/product/spam.adp, and Microsoft provides a description of its personal spam tools at http://security.msn.com/articles/msmailprotect.armx.

[66] *See supra* notes 64 and 65.

[67] *See supra* note 65.

> receiving end have already been incurred by the time a subject line is available for filtering or blocking.[68]

Thus, if all senders of UCE – including fraudulent spammers – used a label in the subject line, and this label was used to filter out all UCE, ISPs would incur substantial bandwidth costs from receiving, storing, and processing the volumes of UCE.

Indeed, representatives of the Internet Engineering Task Force ("IETF")[69] contended that subject line labeling may make it more difficult for computers to perform the necessary operations for sending, receiving, and filtering email.[70] They argued that it can be difficult for a computer to perform multiple operations on a single subject line,[71] and that the more functions a computer is forced to perform on that subject line, the less effective it is at filtering.[72] Although IETF representatives clearly stated that they do not support subject line labeling, if Congress imposes such a requirement, then they recommend the label be placed in a separate header and not in the subject line.[73]

Finally, two participants at the FTC's Spam Forum in 2003 and a representative of the ASRG observed that an English language labeling requirement might be meaningless to non-English speakers, although presumably any labeling requirement would require that a label be in the same language that the email was sent in.[74]

[68] PrivacyClue: Everett-Church, 6.

[69] The IETF is an Internet-standards setting body.

[70] IETF: Malamud, 22-23; IETF: Moore, 19-20.

[71] For example, a computer may have to use the subject line to determine whether the email is in reply to a message, whether it is from a mailing list, and whether it has particular labels. IETF: Moore, 20-21.

[72] IETF: Malamud, 22-23. One member of the IETF submitted a proposal to the IETF outlining an alternative to subject line labeling that is currently on the standards track. IETF: Malamud, 24-25. *See* C. Malamud, A No Soliciting Simple Mail Transfer Protocol (SMTP) Service Extension, Sept. 2004, *available at* http://rfc3865.x42.com/.

[73] IETF: Malamud, 9; IETF: Moore, 17; IETF: Hardie, 28.

[74] KISA: Chung – Spam Forum (May 2, 2003), 115; Federation of European Direct Marketers: Tandberg – Spam Forum (May 2, 2003), 165; ASRG: Levine, 10.

C. Mandatory Subject Line Labeling Would Not Strengthen Anti-Spam Law Enforcement

Identifying spam that contains law violations is easy. The CAN-SPAM Act prohibits spammers' favorite techniques,[75] and spam typically exhibits several of these law violations. The challenge for law enforcement is finding the individuals who send unlawful spam. Subject line labeling would not help law enforcers overcome this difficulty.[76]

Because the present email system lacks any mechanism requiring a sender's identity to be authenticated, spammers can and do easily conceal their identities and their whereabouts from both spam recipients and law enforcers.[77] Subject line labeling would not address these shortcomings in the current email system, and therefore would not help law enforcers identify or track down spammers. As long as there is no standard method for authenticating a sender's identity, law enforcers will continue to face formidable difficulties in tracking down spammers. To strengthen law enforcement, authentication holds more promise than imposition of a subject line labeling requirement.

As the Commission explained in its National Do Not Email Registry Report to Congress, there are promising developments with email authentication that may help solve the spam problem.[78] The marketplace is already moving in this direction and the Commission is actively encouraging the testing and

[75] These techniques include using false or misleading transmission information, deceptive subject lines, open relays, or failing to provide an opt-out opportunity and to honor opt-out requirements.

[76] Adding another "per se" violation would not aid law enforcement actions against fraudulent spammers. It would only add a possible cause of action against those senders of UCE who failed to label their emails but are generally law-abiding and not difficult to find.

[77] Part III of the Commission's National Do Not Email Registry Report describes in detail how the open structure of the email system facilitates the proliferation of spam. *See* Appendix 2.

[78] Authentication aims to remedy the anonymous nature of email. Simply put, email authentication is a system to ensure that you are who you say you are. Although there are a variety of approaches, generally speaking, an authentication system confirms that the sender's second-level domain (what follows the @ sign in an email address) is truly what it purports to be. In other words, if a message claimed to be from abc@ftc.gov, the system 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.

implementation of competing authentication proposals.[79] Other promising developments include progress toward reputation and accreditation services to correct the flaws inherent in the self-regulating, autonomous nature of the current email system.[80] Meanwhile, ISP blocking and filtering, and consumers' ability to enable other protective measures, as noted previously, have greatly improved, and will likely continue to become more effective. These trends promise, ultimately, to arrive at an email system built on accountability. Without authentication and accountability, spammers will continue to use falsity and deception to send their spam, and a federal requirement mandating subject line labeling likely will not change the spammers' actions.

IV. Conclusion

For the foregoing reasons, the Commission concludes that subject line labeling, while it might identify UCE sent by law-abiding marketers, likely would not have any measurable impact on the fraudulent spam sent by outlaw spammers. Consumers already have technological options to identify UCE sent by law-abiding marketers. The Commission recommends, therefore, that Congress not enact a subject line labeling requirement. Emphasis and support would more productively be directed to encouraging emerging industry efforts to combat spam. Accordingly, industry and government are diligently working towards alternatives to the likely ineffective strategy of subject line labeling. These alternatives may promise to alleviate the spam problem through new technologies, improved enforcement, and consumer and business education.

[79] The FTC discussed email authentication in depth at its "Email Authentication Summit" held in November 2004. *See* more detailed discussion, as well as specific authentication proposals, at http://www.ftc.gov/bcp/workshops/e-authentication/index.htm. The Commission recently established a website designed to allow ISPs and other operators of email servers to share the results of tests performed on various domain-level email authentication proposals. The website invites companies that are testing email authentication standards to answer several technological questions regarding the functionality, interoperability, scalability, and effectiveness of these standards, and to update their responses as new information becomes available. By sharing testing results, these members of the public will help identity the domain level authentication standard (or standards) that is most effective at combating spam, can be deployed quickly, can be used easily by unsophisticated operators of email servers (such as small businesses with their own mail servers), and costs little to use. The website is intended to help standards proponents to identify potential problems (such as non-spam messages being treated as spam), and to help operators of mail servers who test the various proposed standards to identify solutions to the problems that reveal themselves. Access to the website is *available at* http://www.ftc.gov.

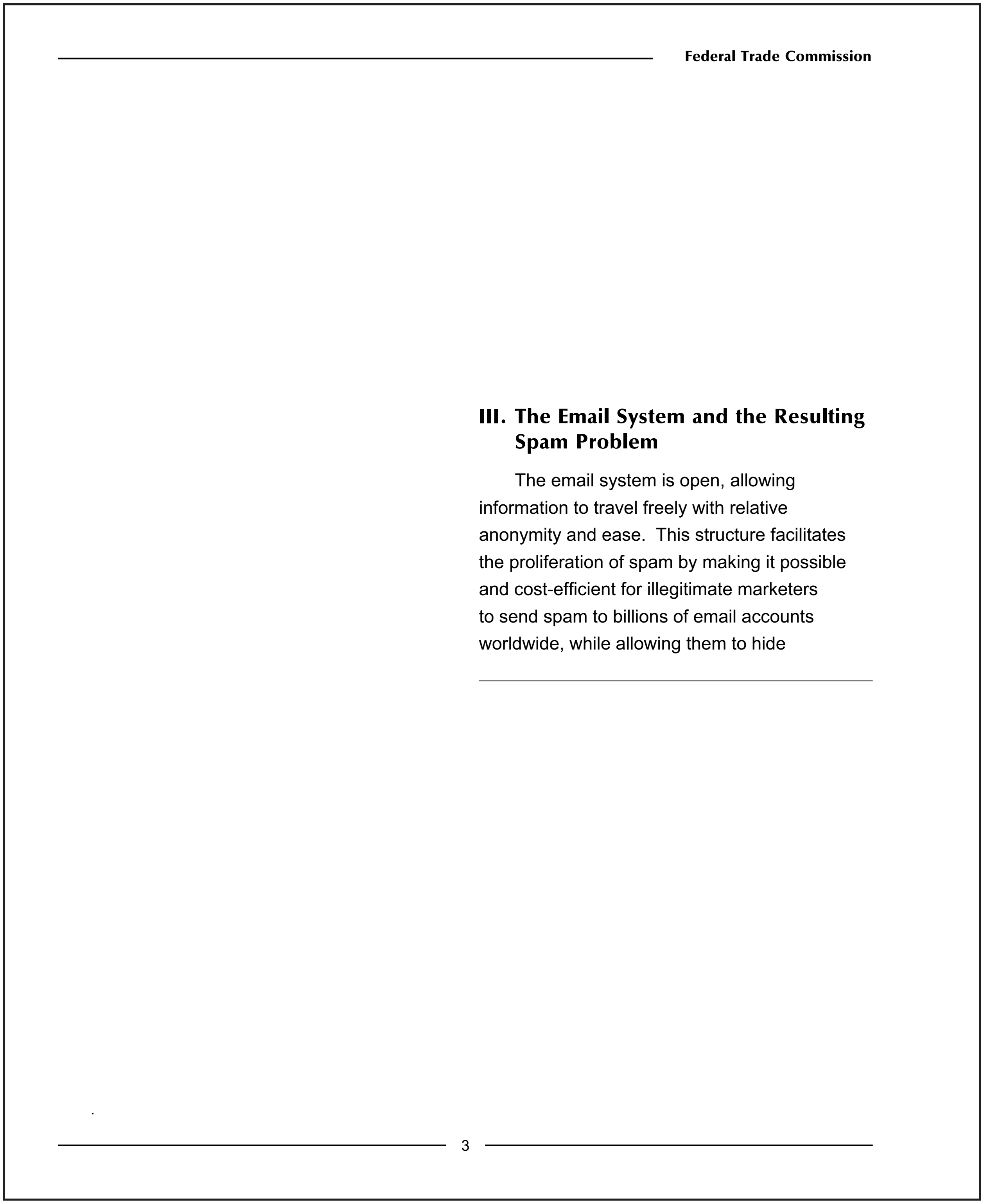
[80] ESPC: Hughes, 23, 33; Earthlink: Youngblood, 23; AT&T: Israel, 23; UOL: Squire, 23-24; Microsoft: Katz, 18-21.

Appendix 1:
List of Interviews

Name (Last, First)	Organization	Date of Meeting	Transcript/ Submission Available?
Ashworth, Bill	Microsoft Corporation	2/3/2005	Yes
Baer, Joshua (“Josh”)	SKYLIST, Inc.	1/24/2005	Yes
Baker, David	Earthlink, Inc.	1/27/2005	Yes
Berkower, Elise	Email Service Provider Coalition (ESPC); DoubleClick	1/24/2005	Yes
Bowles, Elizabeth	ARISTOTLE.net	3/30/2005	No
Brady, Betsy	Microsoft Corporation	2/3/2005	Yes
Egan, Erin M.	Covington & Burling for Microsoft Corporation	2/3/2005	Yes
Everett-Church, Ray	PrivacyClue	1/13/2005	Yes
Fox, Jean Ann	Consumer Federation of America (CFA)	1/24/2005	Yes
Hadley, Tony	Email Service Provider Coalition (ESPC); Experian	1/24/2005	Yes
Halpert, James (“Jim”)	Piper Rudnick for the Internet Commerce Coalition (ICC)	1/27/2005	Yes
Hardie, Ted	Internet Engineering Task Force (IETF); Qualcomm, Inc.	1/19/2005	Yes
Hartman, Sam	Internet Engineering Task Force (IETF); Massachusetts Institute of Technology (MIT)	1/19/2005	Yes
Hollenbeck, Scott	Internet Engineering Task Force (IETF); Verisign, Inc.	1/19/2005	Yes
Hoofnagle, Chris	Electronic Privacy Information Center (EPIC)	1/13/2005	Yes
Hughes, J. Trevor	Email Service Provider Coalition (ESPC); Network Advertising Initiative (NAI)	1/24/2005	Yes
Ingis, Stuart (“Stu”)	Piper Rudnick for Time Warner, Inc. (AOL)	2/3/2005	Yes
Israel, Susan E.	AT&T	1/27/2005	Yes
Jacobsen, Jennifer	Time Warner, Inc. (AOL)	2/3/2005	Yes
Jalli, Quinn	Email Service Provider Coalition (ESPC); Digital Impact, Inc.	1/24/2005	Yes
Katz, Harry	Microsoft Corporation	2/3/2005	Yes

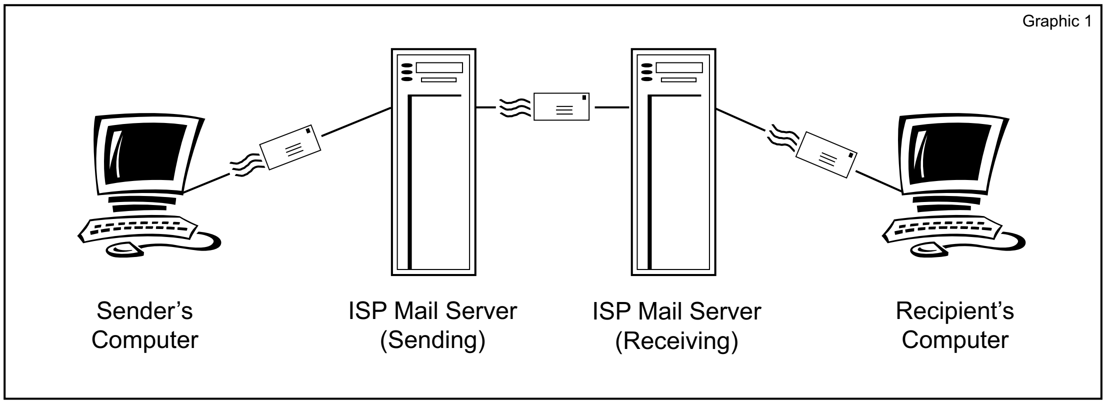
Name (Last, First)	Organization	Date of Meeting	Transcript/ Submission Available?
Kornblum, Aaron	Microsoft Corporation	2/3/2005	Yes
Levine, John	Internet Engineering Task Force (IETF); Anti-Spam Research Group (ASRG)	1/19/2005	Yes
Malamud, Carl	Internet Engineering Task Force (IETF); Media.org	1/19/2005	Yes
Mansourkia, Maggie	MCI, Inc.	2/3/2005	Yes
Moore, Keith	Internet Engineering Task Force (IETF); University of Tennessee at Knoxville	1/19/2005	Yes
Newitz, Annalee	Electronic Frontier Foundation (EFF)	1/13/2005	Yes
Sherry, Linda	Consumer Action	1/24/2005	Yes
Squire, Brooke	United Online, Inc.	1/27/2005	Yes
Youngblood, Mary	Earthlink, Inc.	1/27/2005	Yes

Appendix 2: 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


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.

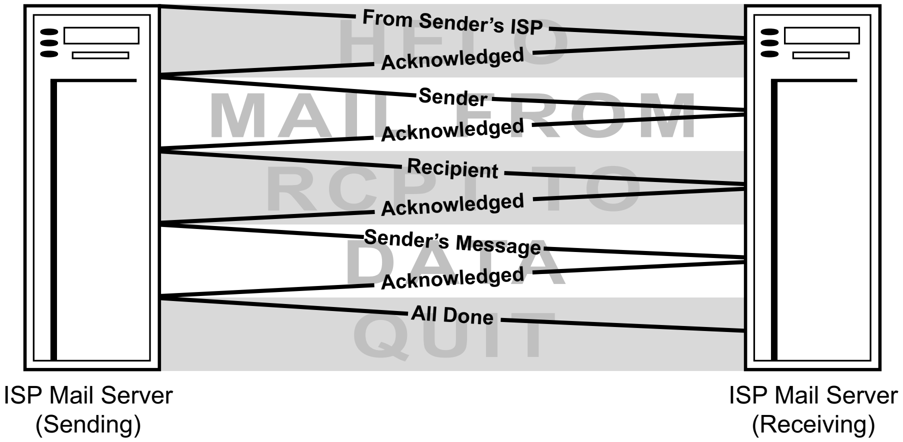
The technical process of how email functions is, of course, much more complex. From the time that a person clicks "send" until the message arrives in a recipient's inbox, many processes occur involving – when reduced to the most basic form – at least four computers:

[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.

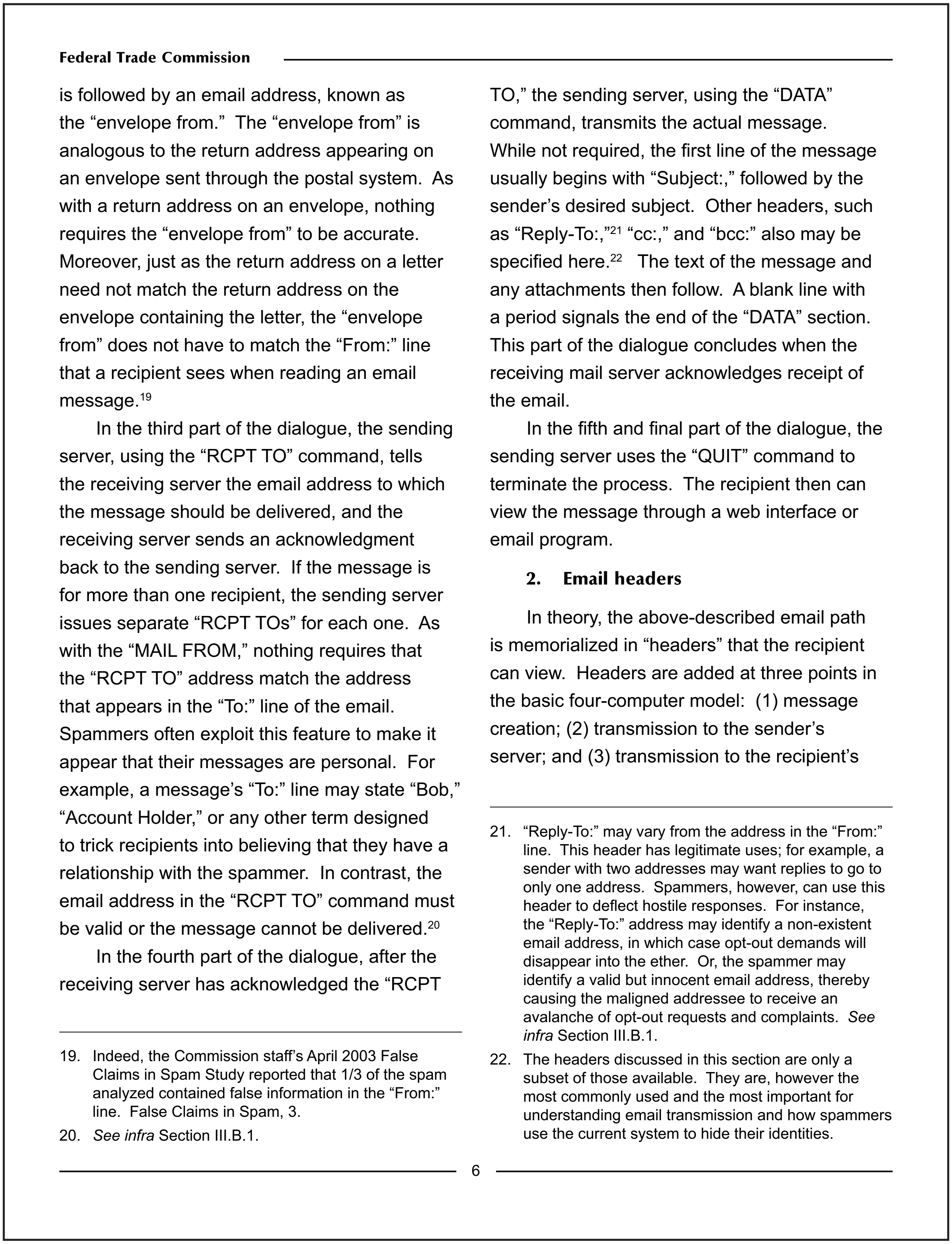
Clicking the "send" button transmits the email message from the sender's computer to the sender's outbound mail server. This sending server locates and begins a dialogue with the recipient's inbound mail server using SMTP. Under SMTP, the sending and receiving mail servers engage in a five-part dialogue.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

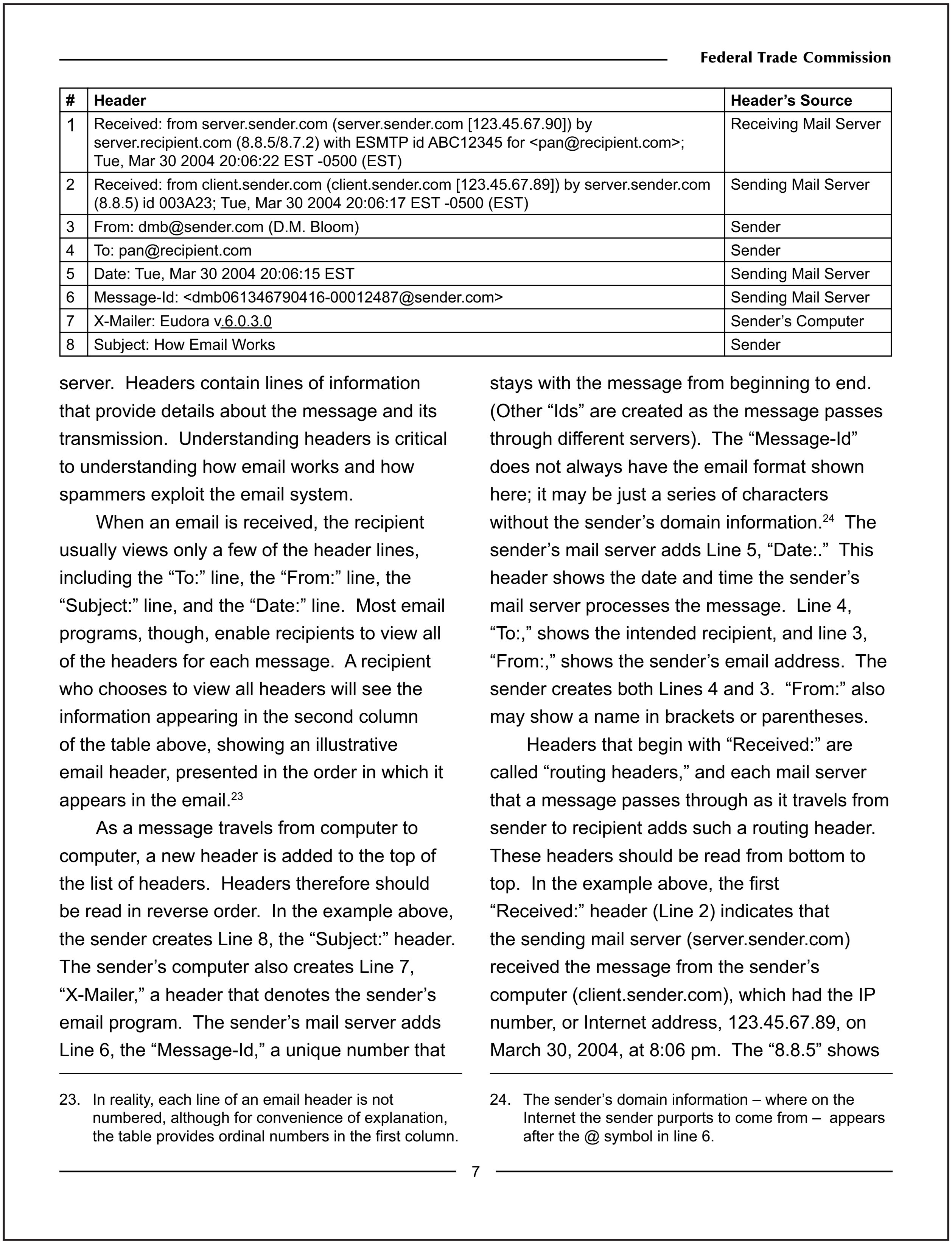
In theory, the above-described email path is memorialized in “headers” that the recipient can view. Headers are added at three points in the basic four-computer model: (1) message creation; (2) transmission to the sender’s server; and (3) transmission to the recipient’s

[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

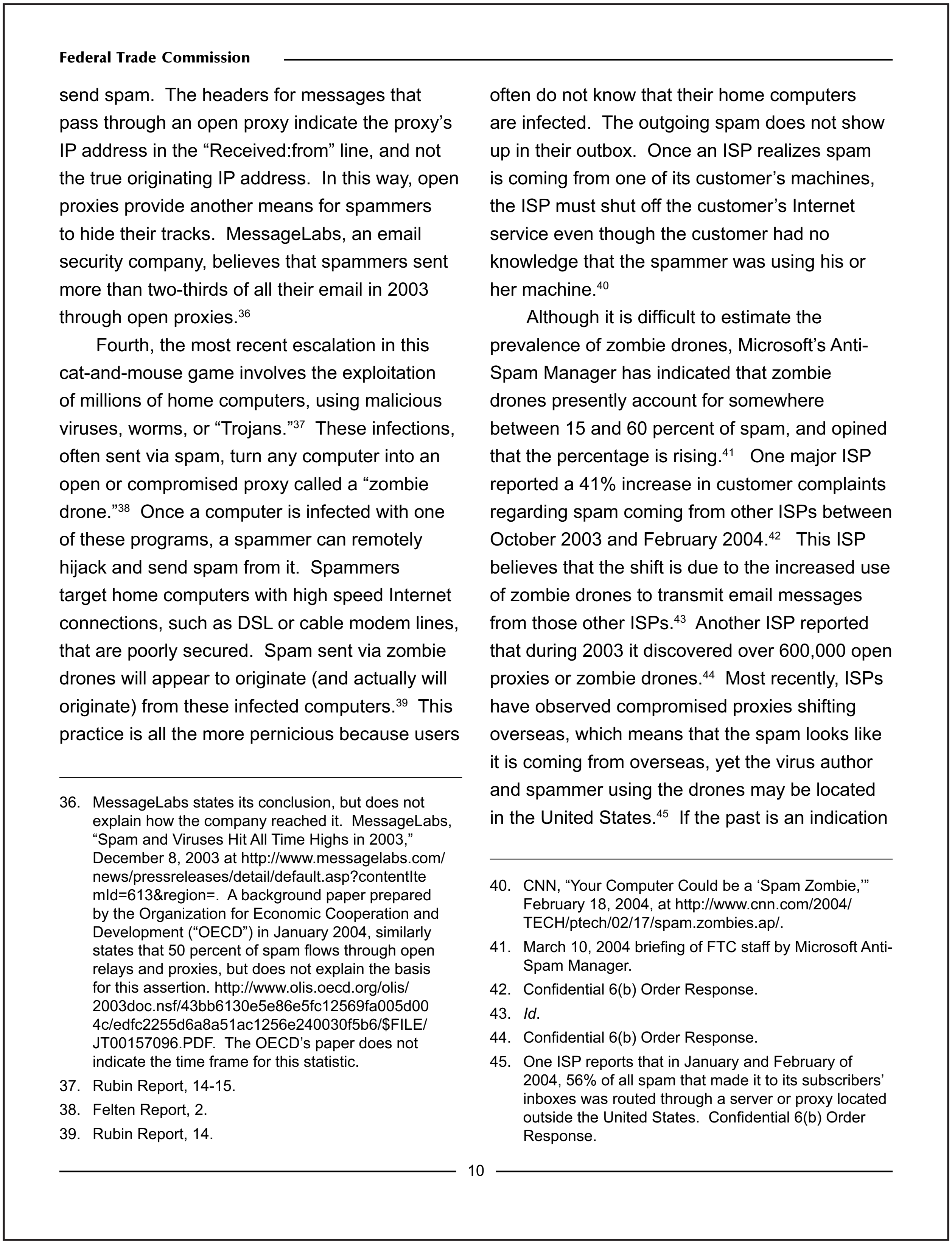
[31] The Commission has charged spoofing as a violation of Section 5 of the FTC Act, 15 U.S.C. § 45. *See e.g., FTC v. GM Funding*, No. SAVC 02-1026 (C.D. Cal. filed Nov. 6, 2002) (one victim of spoofing received 40,000 rejected messages in his inbox); *FTC v. Westby*, No. 032-3030 (N.D. Ill. filed Apr. 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).

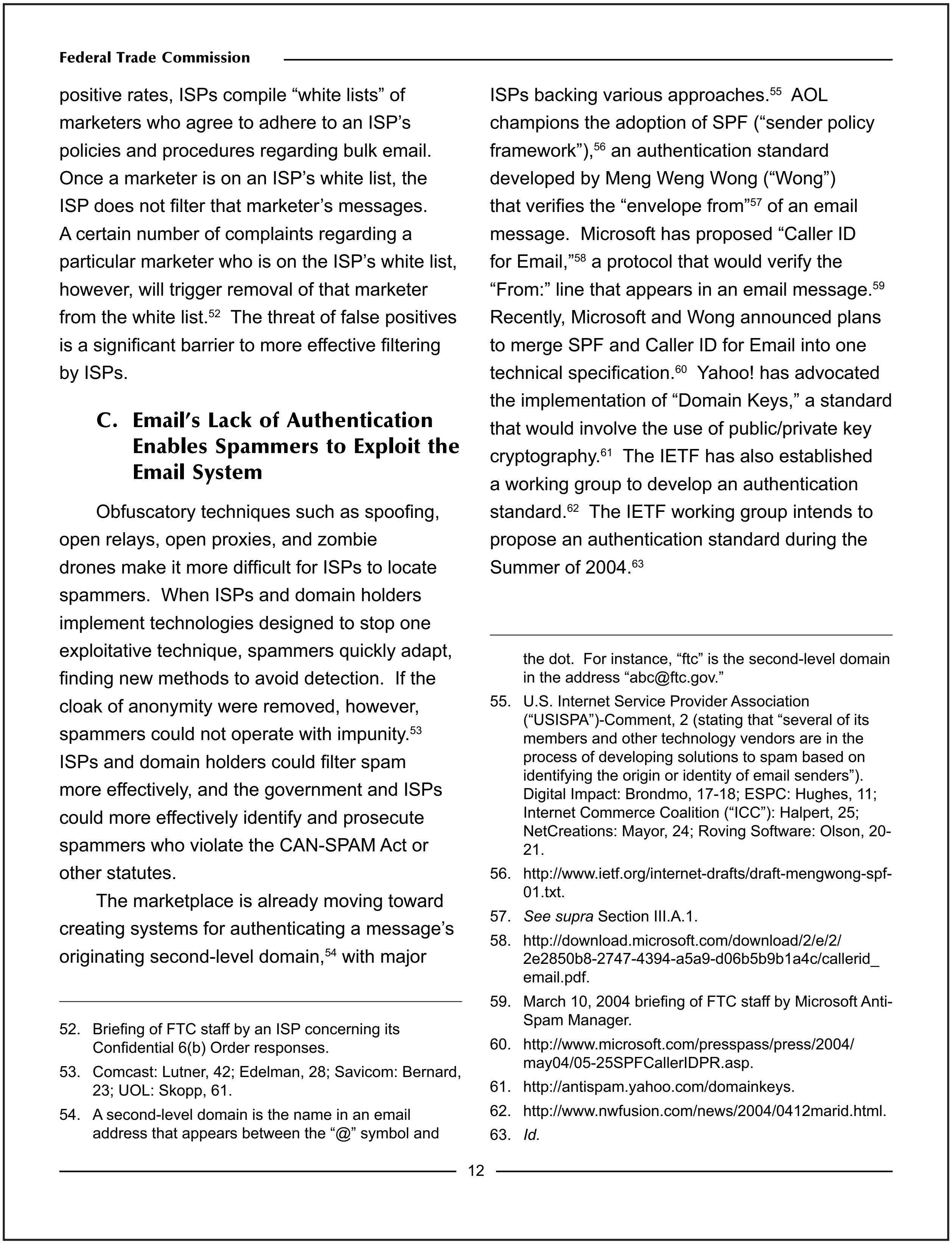
[47] Email blocking occurs at the point of attempted connection to the ISP's network. Email filtering occurs once an email enters the ISP's network, but before it reaches a recipient's inbox.

[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.

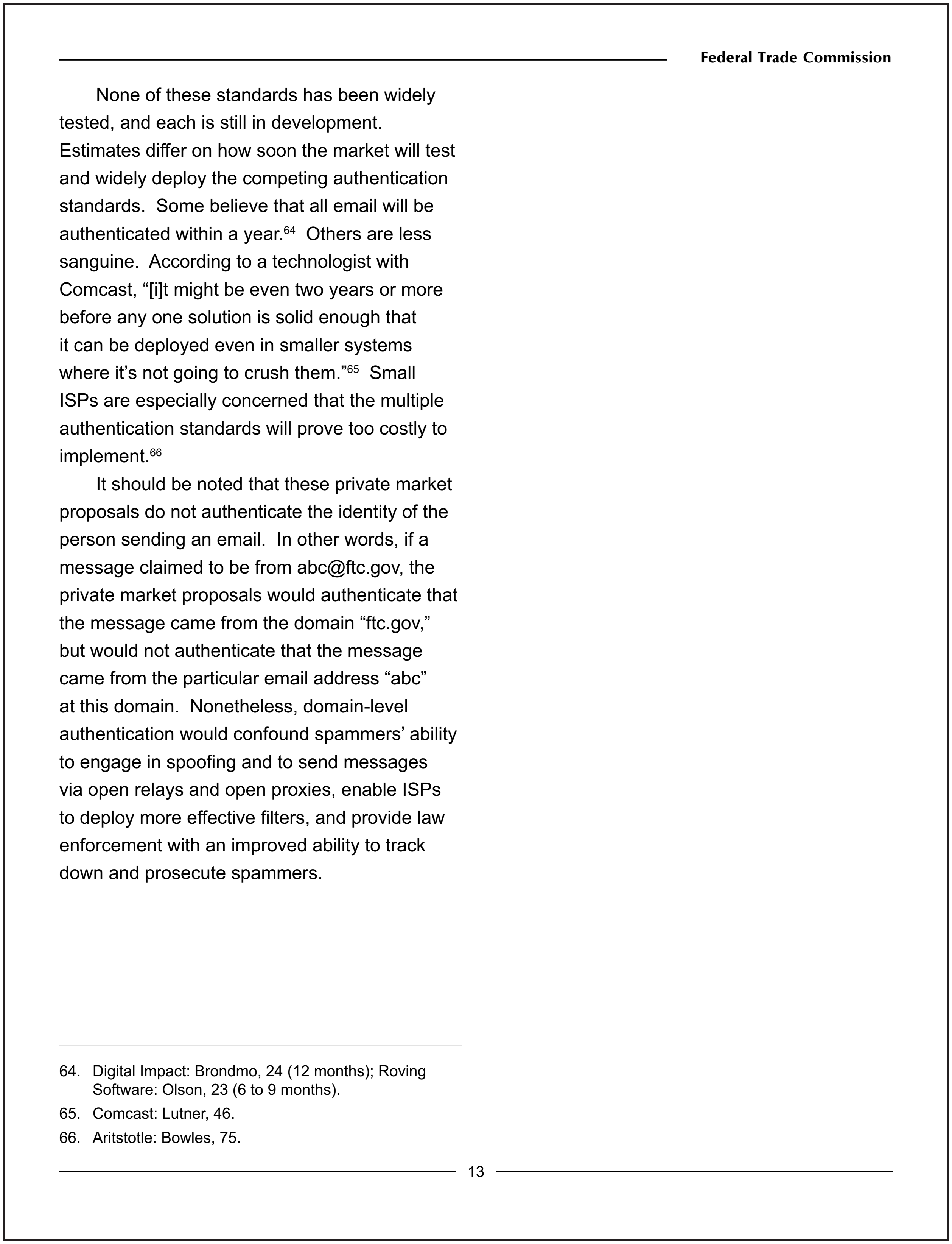
[59] March 10, 2004 briefing of FTC staff by Microsoft Anti-Spam Manager.

[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.

Concurring Statement of Commissioner Pamela Jones Harbour

In Re: CAN SPAM Subject Line Labeling Report

I concur in the release of the Commission's report to Congress concerning subject line labeling, submitted pursuant to Section 11(2) of the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (the "CAN-SPAM Act"), 15 U.S.C. § 7710(2) (2003) (the "Report"). I write separately to highlight the potential usefulness of "ADV labeling" to assist consumers in managing unsolicited commercial email ("UCE").

I agree with Commissioner Leibowitz's separate statement that "an ADV labeling requirement could be a modest tool to empower consumers to filter and sort commercial emails – to read them later, evaluate them individually, or delete them in bulk if they choose." I also agree that Congress asked the Commission to study an ADV labeling requirement precisely because Congress wanted consumers to have the option not to receive or to sort UCE – even emails sent from legitimate marketers.

I, like Commissioner Leibowitz, would have preferred that the Report further emphasize the importance of providing adequate tools to enable consumers, who so wish, to filter UCE, even from legitimate marketers. One consumer's public comment stated: "Treat my email as if it were an extension of my phone, as it is, and do not call me if unsolicited." (Gilliland, Mark - Comment, 1). The desires of such consumers should be respected.

The Report does, however, set forth a number of technological options that consumers can use to sort, delete, or block UCE. Examples include highly calibrated or customized filters; "white-lists" of particular desired senders; personalized Bayesian filtering; and blocking mechanisms that bar all email coming from sources outside of the consumer's address book. If consumers choose to avoid receiving UCE from legitimate marketers, it appears that existing technological solutions will allow them to do so. While ADV labeling would provide consumers with an easy way to sort UCEs from legitimate marketers who would adhere to an ADV labeling requirement, it appears that consumers already have acceptable tools available to assist them.

Accordingly, I have decided to concur in the Commission's release of this Report.

Dissenting Statement of Commissioner Jon Leibowitz

In Re: CAN-SPAM ADV Labeling Report

Requiring commercial email to be labeled is not a panacea but, as the CAN-SPAM Act clearly recognizes, there is no single bullet theory for solving the spam problem. An ADV labeling requirement could be a modest tool to empower consumers to filter and sort commercial emails – to read them later, evaluate them individually, or delete them in bulk if they choose – and for that reason I respectfully dissent from the majority and urge Congress to consider a labeling requirement.

The Report confuses a principal purpose of the CAN-SPAM Act – to attack fraudulent and deceptive spam – with the *sine qua non* of the ADV amendment, to create a convenience tool for consumers. Indeed, the legislative history of CAN-SPAM makes clear that the report provision was largely intended to spur the Commission to study the use of the ADV label for commercial emailers that supply accurate header and address information – not for those sending fraudulent or misleading commercial messages. Senator Schumer, speaking at the Commission's own Spam Forum about his mandatory ADV labeling proposal – one that served as a basis for the provision that ultimately was enacted – stated that the provision would require "*all commercial email*" to have "ADV" in the subject line, indicating that it contains commercial content. Senator Schumer, Speech at FTC Spam Forum (April 30, 2003), at 172 (emphasis added). Senator Corzine, introducing the amendment calling for the ADV study, noted that the FTC Report was to consider how to require "*all unsolicited commercial email* to be identifiable from its subject line." 108th Congress, Cong. Rec. S13041 (daily ed. Oct. 22, 2003) (statement of Senator Corzine) (emphasis added). He believed that the labeling requirement would not only help reduce the amount of spam but "give individuals and ISPs considerable power to keep spam out of their in boxes." *Id.* Senator Wyden spoke in support of Senator Corzine's amendment during floor debate, confirming his understanding that the labeling would apply to "every unsolicited email." *Id.* (statement of Senator Wyden). He recognized that "the question about making sure every unsolicited email has ADV has been contentious" in light of the costs that would be imposed on businesses, but supported the requirement that the Commission should at least study the idea. *Id.*

Legislators in the House, while focused less on the ADV provision, acknowledged the broad scope of CAN-SPAM. House Judiciary Committee Chairman Sensenbrenner declared that CAN-SPAM would give consumers "more information and choices to stop receiving *all forms of unwanted commercial email.*" 108th Congress, Cong. Rec. H12860 (daily ed. Dec. 8, 2003) (statement of Representative Sensenbrenner). House Energy and Commerce Committee Chairman Tauzin, in a joint statement with Ranking Member Dingell, stated that CAN-SPAM would not only "prohibit certain predatory and abusive practices used to send commercial email," but also "provide consumers with the ability to more easily identify and opt-out of receiving other unwanted commercial email, and to give such opt-outs the force of law." 108th Congress, Cong. Rec. E73 (Jan. 28, 2004 extensions of remarks) (statement of Representative Tauzin).

Another way to understand the intent of a law is to look at who opposed it. In the instance of mandatory ADV labeling, it was not "Kingpin Spammers" and other Internet miscreants. Instead, legitimate marketers – some of whom supported the fraud and deception provisions in CAN-SPAM – opposed the labeling requirement (and threatened to block the underlying measure). Simply put, they worried that consumers would not read ADV-labeled emails. Ultimately, Congress replaced the mandatory labeling requirement that some legislators had endorsed with a provision authorizing the Commission to study ADV labeling. It is telling, though, that the report provision directs the Commission to examine the ADV label's application for a *broader* range of email than all unsolicited commercial email – all "commercial email," presumably whether unsolicited or not.

Congress' interest in ADV labeling as a tool to deal with email from legitimate marketers is well-founded. It is not clear that consumers want unsolicited commercial email from legitimate marketers any more than they want, say, unsolicited telephone calls. According to Senate Judiciary Chairman Leahy, for example,

> the fundamental problem adherent to spam – its sheer volume – may well persist even in the absence of fraudulent routing information and false identities. In a recent survey, 82 percent of respondents considered unsolicited bulk email, even from legitimate businesses, to be unwelcome spam.

108th Congress, Cong. Rec. S15947 (daily ed. Nov. 25, 2003) (statement of Senator Leahy). An ADV label, of course, would simply alert the consumer that the email is commercial in nature – it would *not* prevent consumers from receiving or reading ADV-labeled offers. The Report suggests that if labeling were mandatory, ISPs would use the labels to filter email, but that has not proven to be the case. As the Report makes clear, very few ISPs have used the ADV label to filter, and there is no reason to think that they would start doing so if Congress mandated the use of ADV labels.

By focusing mainly on the minor impact of ADV labeling on deceptive and fraudulent spam rather than on its significant impact on unsolicited commercial email from legitimate marketers, the Commission's Report gives short shrift to the area where a labeling requirement is likely to be most promising. Thanks to the great strides made by industry, notably the ISPs, in filtering email before it reaches individuals' in-boxes, email from legitimate marketers who would likely comply with an ADV labeling requirement makes up an ever-increasing percentage of the mail that reaches consumers. ADV labeling would not solve all of the problems consumers face in weeding out unwanted mail, to be sure, but it would give consumers additional flexibility to deal with them. It could save consumers time and money (for those with dial-up access), increase convenience, and – with apologies to Justice Brandeis – help protect the "right to be left alone" in the digital age. To avoid labeling, imaginative marketers seeking to establish a relationship with customers might even come up with incentives to persuade people to opt-in to email offers.

I do agree with my colleagues that an ADV labeling requirement would likely have little impact in assisting the Commission in enforcing the law or in reducing the amount of deceptive and fraudulent spam that consumers receive. I recognize, also, that consumers have other tools available that are designed to give them more control over their in-boxes, including filters and whitelists. I disagree, however, that Congress, in directing the Commission to study ADV labeling, intended the Commission to focus on deceptive and fraudulent spam, and believe that ADV labeling would be a useful tool to supplement other available tools.

FEDERAL TRADE COMMISSION • 1.877.FTC.HELP • FOR THE CONSUMER • FTC.GOV/SPAM