National Do Not Email Registry

A Report To Congress

Federal Trade Commission
June 2004

National Do Not Email Registry
A Report to Congress

June 2004

Federal Trade Commission

Timothy J. Muris, Chairman
Mozelle W. Thompson, Commissioner
Orson Swindle, Commissioner
Thomas B. Leary, Commissioner
Pamela Jones Harbour, Commissioner

Contents

Executive Summary

The Federal Trade Commission (the "FTC" or "Commission") submits this Report pursuant to Section 9 of the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (the "CAN-SPAM Act"), 15 U.S.C. § 7708, which calls for the Commission to: (1) set forth a plan and timetable for establishing a National Do Not Email Registry; (2) explain any practical, technical, security, privacy, enforcement, or other concerns that the Commission has regarding such a Registry; and (3) explain how a Registry would be applied with respect to children with email accounts.

When it directed the Commission to set forth a plan for and to comment on the feasibility of a National Do Not Email Registry, Congress was cognizant of the Commission's highly successful deployment of the National Do Not Call Registry. In essence, Section 9 of the CAN-SPAM Act asks the Commission to determine whether and how the success of the National Do Not Call Registry can be replicated in the context of spam. This Report concludes that a National Do Not Email Registry, without a system in place to authenticate the origin of email messages, would fail to reduce the burden of spam and may even increase the amount of spam received by consumers. Therefore, the Commission proposes a plan that first requires authentication – strengthening of the email system so that the origin of email messages cannot be falsified – as a first step and a prerequisite to any type of Registry.

The Commission reaches its conclusion after soliciting and obtaining input from dozens of individuals and organizations and using a number of information-gathering techniques, including: a Request for Information ("RFI") that resulted in responses from some of the nation's largest Internet, computer, and database management firms; interviews with over 80 individuals representing 56 organizations, including consumer groups, email marketers, Internet Service Providers ("ISPs"), and technologists; requiring the seven ISPs that collectively control over 50 percent of the market for consumer email accounts to provide detailed information about their experiences with spam; soliciting public comments through an Advance Notice of Proposed Rulemaking ("ANPR") concerning the CAN-SPAM Act rules; and retaining the services of three of the nation's preeminent computer scientists.

Based on input from these sources, the Commission has determined that spammers would most likely use a Registry as a mechanism for verifying the validity of email addresses and, without authentication, the Commission would be largely powerless to identify those responsible for misusing the Registry. Moreover, a Registry-type solution to spam would raise serious security, privacy, and enforcement difficulties. The Commission's concerns with the security, privacy, and enforcement challenges surrounding a Registry reach a zenith with respect to children's email accounts. A Registry that identified accounts used by children, for example, could assist legitimate marketers to avoid sending inappropriate messages to children. At the same time, however, the Internet's most dangerous users, including pedophiles, also could use this information to target children.

The Commission therefore strongly believes that implementation of a National Do Not Email Registry would not reduce the volume of spam, particularly given currently available technology to authenticate the origin of email messages. The Commission thus proposes a program to encourage the widespread adoption of email authentication standards that would help law enforcement and ISPs better identify spammers. If, after allowing the private market sufficient time to develop, test, and widely implement an authentication standard, no single standard emerges, the Commission could begin the process of convening a Federal Advisory Committee to help it determine an appropriate email authentication system that could be federally required. If the Commission were to mandate such a standard, after a reasonable period of time following the effective date of such a standard, the Commission will consider studying whether an authentication system combined with enforcement or other mechanisms (e.g., better filters) had substantially reduced the burden of spam. If spam continued to be a substantial problem, if a Registry could significantly reduce it once an authentication system is in place, and if other technological developments removed the security and privacy risks associated with a Registry, the Commission will consider issuing an ANPR proposing the creation of a National Do Not Email Registry.

Before expending resources on the implementation of a Registry, the marketplace should be encouraged and allowed to correct a flaw in the email system's architecture that enables spam – the lack of domain-level authentication. Without effective authentication of email, any Registry is doomed to fail. With authentication, better CAN-SPAM Act enforcement and better filtering by ISPs may even make a Registry unnecessary.

I. Introduction and Overview

The Federal Trade Commission (the "FTC" or "Commission") submits this Report pursuant to Section 9 of the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (the "CAN-SPAM Act"), 15 U.S.C. § 7708 (2003), which requires the Commission to: (1) prepare a report setting forth a plan and timetable for establishing a National Do Not Email Registry; (2) explain any practical, technical, security, privacy, enforceability, or other concerns that the Commission has regarding such a Registry; and (3) explain how such a Registry would be applied with respect to children with email accounts.[1]

Unsolicited commercial email ("UCE" or "spam") poses a serious threat to electronic communication over the Internet for consumers and businesses. Deception and fraud appear to characterize the vast majority of spam.[2] Spam, even if not deceptive, may also lead to significant disruptions and inefficiencies in Internet services as when it spreads viruses that wreak havoc for computer users. Moreover, a serious Internet infrastructure problem flows from the sheer volume of spam that is now being sent. These problems are significant for consumers and businesses and threaten their confidence in the Internet as a medium for communication.

Solving the spam problem begins with recognition that spammers are essentially anonymous. The current email system enables spammers to hide their tracks and thereby evade ISPs' anti-spam filters and law enforcement. A prerequisite for fighting spam is ending this anonymity through a robust authentication standard that ensures that a message actually comes from the domain listed in the message's headers. Without authentication, a Registry will, at best, have no impact on spam and, at worst, result in more spam. Effective authentication would improve CAN-SPAM Act compliance and, coupled with better filtering by ISPs, would greatly reduce the volume of spam.

This Report therefore proposes a plan that recognizes the need for an authentication standard.[3] Section II of this Report describes the

1. Section 9 of the CAN-SPAM Act provides:

   Not later than 6 months after December 16, 2003, the Commission shall transmit to the Senate Committee on Commerce, Science, and Transportation and the House of Representatives Committee on Energy and Commerce a report that –

   (1) sets forth a plan and timetable for establishing a nationwide marketing Do-Not-E-Mail Registry;

   (2) includes an explanation of any practical, technical, security, privacy, enforceability, or other concerns that the Commission has regarding such a Registry; and

   (3) includes an explanation of how the Registry would be applied with respect to children with e-mail accounts.

2. In an April 2003 study of over 1000 pieces of spam, Commission staff found that about two-thirds of the spam analyzed contained likely false claims in the "From:" line, "Subject:" line, or message text. False Claims in Spam, 10. Further analysis revealed that 84.5 percent of the spam analyzed were deceptive on their face or advertised an illegitimate product or service. The Commission has posted the False Claims in Spam report online at http://www.ftc.gov/reports/spam/030429spamreport.pdf.

3. A mechanism for shifting the cost of spam from the recipient to the sender would also contribute to solving the spam problem by addressing another fundamental problem, namely, the low cost of sending spam. The Commission does not presently propose a mechanism for accomplishing such a cost shift because numerous issues exist regarding who should pay for the cost of email, who should be paid, how much should be paid, and the mechanism for collecting and distributing such payments. In addition, cost-shifting would require a more fundamental Internet protocol change whereas authentication standards are at the point where they can be tested and implemented in the near term.

information gathering methods the Commission used to prepare this Report. Section III provides a basic explanation of the email system, including how it enables spam by permitting the sending of unauthenticated messages and how the creation of an authentication system is a first step to help bring the spam epidemic under control. Section IV describes three possible models for a National Do Not Email Registry and explains the practical, technical, security, privacy, enforceability, and other concerns that the Commission has regarding each Registry model. Finally, Section V sets forth a plan and timetable for establishing a Registry.

II. Information Gathering Processes

In preparing this Report on a National Do Not Email Registry, the Commission used a number of information-gathering techniques to obtain information from dozens of individuals and organizations. First, the Commission issued a Request for Information ("RFI") seeking detailed Registry proposals from businesses with the technological skill to design and manage a Registry.[4] The RFI described various formats for a possible Registry and invited responders to use their technical skill and creativity to design alternative formats. The Commission received 13 responses to the RFI, ten of which proposed the creation of a Registry.[5] These ten responses provided the Commission with detailed information that greatly assisted its analyses of the practical, technical, security, privacy, and enforceability issues surrounding a Registry.

Second, between January and March 2004, the Commission interviewed over 80 individuals representing 56 organizations, including consumer groups, email marketers, Internet Service Providers ("ISPs"), law enforcement, private attorneys with spam enforcement experience, and technologists.[6] A court reporter transcribed most of these interviews.[7] These interviews enabled the Commission to draw upon the skills and backgrounds of a wide variety of organizations.

Third, using its compulsory process powers under Section 6(b) of the FTC Act, 15 U.S.C. § 46(b), the Commission required the seven ISPs that collectively control over 50% of the market for consumer email accounts to provide detailed information concerning their experiences with spam.[8] The 6(b) Orders asked for data concerning the volume and types of spam hitting these companies' mail servers and being delivered to their subscribers' inboxes. The 6(b) Orders also required the ISPs to provide detailed information regarding their anti-spam technologies and enforcement efforts.[9]

4. The RFI is attached as Appendix 1.
5. All but one of the RFI responders requested that their responses be treated as confidential. This Report, therefore, does not identify the RFI responders or describe confidential details of their proposals.
6. A complete list of interviewees has been attached to this Report as Appendix 2.
7. Citations to these transcripts identify the organization, representative from the organization, and page number of the transcript. For instance, the citation "Microsoft: Goodman, 16," would refer to a statement made by Microsoft employee Joshua Goodman on page 16 of the transcript. The Commission has posted the transcripts online at http://www.ftc.gov/reports/dneregistry/xcripts/index.pdf.
8. The Commission issued 6(b) Orders to America Online, Comcast, Earthlink, Microsoft, MCI, United Online, and Yahoo!.
9. To ensure that their anti-spam techniques do not become known to spammers, the ISPs have

Fourth, the Commission solicited comments from the general public in a March 11, 2004 Advance Notice of Proposed Rulemaking concerning CAN-SPAM Act rules (the "ANPR").[10] By the close of the comment filing period, the Commission received 7,147 comments regarding the creation of a National Do Not Email Registry.[11]

Finally, to ensure that the Commission's assessment of the technological and security issues posed by a possible Registry were well-grounded, the Commission retained the services of three preeminent computer scientists: Edward W. Felten, Associate Professor of Computer Science at Princeton University; Matthew Bishop, Associate Professor of Computer Science at the University of California ("UC") Davis and Co-director of the UC Davis Computer Security Laboratory; and Aviel Rubin, Professor of Computer Science at Johns Hopkins University and the Technical Director of Johns Hopkins' Information Security Institute.[12] The Commission retained these three experts because of their extensive background in analyzing the security of large computer systems. These experts have conducted independent appraisals of the security and technical issues surrounding a possible National Do Not Email Registry, and their assessments provide unbiased views of the challenges involved in creating a viable National Do Not Email Registry.[13]

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

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.

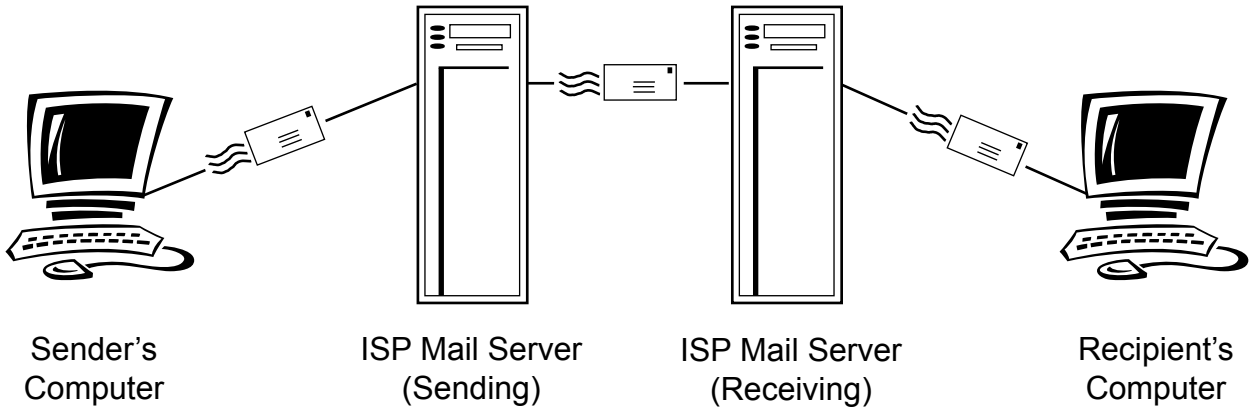
10. Citations to these comments identify the organization or person submitting the comment and the page number of the comment. For instance, the citation "DMA-Comment, 3" refers to page 3 of the comment submitted by the Direct Marketing Association. The Commission has posted the comments online at http://www.ftc.gov/os/comments/canspam/index.htm.

11. Over 6,000 of these comments were form letters from members of the National Association of Realtors arguing that a Registry would impose a significant burden on legitimate businesses while doing little to control abusive spammers. Forty of the total comments were from various industry groups, trade associations, consumer groups, educational institutions, and a government entity, of which at least 34 opposed a Registry based on practical, technical, privacy, and security concerns. The remaining 797 comments, which varied in scope and substance, were from individuals.

12. The Commission has posted reports prepared by these three computer scientists online at http://www.ftc.gov/reports/dneregistry/expertrpts/index.pdf. Citations to these expert reports identify the name of the expert and the page of the report. For instance, the citation "Bishop Report, 2" refers to a statement appearing on page 2 of the report prepared by Matthew Bishop, Ph.D.

13. The Commission's considerable prior experience with the issue of spam, including its enforcement experience and the Spam Forum, a three-day conference held in the Spring of 2003, also guides its analyses of the issues discussed in this Report. The Commission has posted transcripts of the Spam Forum 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 "Aristotle: Shivers - Spam Forum (May 1, 2003), 30" would refer to a statement made by Aristotle employee Carl Shivers that can be found on page 30 of the May 1, 2003 Spam Forum transcript.

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.

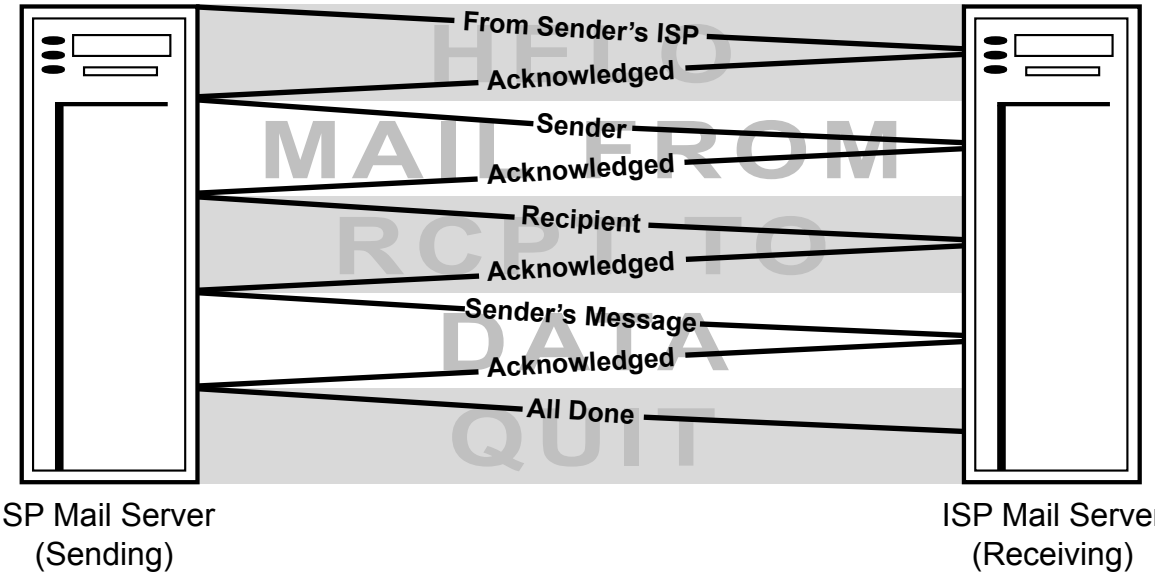
The technical process of how email functions is, of course, much more complex. From the time that a person clicks "send" until the message arrives in a recipient's inbox, many processes occur involving – when reduced to the most basic form – at least four computers:

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.

IV. Possible Models for a National Do Not Email Registry and the Commission's Concerns

In February 2004, the Commission issued an RFI to obtain information from businesses with the technical sophistication to design and manage a National Do Not Email Registry. The RFI described possible models for a National Do Not Email Registry, including the creation of a registry of individual email addresses, a registry of domains, and a registry combined with a certified third-party email forwarding service.[67] The RFI also invited responders to think "outside the box" and stated that "[t]he model registry you propose may consist of . . . an entirely different form of registry."[68]

The Commission received 13 responses. Two provided little useful information, merely advertising their software. One response proposed a dramatic reshaping of the email system that would divide email into classes of

67. The RFI stated that responders should assume that a registry of individual email addresses would include 300 million initial registrations and grow to include as many as 450 million email addresses. In estimating the likely number of registrations, the Commission assumed that the typical Internet user would register between two and three email accounts and that a registry of domains would include 30 million domains. Approximately 150 million American consumers use the Internet. http://www.clickz.com/stats/markets/finance/article.php/5961_3091091. The Commission based its estimate of the number of domains likely to be registered in a domain wide registry on the number of domain names registered in the .com and .org registries. Whois Source, "Detailed Domain Counts and Internet Statistics," April 2004 at http://www.whois.sc/internet-statistics/. Also, following the Do Not Call Model, the RFI posited that a National Do Not Email Registry would include mechanisms to permit consumers to submit complaints (along with offending emails) and to preserve these complaints for future law enforcement purposes.

68. RFI, 2.

users.[69] The remaining ten responses proposed three possible models for a National Do Not Email Registry – a registry of individual email addresses, a registry of domains, and a registry combined with a third-party forwarding service.[70] These ten responses included submissions from some of the largest and most technically-sophisticated Internet, computer, database management, and communications companies in the United States.

Subsection A describes the three proposed Registry models. Subsection B discusses the security and privacy concerns raised by these three models. Subsection C explains the obstacles to enforcing a Registry. Subsection D considers other practical and technical issues raised by a Registry. Subsection E explains why a Registry would fail to reduce the volume of spam hitting consumers' inboxes. Finally, subsection F describes the threat to children with email accounts posed by a National Do Not Email Registry.

A. Proposed Registry Models

1. Registry of individual email addresses

Some of the RFI responses proposed a Registry closely modeled on the National Do Not Call Registry. Such a Registry would consist of a centralized database containing the email addresses of consumers who do not want to receive unsolicited commercial email. These consumers would enter their email addresses on the Registry using a web-based form. Confirmation emails would be sent to the consumers' email addresses. To activate the registration, consumers would return to the Registry's web site and enter a code that appeared in the confirmation email.

Unsolicited commercial email marketers' distribution lists would be scrubbed against the Registry and the addresses on the Registry would be purged from the distribution lists in one of two ways. In a "distributed model," the marketers would receive a copy of the Registry from the Commission, compare their distribution lists to the Registry, and purge from their lists all addresses on the Registry. (This is similar to the process telemarketers use for the National Do Not Call Registry). Alternatively, in a "central-scrubbing model," marketers would submit their distribution lists to the Commission (or the Commission's contractor), which would compare the distribution lists to the Registry and return to each marketer a list with the email addresses appearing on the Registry deleted.

2. Registry of domains

Some RFI responders proposed permitting ISPs and other domain holders to register their objection to receiving spam addressed to

69. The proposed plan would require the FTC to create two classifications of email recipients. Commercial emailers would be prohibited from sending email to the first class of recipients and would be permitted to send email to the second class of recipients only if they had an established business relationship with the recipients. Under the proposal, ISPs would be required to block all commercial email to the first classification of email recipients – those who may not be solicited via commercial email. Such a dramatic reshaping of the email system does not seem practicable at the present time.

70. One of these ten responses proposed a Registry of individual email addresses combined with a mechanism for shifting the cost of email to the sender.

any email addresses located at their domains. According to this model, an official at a domain could inform the Commission that the domain did not want spam sent to any email address located at the domain. For instance, if the domain "ftc.gov" were listed on the Registry, a law-abiding bulk emailer would delete from its mailing list all addresses located "@ftc.gov."[71] Because domain names are already public information, a list of registered domains could be maintained on a public web site. Spam marketers would then be required to scrub their own lists, deleting addresses appearing at domains listed on the Registry.

Some entities have advocated a Domain Wide Registry with the added feature of enabling individual consumers to override their ISP's decision to participate or refrain from participating in a Domain Wide Registry.[72] In other words, with this feature, if a consumer's ISP decided to register its domain as a "no spam" domain, the consumer could still register an email address within this domain that welcomed UCE.

3. Registry of individual email addresses with a third-party forwarding service

Some RFI responders proposed a third-party forwarding service approach, consisting of the creation of a Registry of individual email addresses and a requirement that marketers who use UCE submit their distribution lists and the email messages they wished to distribute to an FTC-approved forwarding service. This service would then scrub the lists against the Registry and forward only those messages that were addressed to recipients whose addresses did not appear on the Registry. Use of the forwarding service could be required of senders of UCE, senders of all commercial messages (whether solicited or not), or even senders of all types of messages (whether "commercial" or not). The marketer would never receive access to the Registry database, nor would it receive its own distribution list purged of email addresses on the Registry.

B. Security/Privacy Concerns

A National Do Not Email Registry containing individual email addresses (or a Domain Wide Registry that permits individuals to override the registration decision of their ISP),[73] would suffer from a significant security weakness that would enable spammers to treat the Registry as the

71. Some entities we spoke with during the preparation of this Report proposed that instead of having a Registry, domain holders could indicate their anti-spam policies by including a notation in the information provided on Domain Name Servers. Anti-Spam Research Group ("ASRG"): Levine, 23; Junkbusters: Catlett, 27-28, 35-36.

72. National Consumers League ("NCL"): Grant, 16-17; Savicom: Bernard, 17; Wilson, Sun, Fee, Goodrich & Risotti ("WSFGR"): Kramer, 14-15; Word to the Wise: Atkins, 39.

73. This critique does not apply to a Domain Wide Registry that prohibits consumers from indicating their individual preferences. Such a model would not be prey to the security and privacy risks described in this portion of the text, because no actual email addresses would be listed on the Registry. Such a Registry, however, would raise serious enforcement and practical concerns. *See infra* Section IV.C and Section IV.D. Similarly, a third-party forwarding service model would significantly reduce the security risks described in this Section because spammers would not be able to use the scrubbing process to validate email addresses. A third-party forwarding service model, however, would be difficult to enforce and would likely result in significant disruption to the email system. *See infra* Section IV.C and Section IV.D.

National **Do** Spam Registry,[74] causing more spam,[75] including more of the most offensive spam, such as pornographic messages, to clog consumers' inboxes and degrade their privacy.[76]

This security weakness – the risk that spammers will use the Registry to determine valid email addresses – exists regardless of whether the Registry is distributed to marketers or centrally-scrubbed by the Commission. The risk that spammers would misuse a Registry is so high that Consumers Union has stated that if the Commission were to adopt an individual email address Registry and distribute the Registry to marketers, it "would emphatically tell all 42 million subscribers [of Consumer Reports] not to sign up for it."[77]

74. Association of National Advertisers-Comment, 2; Innovyx-Comment, 3; USISPA-Comment, 3.

75. American Business Media-Comment, 5; American Council of Life Insurers-Comment, 3; ASRG: Levine, 26-29; Edelman, 8; Greater Washington Community Ass'n of Realtors-Comment, 1; Promotion Marketing Ass'n, Inc.-Comment, 3; UOL: Skopp, 27.

76. "Phishers" pose another security concern for a National Do Not Email Registry. Rubin Report, 13; Comcast: Lutner, 41. "Phishers" are Internet outlaws who collect personal information from consumers by masquerading as companies with whom the consumers have a business relationship. *See, e.g. FTC v. Hill*, No. H 03-5537 (S.D. Tex. 2003). Most phishing schemes have involved spam claiming to be from the billing departments of ISPs and online financial institutions. Government web sites have not been immune to phishing attacks, however. One phisher attempted to trick consumers into providing personal information by claiming to be the web site "regulations.gov." http://www.ftc.gov/bcp/conline/pubs/alerts/phishregsalrt.htm. More recently, in April 2004, a phisher attempted to obtain personal information from consumers by purporting to be the web site www.fdic.gov. http://www.fdic.gov/news/news/press/2004/pr3804.html. A phishing attack against a National Do Not Email Registry could take the form of spam asking recipients to verify their registration status.

77. Consumers Union ("CU"): DeGraff, 29.

Several RFI responders have proposed computer security techniques that they claim would eliminate or alleviate these risks. The Commission has carefully examined these techniques to determine whether these techniques can effectively control these risks, and has concluded that none of them would be effective.

1. The high value of email addresses would likely make a Registry the National *Do* Spam Registry

Unlike the National Do Not Call Registry with which it has been compared, a National Do Not Email Registry would pose substantial security risks because a list of valid email addresses is extremely valuable – far more valuable than a list of working telephone numbers. Telemarketers can easily find working numbers. Unless specifically requested by a subscriber, telephone companies publish telephone numbers in public directories. Moreover, telemarketers can call active unlisted numbers using sequential dialing – an automated method of calling possible telephone numbers in numerical sequence.

Spammers, on the other hand, cannot identify valid email addresses easily. No master list or directory of email addresses exists.[78] As the legal director of the Electronic Frontier Foundation noted:

> I think there's a fundamental difference between telephone numbers and email addresses that plays into this, which is that while telephone numbers really are not "born" private, they are to a certain extent either public or even if you have an unlisted number, pretty easily

78. Felten Report, 2; ASRG: Levine, 15; National Retail Federation ("NRF"): Treanor, 7.

known. Email addresses are "born" private. There is no international or national registry of email addresses that exist[s].[79]

Furthermore, spammers cannot use the equivalent of sequential dialing to reach consumers' inboxes. Although one technique used by spammers approximates sequential dialing, it is far less effective. Spammers can launch a "dictionary attack," which generates email distribution lists by creating a list of alphanumeric character strings that are inserted in front of the "@" sign and then sending a high volume of emails with these character strings to a mail server.[80] The mail server delivers the email to those recipients who accept mail through that server and generally bounces back messages to those recipients who do not. The spammer can use software to track which addresses are valid and which are not, and use that information to create a list of the resulting valid email addresses for future spamming.[81]

The effectiveness of dictionary attacks pales in comparison to that of sequential dialing because of the almost limitless number of possible email addresses. Telephone numbers involve finite combinations of ten digits,[82] but email addresses can contain any number of alphanumeric characters. When a spammer engages in a dictionary attack, it sends a message to a high percentage of undeliverable addresses. The high undeliverable rate triggers the ISPs' filters and results in the ISPs' refusal to deliver the messages.[83] Consequently, spammers prize valid addresses.

Creation of a National Do Not Email Registry database would amount to the compilation of an extensive directory of active email addresses that currently does not exist.[84] According to the Association of National Advertisers, the "Registry would truly be the 'Fort Knox' list of email addresses for a criminal spammer."[85] Further, there seems to be a consensus that while a list of unconfirmed email addresses is valuable to spammers, a list of *live* email addresses would be a gold mine.[86] As the technology stands today, it is impossible to know whether there is a real person behind an email address unless it is tested to verify that it is a valid address.[87] A National Do Not Email Registry database would remove that technological hurdle, one of the

79. Electronic Frontier Foundation ("EFF"): Cohn, 10.
80. For instance, the spammer could send a message to the FTC's mail server addressed to "aaa@ftc.gov," "aab@ftc.gov," "aac@ftc.gov," etc.
81. Postini: McLean - Spam Forum (April 30, 2003), 109-10.
82. A telephone company assigns a subscriber a unique telephone number containing ten digits – a three digit area code, a three digit local exchange, and a four digit number. A sequential dialing program can be programmed to dial only those numbers with valid area codes and local exchanges.
83. Confidential 6(b) Order response.
84. Such a Registry would be a unique source of valid email addresses. ASRG: Levine, 15; Comcast: Lutner, 8; Junkbusters: Catlett, 6; NRF: Treanor, 7.
85. Association of National Advertisers-Comment, 2. According to many the Commission consulted, a list of merely active email addresses is far more elusive and much more valuable than a list of phone numbers. *See* Aristotle: Bowles, 14; ASRG: Levine, 15; Comcast: Lutner, 8; EFF: Cohn, 12; Newsletter & Electronic Publishers Association ("NEPA")-Comment, 2; NortelNetworks: Lewis, 16; Verizon-Comment, 3; Washington Office of Attorney General ("WAOAG"): Selis, 26.
86. Aristotle: Bowles, 15; Comcast: Lutner, 8; EFF: Cohn, 12; NEPA-Comment, 2; NortelNetworks: Lewis, 16; Verizon-Comment, 3; WAOAG: Selis, 26.
87. EFF: Cohn, 12.

only remaining barriers that can slow spammers down.[88] As a Virginia Assistant Attorney General stated:

> [That is] a goldmine that you actually now have confirmed email addresses. There are spammers that spam just to find legitimate email addresses. And you go to a list there that is already guaranteed.[89]

Knowing that they will be reaching millions of people, spammers very likely would pay a premium for a list of active email addresses.[90] Because a Registry likely would be so valuable to spammers,[91] many sources we spoke with expressed serious concern. They are convinced that spammers would stop at nothing to obtain this list and misuse it to the detriment of consumers.[92] The Commission agrees with their assessment.[93]

2. Existing computer security techniques are inadequate

RFI responders proposed three computer security techniques that they claim would significantly reduce the security and privacy risks associated with a Registry of individual email addresses: (1) the centralized scrubbing of marketers' distribution lists; (2) the conversion of addresses to one-way hashes; and (3) the seeding of the Registry with "canary" email addresses. As explained below, while each of these techniques can reduce certain types

88. MCI: Mansourkia, 9.

89. Virginia Office of Attorney General ("VAOAG"): McGuire, 30.

90. CipherTrust: Judge, 29-30; Comcast: Lutner, 8; NortelNetworks: Lewis, 29. It is difficult to predict how much a valid address on the Registry could command in the market. One computer security expert retained by the Commission estimates that a list containing hundreds of millions of addresses would be worth millions of dollars. Rubin Report, 5. The Commission finds this estimate plausible. Unverified addresses sold on the Internet cost fractions of a cent. According to a report at www.internetnews bureau.com, email marketers can rent verified email addresses (for one time use) at a cost of 10 to 40 cents each. http://www.internetnewsbureau.com/ medianet/fourFour.html. A technologist interviewed by the Commission reports that verified email addresses sell for as much as 50 cents each. CipherTrust: Judge, 29. Even if valid addresses on the Registry sold for one cent each, a Registry of 300 million addresses would fetch $3 million.

91. Email marketers can charge their clients using a variety of metrics. For instance, a marketer could charge based on the number of messages sent or even the number of messages opened. As one email marketer who spoke at the Spam Forum explained, by including an html pixel in each message (also known as a "web beacon"), the marketer can tell when a message has been opened. Betterly - Spam Forum (May 1, 2003), 18. For spammers who charge clients based on the number of delivered messages, a list of valid email addresses would be especially valuable. Moreover, according to www.wired.com, a significant number of spammers make money by trafficking in email addresses. For these spammers, a list of valid email addresses would be valuable, as well. http://www.wired.com/news/ebiz/ 0,1272,57613,00.html.

92. Direct Marketing Association ("DMA")-Comment, 9; ESPC-Comment, 7; Junkbusters: Catlett, 6; MBNA: Collingwood, 44-45; NortelNetworks: Lewis, 16; USISPA-Comment, 3; Verizon-Comment, 3; VOAG: McGuire, 29; *but see* NCL-Comment, 3 (NCL does not believe that the information will be used for illegal marketing or malicious purposes because there would likely be substantial penalties for misuse and spammers would refrain from targeting registered addresses because these would be the least likely consumers to be receptive to spam). The Telemarketing Sales Rule includes certain structures and sanctions to prevent misuse of the Registry. See 16 C.F.R. §§ 310.4(b)(2), 310.4(b)(3)(iv), and 310.8. The success of these measures cannot easily be replicated in the email context, however, because the anonymity of email allows spammers to remain hidden and unaccountable for their actions. *See infra* Section IV.C.

93. According to a widely-held view, "[t]here is little reason for a spammer to limit the number of messages sent, or be selective about the chosen recipients, since the marginal cost of every

of computer security threats, they would not prevent the misuse of Registry data by spammers.

a. Centralized scrubbing would not prevent Registry misuse

Rather than distributing copies of the Registry, the Commission could instead require email marketers to submit their distribution lists to the Commission or its contractor to be scrubbed. The Commission or its contractor would then return a list purged of email addresses appearing on the Registry. Although all ten of the RFI responses that proposed registries favored the use of a centralized scrubbing mechanism, centralized scrubbing would not prevent spammers from using the Registry to obtain valid email addresses.[94]

While a centrally-scrubbed Registry would prevent spammers from obtaining a full copy of the Registry, they would still be able to use the Registry to find valid email addresses by comparing their pre-scrubbed and post-scrubbed lists.[95] Email addresses that are removed by scrubbing are valid addresses on the Registry. Addresses that remain may or may not be valid. Thus, list scrubbing has a fatal flaw; spammers can use it to purify their mailing lists.[96] By submitting numerous lists of email addresses to the Commission or its contractor, over a period of time, spammers could reconstruct a large subset of the Registry or perhaps virtually the entire database.[97] Indeed, spammers could run

additional message is effectively zero." *Legislative Efforts to Combat Spam: Hearings before the House Subcommittee on Commerce, Trade, and Consumer Protection and the Subcommittee on Telecommunications on the Internet,* 108th Cong., 1st Sess. (2003) (testimony of Ira Rubenstein on behalf of Microsoft Corp.). At the same time, commentators agree that spammers will pay a premium for valid email addresses. These two popular beliefs produce an apparent paradox: if the marginal cost of sending an additional message is close to zero, why are address lists so valuable? A spammer should not be willing to pay for 500 valid addresses if it is costless to send messages to another one million addresses, only 500 of which happen to be valid. This apparent paradox, however, may be resolved if spammers face other costs beyond the direct cost of sending another email.

At least two other costs may be significant. First, as spammers send more messages, they necessarily increase the number of undeliverable messages coming from their IP addresses. ISPs, however, filter out all messages from an IP address from which a high number of undeliverable messages are sent. This filtering increases the probability that *all* of a spammer's messages from that IP address will not be delivered, including those messages that would have been delivered but for the undeliverable messages that were sent with them. The loss of sales from those otherwise deliverable messages is an *expected* cost of sending additional undeliverable messages (i.e., the increased probability of detection by a spam filter times the expected lost revenue from the filtered messages). Second, if the spammer wishes to avoid this lost revenue, he or she must expend additional resources to evade filtering. Although the Commission is unaware of any reliable studies focused on spammers' precise costs, avoiding detection undoubtably results in expenditures such as those associated with activating zombie drones, identifying open proxies, and including random characters in messages so each message appears unique.

94. Besides the risk that spammers with authorized access to the Registry would misuse that access, there is a risk that hackers could obtain a copy of the Registry. A computer security expert retained by the Commission opines that a Registry would be "the kind of *prize* that attracts hackers." Rubin Report, 7.

95. ASRG: Levine, 7, 13; Consumer Action ("CA"): McEldowney, 9; Consumer Federation of America ("CFA"): Fox, 8-9; Edelman, 11; Google: McLaughlin, 12-13; Net Creations: Mayor, 10; Roving Software: Olson, 51; Spamcop: Haight 6-7; Word to the Wise: Atkins, 15.

96. Felten Report, 4; Rubin Report, 6.

97. Spamcop: Haight, 6-7.

dictionary attacks against the Registry, itself, thereby assuring that their spam would only go to valid addresses.[98]

Although the Commission would know the identities of marketers who submitted their lists, it would have no means of knowing whether they misused the Registry data. A law-abiding marketer who purchased an email list on the Internet and submitted it to the Commission for scrubbing would be indistinguishable from a malicious spammer who purchased the same list on the Internet and submitted the list to validate addresses for future spam. The Commission would only know if a spammer had misused the list data if the spammer included its own name in the violative spam – an unlikely scenario. Similarly, if the spammer sold the list of valid addresses to another spammer, the Commission could not know whether the spammer who submitted the list had misused Registry data.[99]

b. One-way hashing would not prevent Registry misuse

Some RFI responses proposed the use of one-way hashes to encrypt Registry data. One-way hashing involves using cryptographic algorithms to transform a string of text into character strings called "hashes."[100] (*See* Graphic 3).[101] It is virtually impossible using current computing power to determine an original un-hashed text by analyzing the resulting hash. Thus, if someone obtained the Registry of hashed email addresses, the database could not be un-hashed and turned back into a list of email addresses. The robust nature of one-way hashes has led some to conclude that a hashed database could substantially reduce the risk that the Registry of individual email addresses would become available to spammers.[102]

A hashed Registry would work like a Registry of individual email addresses,[103] with some important additional features. A consumer would enter an email address on the Registry using a web-based form. The Commission would then send a confirmation email to the consumer's email address. To activate the registration, the consumer would return to the Registry's web site and enter a code appearing in the confirmation email. Upon activation of the registration, the Commission would convert

98. Rubin Report, 9; Junkbusters: Catlett, 19; Microsoft: Goodman, 10; SpamCop: Haight, 7-9; UOL: Popek, 11-12.

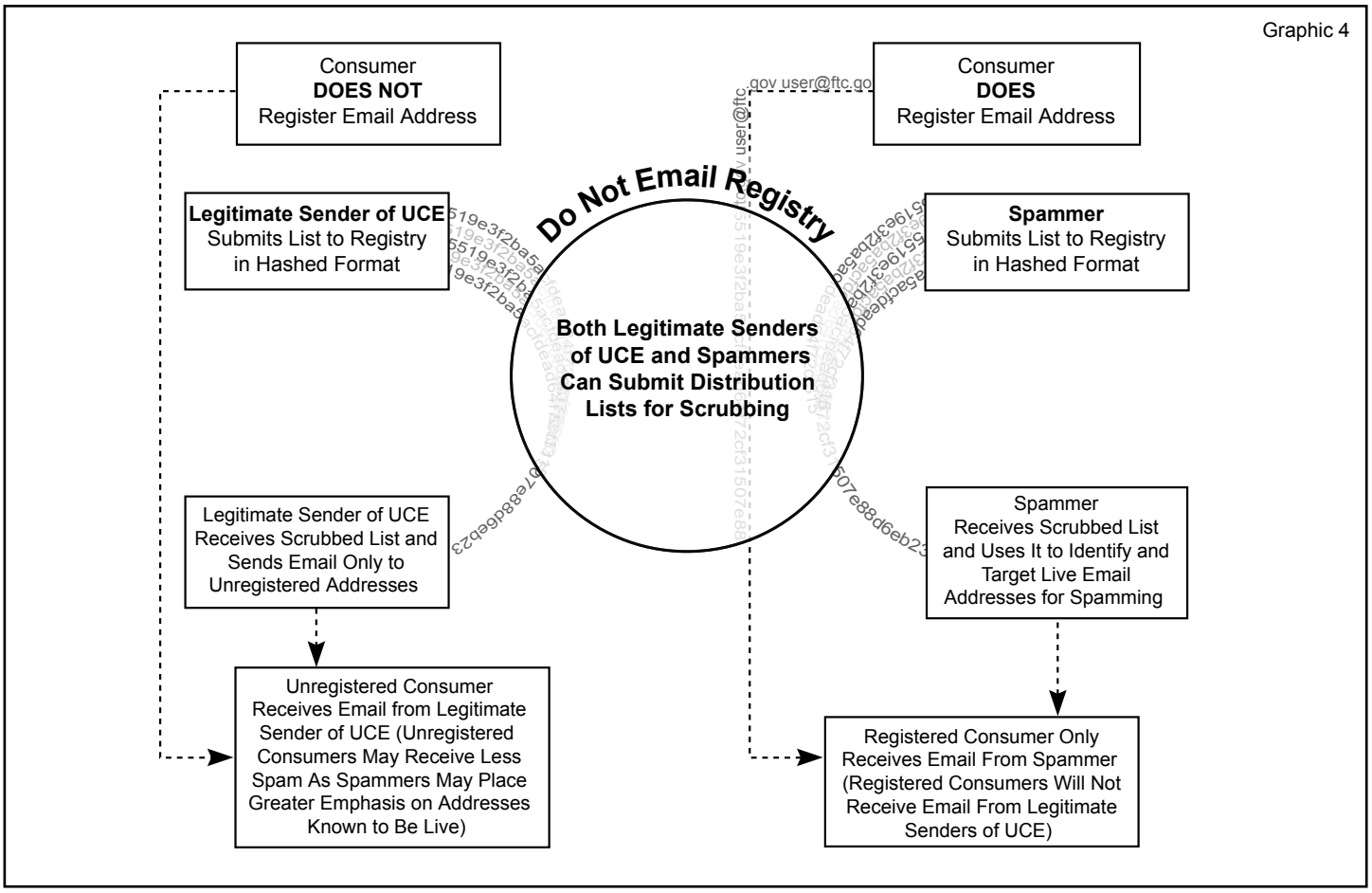
99. Notably, although the RFI asked responders to describe security precautions that would identify misuse of Registry data by registered marketers, none of the RFI responses proposed a method for distinguishing between legitimate marketers who present lists for scrubbing and illegal spammers who present lists for address validation.

100. Hashing algorithms are publicly available. The National Institute for Standards and Technology requires government agencies to use particular hashing algorithms for securing unclassified, sensitive data. http://csrc.nist.gov/publications/fips/fips180-2/fips180-2withchangenotice.pdf.

101. The hashed email address in Graphic 3 was created using the secure hashing algorithm standard known as "SHA-1."

102. Coalition Against Unsolicited Commercial Email ("CAUCE"): Everett-Church, 14.

103. *See supra* Section IV.A.1.



the email address to a one-way hash using a publicly-known hashing algorithm. The entire Registry would be stored as one-way hashes.

A marketer authorized to use the Registry would convert registered email addresses on its distribution list into hashes using the same hashing algorithm used by the Commission.[104] The marketer would also create a database that identified each original email address and its associated hash. The marketer would then submit its hashed distribution list to the Commission for scrubbing. The Commission would compare the marketer's hashed distribution list to the hashed Registry and return to the marketer a hashed distribution list purged of those hashes appearing on the Registry. A legitimate marketer would then send messages only to those addresses that corresponded to hashes on the list returned by the Commission. An illegitimate spammer, however, could determine which of the addresses on its original distribution list were on the Registry (and therefore valid addresses) by comparing the hashed list submitted to the Commission with the scrubbed list of hashes returned by the Commission and determining the email

104. Random characters known as a "salt" are often added to a string of characters prior to conversion of the characters to a hash. In other words, rather than simply hashing "abc@ftc.gov," a random string of characters would be added to this email address and the resulting character string (e.g., "05d6aabc@ftc.gov") would be converted to a hash. Salting provides little, if any security benefit because salts would need to be stored along with the hashes. Bishop Report, 4; Rubin Report, 11. Moreover, using a simple personal computer, a spammer could easily conduct a dictionary attack on a salted and hashed version of the Registry. Bishop Report, 4.

addresses that corresponded to the purged hashes.[105] (*See* Graphic 4).

Although a hashed Registry would provide some measure of security against a hacker, it would not protect against the more likely threat of a spammer using the Registry as a tool for validating email addresses. As a computer security expert retained by the Commission explained:

> Cryptographic hashing can be thought of as a method for "anonymizing" an address, so that the original address cannot be recovered from the anonymized version. Giving emailers only the anonymized version of the list, and not the original list itself, helps to protect the original list from becoming a source of new addresses for spammers. However, due to the mathematical properties of cryptographic hashes, it is still possible for a person who knows an email address to tell whether that address is on the anonymized list. So a system based on cryptographic hashes is roughly equivalent, from a security standpoint, to one that allows emailers to query a centralized database to check whether particular addresses are on the list.[106]

In sum (as Graphic 4 depicts), either un-hashed or hashed, centrally-scrubbed or distributed, the legitimate bulk emailer needs to know which addresses on its distribution list are on the Registry. The necessary corollary is that the illegitimate spammer can use the Registry to deduce valid email addresses.[107] As the executive director of the ESPC noted:

> I believe there is absolutely no technical way of avoiding that problem. That is an inherent part of this. If I have a list and I want to send a mail, and you want to tell me not to mail certain people on it, you have to tell me who not to mail it to.[108]

c. Seeding the Registry would not prevent abuse

Some RFI responders also claimed that the risks of Registry abuse could be reduced by seeding the Registry database with secret FTC-controlled addresses ("canary addresses").[109] To ensure that the emails the canary addresses received were true indicators of Registry misuse, each canary address would have to be extremely unlikely to receive spam, absent a Registry violation. In other words, the canary addresses could not be circulating on email lists on the Internet and would need to include characters unlikely to be generated by a dictionary attack program.[110] For instance, using a random character generation program, the Commission could establish the email address "25ce12a4 @federaltcommiss.com." The address would be monitored constantly. Any email sent to the canary address would indicate that the Registry had been misused.

105. A spammer with little technical sophistication could easily convert millions of email addresses to hashes in seconds using a standard desktop computer. Rubin Report, 8.

106. Felten Report, 3-4 n.2. Another computer security expert retained by the Commission explained that "hashing provides absolutely no security against a marketer who obtains a scrubbed list and uses [it] to sell the addresses that were scrubbed by the Registry." Rubin Report, 8.

107. EFF: Cohn, 21.

108. ESPC: Hughes, 52.

109. *See also* Aristotle-Comment, 2.

110. If the Registry were seeded with FTC-controlled email addresses that were likely to be targeted by dictionary attack programs (e.g., "john@ftc.gov"), the receipt of a message at this address would not necessarily indicate that the Registry had been misused to search for valid addresses. A spammer with a dictionary attack program may have sent the message.

Although seeding the Registry with canary addresses could aid the detection of the outright hacking of an un-hashed Registry,[111] it is difficult to see how seeding could prevent spammers from misusing a Registry. Because a canary address would not be circulating on email lists and would include character strings unlikely to be created by a dictionary attack program, the canary address would not appear in a spammer's pre-scrub distribution list and would, therefore, never be included in the scrubbed list.[112]

Even if the Commission were to distribute un-hashed copies of a Registry to marketers, the receipt of email at a canary address would be too little and too late to help. The widespread use of false headers, open relays, open proxies, and zombie drones would make it exceedingly difficult to trace a message from the seeded address back to its source.[113] Furthermore, seeding the database would not prevent abuse. It merely would make it possible to detect misuse of the Registry *after* the Registry has been compromised.[114] By the time misuse is detected, however, the "cat is already out of the bag."[115] Once the Registry, or a substantial portion of addresses on the Registry, were leaked, those consumers would become targets for even more spam than before registering. One representative from NortelNetworks speculated that, within days, the database would be offered on the Internet.[116] The only remedy at that point would be for millions of registrants to change their email addresses.

In sum, a Registry with individual email addresses would suffer from a significant security weakness. Spammers could use the Registry to validate email addresses, thereby causing consumers to receive more spam. Centralized scrubbing, hashing, and seeding with canary addresses fail to alleviate this risk.

C. Obstacles to Enforcement

The Commission has pursued a vigorous law enforcement program against deceptive spam, and to date has brought 62 cases in which spam was an integral element of the alleged overall deceptive or unfair practice.[117] The FTC's experience in these cases shows that the primary law enforcement challenge is

111. If a hacker were to obtain an un-hashed copy of the entire Registry and sell the data to a spammer, the canary address would receive spam. If a hacker obtained a copy of a hashed Registry, the hacker would convert distribution lists found on the Internet or created with dictionary attack programs into hashes and scrub these hashed distribution lists against the hashed Registry. The canary addresses would be unlikely to appear on the hacker's pre-scrubbing distribution lists because the canary addresses would be designed to be virgin addresses that were dictionary-attack resistant. As one computer security expert concluded, "canaries are useless when dealing with a hashed registry." Rubin Report, 12.

112. Rubin Report, 11-12.

113. CipherTrust: Judge, 27.

114. Rubin Report, 12.

115. Junkbusters: Catlett, 6; Comcast: Lewis, 14; NortelNetworks: Lewis, 30.

116. NortelNetworks: Lewis, 17. By the time a canary address received a message, "in all likelihood, all of the addresses have already been compromised, and the owners of those addresses will realize this when they start to get flooded with spam." Rubin Report, 12.

117. Most of those cases focused on the deceptive content of the spam message, alleging that the various defendants violated Section 5 of the FTC Act through misrepresentations in the body of the message. Two recent cases also alleged violations of the CAN-SPAM Act. *See FTC v. Phoenix Avatar, L.L.C.*, No. 04C 2897 (N.D. Ill. 2004) and *FTC v. Global Web Promotions Pty. Ltd.*, No. 04C 3022 (N.D. Ill. 2004).

identifying and locating the targeted spammer. The ability of spammers to hide their identities by using false headers, open relays, open proxies, zombie drones, and foreign servers makes tracing an email's path an often fruitless task.[118] Tracing an email almost always leads to a dead end because spammers rarely send messages from their own email accounts. ISPs which, like the Commission, have considerable experience dealing with spam, have been similarly stymied by spammers' use of zombie drones and other camouflage tactics.[119] Absent the adoption of an effective domain-level authentication system for email, a National Do Not Email Registry would not improve the ability to track down spammers and would, therefore suffer from the same enforcement obstacles that currently beset law enforcement and ISPs.[120]

Unable to identify a spammer based on the email trail,[121] law enforcement and ISPs must locate spammers by tracing the flow of funds from victim to spammer. Experiences of law enforcement and ISPs belie claims that spammers can be caught easily.[122] First, numerous spam messages, such as those that are purely malicious vehicles for viruses and Trojans, do not request money. Second, spammers that request funds often use novel payment methods, offshore banks, stolen credit card accounts, and other techniques that make tracing the flow of money a painstaking, and often futile, endeavor.[123]

The difficulties of pursuing spammers can be seen in the experiences of prosecutors from Washington and Virginia – two states that have been in the forefront in bringing civil and criminal cases against spammers. Prosecutors in both states agree that these cases are difficult and costly, mainly due to the challenge of tracing and identifying the spammers. A prosecutor in Washington State spent four months and sent out 14 pre-suit civil investigative demands ("CIDs") just to identify the spammer in one lawsuit.[124] Likewise, in another case, it took the Virginia Attorney General, over the course of four months, multiple subpoenas to domain registrars, credit card companies, and Internet providers, and the execution of a search warrant,

118. Some have argued that a Registry would assist the Commission's enforcement because it would provide a cut-and-dried, easy-to-prove violation. Internet Law Group ("ILG"): Praed, 9. The enforcement challenge, however, does not consist of having inadequate legal bases to challenge spammers' conduct. WAOAG: Selis, 36. As one prosecutor pointed out, "finding the person is the trick." VAOAG: McGuire, 37; *see also* Piper Rudnick-Comment, 1; Software and Information Industry Association-Comment, 4.

119. Communications with ISPs regarding Confidential 6(b) Order responses.

120. An unsecure and unenforceable Registry would likely result in public discontent due to unfulfillable expectations. AT&T: Cade, 20; Junkbusters: Catlett, 9; National Association of Realtors-Comment, 4; U.S. Internet Service Provider Association-Comment, 3-4; Verizon-Comment, 5.

121. The Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. §§ 2702-03, further complicates Commission spam investigations by limiting the types of information that the Commission can obtain from ISPs.

122. NCL: Grant, 11-12.

123. When spammers operate from outside the United States, the Commission faces additional, and sometimes insurmountable, enforcement hurdles. The Commission has found no reliable statistics on the percentage of spam that comes from marketers located within or outside of the United States. Rampant spoofing and the use of open relays, proxies, and zombie drones often make it impossible to determine a spam message's originating country.

124. WAOAG: Selis, 15. The Commission's spam cases routinely require the issuance of numerous CIDs. For instance, in one case, it took a series of 12 CIDs for the Commission to identify the spammers. *See FTC v. Cella*, No. CV03-3202 (C.D. Cal. 2003).

before having enough information to file a case against a spammer.[125]

ISPs have experienced similar obstacles in bringing suits against spammers. An attorney for Earthlink explained that finding the spammer is the greatest challenge in spam litigation.[126] One major ISP reports that after collecting and analyzing over 45 million spam messages received by its "honeypot" email accounts[127] during 2003, it linked only about 2.6 million to a person responsible for them.[128] In all, this ISP identified 271 parties responsible for these 2.6 million spam messages, but acquired sufficient information to file a lawsuit or send a warning letter to only 91 of the parties.[129] To identify these 91 parties, the ISP estimates that its internal and outside legal teams expended approximately 12,100 hours – an average of 133 hours per spammer.[130] The ISP expended these resources solely to identify the spammers; these costs do not include litigation expenses. Another major ISP reported that as a result of spammers' obfuscatory techniques, amassing the required evidence for one lawsuit required eight people who expended approximately 1,000 hours of work.[131]

In addition, many cases filed by major ISPs must be filed as "John Doe" lawsuits because the ISPs cannot identify the spammer prior to filing.[132] For instance, Microsoft, AOL, Yahoo!, and Earthlink recently announced six lawsuits against 225 defendants, charging violations of the CAN-SPAM Act. These ISPs charged all but nine of the defendants as "John Does" at the time the suits were filed. In previous "John Doe" lawsuits, ISPs have needed to issue up to ten subpoenas to determine the identity of the spammer.[133] According to one ISP that has sued numerous spammers, litigation costs can range from $100,000 or less (when the spammer is easily identifiable) to more than $2 million (when the spammer mounts an aggressive defense).[134] Not surprisingly, some ISPs believe that lawsuits against spammers are an expensive and often fruitless way to stop spam.[135] Instead, these ISPs expend the bulk of their anti-spam resources improving their filtering technologies.[136]

125. VAOAG: McGuire, 5-11. By contrast, in an FTC telemarketing fraud case, the Commission can frequently identify culpable parties and gather sufficient evidence to warrant filing a complaint and seeking a temporary restraining order without issuing a single civil investigative demand, or by issuing only a single CID to a telephone or shipping company. Instead, the Commission staff collect evidence from victims, pose as potential customers, and obtain information from publicly-available sources.

126. Wellborn & Butler, LLC: Wellborn-Spam Forum (May 2, 2003), 171; *See also* Comcast: Lutner, 38; MBNA: Marshall, 13; NetCreations: Mayor, 10-11; NRF: Treanor, 9-10; Savicom: Bernard, 14-16.

127. A "honeypot" email account is an email account established for the purpose of monitoring email traffic.

128. The ISP uses these "honeypot" email accounts in connection with its spam filtering activities. The spammers responsible for these 2.6 million messages undoubtably sent millions more messages to consumers' email addresses. Confidential 6(b) Order Response.

129. The evidentiary requirements for filing a lawsuit are obviously much more rigorous than the factual standard for sending a private cease and desist letter.

130. Confidential 6(b) Order Response.

131. Confidential 6(b) Order Response.

132. A "John Doe" lawsuit is a case filed against an unknown defendant. The plaintiff in such a case hopes to use court-authorized discovery to determine the name of the defendant.

133. Confidential 6(b) Order Response.

134. Confidential 6(b) Order Response.

135. Conversations with ISPs regarding Confidential 6(b) Order Responses.

136. Conversations with ISPs regarding Confidential 6(b) Order Responses.

The success of the National Do Not Call Registry stems in large measure from the fact that most telemarketers and their clients are law abiding businesses that care about their reputations and want to follow the law. For the small number of unscrupulous telemarketers, the realistic threat of law enforcement provides considerable incentive to obey the law. This threat is based on the ease of determining the party responsible for the telephone number from which a call is placed. Because the telephone system is a "caller-pays" model, it enables carriers to bill charges to numbers from which calls are placed. This is done through the Automatic Number Identification system (ANI), which is the basis for telephone billing.[137] The ANI data creates an auditable trail, which facilitates accountability.

In contrast, most bulk emailers appear to be spammers who have shown little concern for their reputation and even less inclination to obey the law. Moreover, as discussed previously, the barriers to robust law enforcement render the threat of legal action an ineffective means of ensuring widespread compliance.

D. Practical/Technical Concerns

All variations of a National Do Not Email Registry pose practical and technical problems for legitimate email marketers that, given the current state of technology, threaten to make a Registry unworkable. The following Sections describe the practical concerns raised by a Registry that includes individual email addresses, domains, and a third-party forwarding component, respectively.

1. A National Do Not Email Registry that includes individual email addresses poses practical concerns

The sheer size of a National Do Not Email Registry database would affect the scrubbing processes.[138] The RFI responses all assumed that consumers would initially register 300 million email addresses, and that the Registry might grow to include as many as 450 million addresses.[139] For individual marketers to scrub their distribution lists against a distributed Registry could pose significant challenges. The International Council of Online Professionals ("ICOP") believes that the "constant list-scrubbing requirements of the Registry would be beyond the technological capabilities that most online micro-businesses would possess or could hire."[140] Moreover, the ESPC believes that the technological infrastructure costs to support the volume of requests for access to the Registry would be "daunting."[141] A representative from the National Retail Federation explained that scrubbing against the Do Not Call List of 60 million phone numbers can take several days for some of its members.[142] Delays like this for scrubbing against an email Registry, which could contain at least 300 million email

137. In addition, since January 29, 2004, telemarketers have been required to transmit caller identification information. 16 C.F.R. § 310.4(a)(7); 47 C.F.R. § 1601(e). Only the most sophisticated telemarketers can falsify caller identification information without the assistance of their telephone carrier. Nov. 19-20, 2003 briefings of FTC staff by telephone carriers.

138. NRF-Comment, 9.

139. Some have estimated that the database would grow to a billion or more email addresses. ASRG: Levine, 19; IMN, Inc.: Mesnik, 33; Junkbusters: Catlett, 31.

140. ICOP-Comment, 8.

141. ESPC-Comment, 5.

142. NRF: Treanor, 9.

addresses, could potentially jeopardize business for legitimate companies engaged in email marketing.[143]

Under either a distributed or centrally-scrubbed model, legitimate marketers would incur an increase in scrubbing costs over time because no effective method exists to purge defunct email addresses from a Registry. Unlike the Do Not Call Registry, which purges outdated phone numbers through the use of databases of phone numbers, a Do Not Email Registry would continue to balloon in size because there is no such database of outdated email addresses. This means that the burden would be on consumers to update the Registry when they stop using email addresses – an unlikely scenario.[144] Estimates of email address churn rates vary,[145] but even the lowest estimated rates could result in a very large list containing many stale addresses, causing an inefficient and expensive scrubbing process for marketers.[146]

143. A centrally-scrubbed Registry could pose similar challenges for small marketers. Although the Registry would perform the actual scrubbing function, the marketers would need to prepare their distribution lists for submission to the Registry and process the information received from the Registry.

144. Center for Democracy and Technology ("CDT")-Comment, 3.

145. A RoperASW study commissioned by Bigfoot Interactive in November 2003 found that 11 percent of adults had switched their ISPs or email service providers within a six-month period. *Email and Spam: Consumer Attitudes and Behaviors*, 4. The DMA estimates the churn rate for email addresses to be 32 percent. DMA-Comment, 10. Consumers abandoning email addresses clogged with spam undoubtedly contribute significantly to the churn rate.

146. DMA: Cerasale, 35-36; National Multi-Housing Council and National Apartment Association-Comment, 2. Shortening the effective period of a registration could reduce the stale address problem and the consequent growth of the list. The shorter the period, the fewer stale addresses would be on the list. Shorter registrations, however, would require consumers to renew their registrations regularly.

147. *See supra* Section III.B.2.

148. *See supra* n.73.

149. *See supra* Section IV.C.

150. UOL: Popek, 31.

2. A National Do Not Email Registry that permits registration of domains poses additional concerns

A National Do Not Email Registry that permits registration of domains would merely put the government's imprimatur on ISPs' existing anti-spam policies without reducing the scope of spam. In addition, the ineffectiveness of the opt-in regime instituted in the United Kingdom illustrates the inherent weakness of a domain-level Registry without effective domain-level authentication for the source of email messages.

a. The failure of ISPs' current anti-spam policies illustrates the likely ineffectiveness of a domain-wide Registry.

The ISP industry's current standard policy is to block "unsolicited bulk email."[147] Although a National Do Not Email Registry containing domain names would alleviate the security issues inherent in a list of individual email addresses,[148] given the challenge in enforcing any form of a National Do Not Email Registry,[149] such a Registry of domains would be no more effective than ISPs' current policies. Without additional enforcement tools, restating the industry's well-known standard policy would "change relatively little."[150]

b. A Registry of domain names would create an opt-in system similar to the United Kingdom's regime, which has not had a significant impact on the spam problem.

A National Do Not Email Registry containing domain names would be tantamount to establishing an opt-in system similar to that recently enacted in the United Kingdom. This is because if all domains registered on a National Registry, then consumers who wanted to receive email from any marketer, legitimate or illegitimate, would have to opt-in to such messages.[151] The United Kingdom instituted its opt-in system in December 2003 pursuant to the European Community's Directive on Privacy and Electronic Communications.[152] Based on statistics provided by Brightmail, an international email filtering company, this opt-in system has not had any meaningful effect on the volume of spam. Graphic 5 illustrates this point.[153] In June 2003, Brightmail identified 37 percent of the United Kingdom's monthly incoming email as spam. Between June 2003 and April 2004, this percentage steadily increased. Although the opt-in system was instituted in December 2003, when spam accounted for 54.9 percent of United Kingdom email traffic, by April 2004, spam accounted for 60.1 percent of incoming email. These data suggest that the opt-in system has not decreased the amount of spam United Kingdom citizens receive.

3. A National Do Not Email Registry that includes a third-party forwarding service poses additional concerns

A third-party forwarding service model would allow consumers to register their individual email addresses while keeping the Registry secure from rogue marketers.[154] Although this model would maintain the integrity and security of the Registry database, it would: (1) be ignored by the majority of spammers; (2) threaten the email system; and (3) deprive legitimate bulk emailers of key marketing data.

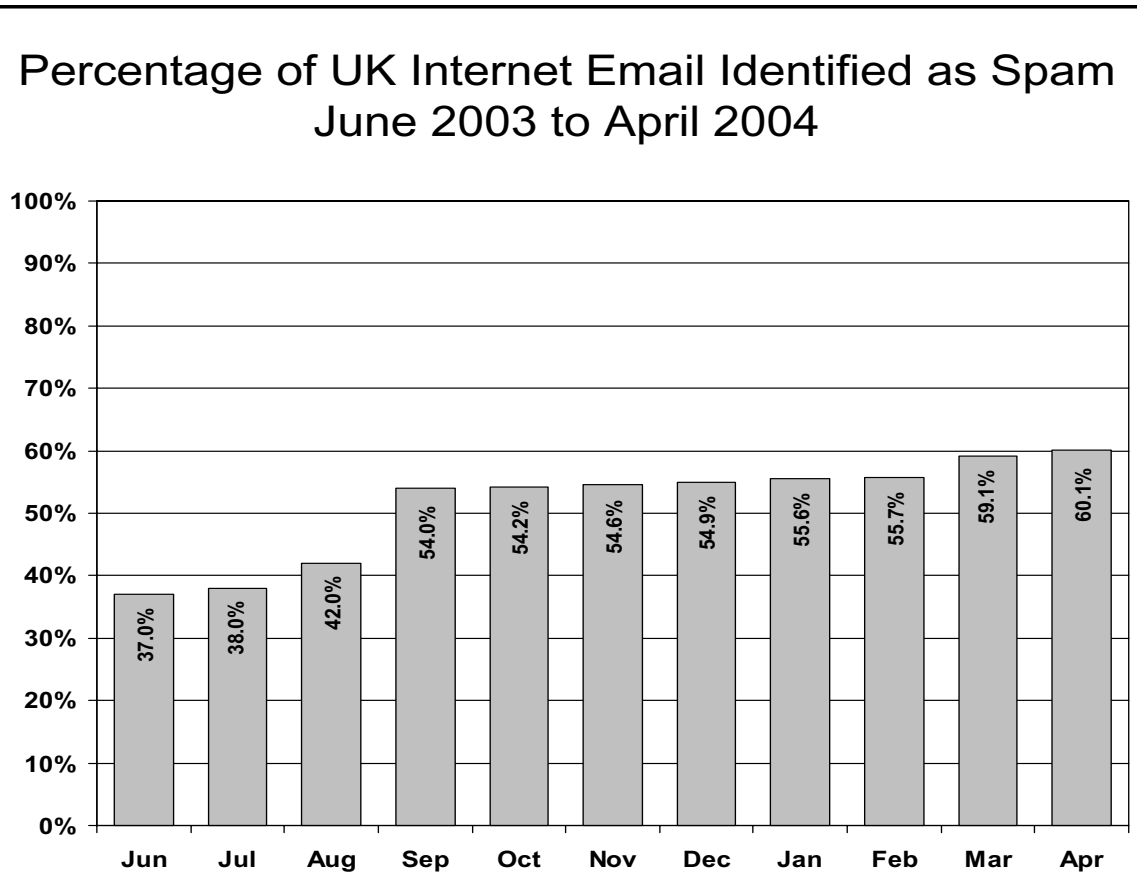
151. One argument posited against a domain-wide Registry is that it would effectively take away a consumer's choice to determine whether to receive spam or not. ASRG: Shafranovich, 20; NCL: Grant, 17. The Commission discounts this argument because if consumers really wanted to receive UCE, there are plenty of ways they could do so. ASRG: Levine, 21.

152. The Directive on Privacy and Electronic Communications (E-Privacy Directive) was adopted in July 2002. The Directive includes a "ban on spam" that must be incorporated into national law by European Union member states. *See* http://europa.eu.int/information_society/topics/ecomm/all_about/todays_framework/privacy_protection/index_en.htm. The United Kingdom's implementation of this directive prohibits emails to individual subscribers unless they have given prior consent and does not cover unsolicited email to corporate subscribers. Corporate subscribers, however, may opt-out of unsolicited email. http://www.dti.gov.uk/industries/ecommunications/directive_on_privacy_electronic_communications_200258ec.html.

153. Brightmail's statistics indicate that the United Kingdom's business to business exemption from the opt-in system has not had a significant impact on the amount of spam received in the United Kingdom because 80 percent of Brightmail's email traffic is addressed to ISPs while only 20 percent is addressed to commercial customers.

154. A third-party forwarding service Registry model envisions that a government contractor would maintain the database of email addresses that consumers register. This contractor – the forwarding service – would receive marketers' distribution lists and "scrub" them against the Registry database. It would then forward the marketers' email messages to the addresses not entered on the Registry. Thus, the marketer would never know who on its distribution list received email and would not receive a scrubbed distribution list back from the forwarding service. This would ensure the security of the Registry list.

Graphic 5



Source: Brightmail

a. The majority of spammers would ignore a third-party forwarding service.

ISPs' filters cannot distinguish between commercial and non-commercial email.[155] This simple fact dooms a third-party forwarding service. If only unsolicited commercial email were required to be sent through the forwarding service, spammers would simply continue to disguise their spam as permission-based, transactional, or personal messages.

Recognizing this fatal shortcoming, one RFI responder proposed a third-party forwarding service model in which all email – commercial, non-commercial, personal, permission-based, spam, etc. – must be submitted to the forwarding service.[156] Under this RFI responder's plan, senders of spam would have to label their messages as "UCE." The forwarding service would then refrain from delivering any messages bearing the label "UCE" to email addresses on the Registry. All other email would be forwarded to ISPs and domain holders, which could use their normal filtering techniques on this non-labeled email stream.

The Commission believes that this plan is wholly unworkable. First, knowing that the inclusion of a "UCE" label will prevent the delivery of their messages, few spammers would

155. Google: McLaughlin, 33; ICC: Halpert, 18, 22; NRF: Treanor, 41.

156. By forcing all email to pass through the hands of an intermediary, this RFI responder's proposal raises serious privacy concerns because the third-party forwarding service would have access to all email messages sent to email addresses in the United States.

comply with the labeling requirement;[157] instead, they would send spam that masquerades as personal, transactional, or permission-based messages through the forwarding service.[158] ISPs and domain holders would be in no better position to filter spam than they are in now. All messages coming through the forwarding service would need to be filtered because a substantial portion of them would likely be spam that did not bear the "UCE" label.

b. A third-party forwarding service would threaten the email system.

A third-party forwarding service model would prevent spammers from using the Registry as a database of valid email addresses. Routing all email through a forwarding service, however, would impose a costly and fragile restructuring on the email system infrastructure. Such a restructuring would threaten email's viability as a communications medium.[159] A technologist from Comcast believes that the infrastructure requirements to build a network to handle the volume of email that would flow through such a service would be "staggering" and would only increase with the passage of time.[160]

This Registry model would increase the volume of email traffic while creating choke points in the email system that do not currently exist. Spam would first be sent to the forwarding service. Then, if the message were sent to an address not on the Registry (i.e., an actual but unregistered address or an invalid address), the message would be sent back into the email system, thereby doubling the amount of bandwidth used. Moreover, if all email were forced to traverse the forwarding service, the robust, decentralized email system would be replaced with a single choke point, transforming email into a fragile system that could grind to a halt, either due to a technical or infrastructure flaw (e.g., a server crash or a blackout) or due to malicious activity (e.g., a denial of service attack).[161] Indeed, two RFI responders – both of which are large computer infrastructure managers – specifically cautioned against the use of a third-party forwarding service model, noting the potential disruption such a forwarding service could cause.[162]

c. A third-party forwarding service may hinder legitimate marketing.

Some legitimate marketers are concerned that this type of forwarding service would take

157. *See infra* n.174.

158. Rubin Report, 6; Google: McLaughlin, 33.

159. Rubin Report, 4. A single denial of service attack against the forwarding service could completely disable email for all people in the United States. *Id.* According to one computer security expert retained by the Commission, "the entity running the forwarding service would represent a huge target for attackers and is likely to be hit hard and often." *Id.*

160. Comcast: Lutner, 35.

161. Rubin Report, 3; AT&T: Cade, 41; CAUCE: Everett-Church, 33; CDT: Bruening, 43; Comcast: Lewis, 34; EFF: Cohn, 41-42; MCI: Mansourkia, 40; Word to the Wise: Atkins, 32. Use of a small set of forwarding services would eliminate a single choke point, but would still create congestion in the networks, clog key portions of the Internet, and slow email to an unacceptable level. Bishop Report, 7. To avoid this congestion, the forwarding service would need to use "thousands, if not tens of thousands or more, servers to check and forward the email." *Id.*

162. One computer security expert the Commission retained, however, believes that a forwarding service model could be implemented in a manner that would not disrupt the email system. Felten Report, 4. This expert, nonetheless, concludes that the Commission should not implement such a forwarding service model because it "will do little good in addressing the spam problem," which is caused by outlaw spammers who would ignore the Registry. *Id.* at 6.

away key components to any marketing strategy – measuring the success of the campaign and understanding the customer.[163] With this type of model, marketers would never know who on their list received their email and would not be able to measure their response rate to a particular email marketing campaign accurately.[164] This type of data helps marketers focus their campaigns to maximize effectiveness. Focusing also reduces the number of people who receive unwanted email.

The costs for legitimate marketers would also increase under this model, including costs associated with scrubbing and forwarding the mail, as well as with the potential loss of business. A representative from the DMA expressed concern over the costs of scrubbing because a marketer would have to submit its full customer list to get scrubbed every time it wanted to engage in an email campaign. This duplicative effort would be necessary because the marketer would never know who was taken off the list previously.[165]

Lastly, there may be costs associated with a loss of business if the turnaround time for the forwarding service is too slow. One advantage of email marketing is the ability to get campaigns out quickly and efficiently. This is especially true during the holiday seasons when businesses are fiercely competing for consumers through price wars, sales, and promotional offers. If the mailing process is delayed, it could not only reduce the effectiveness of email marketing, but could put some businesses at a competitive disadvantage.[166] It could also reduce the incentives for price competition.

E. Impact on Spam

The establishment of a National Do Not Email Registry right now would create expectations on the part of the public that spam, like unwanted telemarketing calls, will disappear or greatly diminish almost immediately.[167] Establishment of a National Do Not Email Registry at this time, however, regardless of its form, would fail to meet these expectations,

163. In addition, some marketers may be concerned about the trustworthiness and reliability of any third-party hired to perform this forwarding service and are apprehensive about handing over their customer lists and advertisements, which contain very valuable information to the marketer, to someone they do not know and have not approved. Comcast: Lewis, 33; MBNA: Marshall, 50-52; UOL: Skopp, 15. Legitimate marketers would not be involved in choosing the forwarding service, and would have to trust that their lists and information would not be compromised or altered. MBNA: Marshall, 52; Spamcop: Haight, 15. Permitting marketers to use one of a number of approved forwarding services could partially alleviate this particular concern.

164. DMA: Cerasale, 28-29; MCI: Mansourkia, 37-38; Shop.Org: Silverman, 57-58.

165. If the marketer must pay for scrubbing on a per email basis, the costs would not diminish with each subsequent campaign. This could make email marketing unaffordable. DMA: Cerasale, 29-30. Of course, a Registry could be financed through mechanisms other than a per-address scrubbing fee.

166. NetCreations: Mayor, 20-21; NRF: Treanor, 10-11; Shop.Org: Silverman, 55.

167. The National Do Not Call Registry has dramatically reduced the number of unwanted and intrusive telemarketing calls American consumers receive. A Harris Interactive® poll released on February 13, 2004, indicates that more than half of all U.S. adults (57 percent) say that they have signed up for the Registry. Ninety-two percent of those who signed up report receiving fewer telemarketing calls, and twenty-five percent of those registered say they have received no telemarketing calls since registering. The success of the Registry results largely from extraordinarily high compliance rates, which in turn depend on the ability of consumers to use caller ID and law enforcement to obtain ANI records to identify violators. Through the end of May 2004, consumers registered over 61.5 million telephone numbers and reported about 400,000 violations.

particularly in the absence of an effective system for authenticating the source of email messages. The Commission does not believe that a National Do Not Email Registry would result in any appreciable reduction in the amount of spam. In fact, it could actually increase the volume of spam.[168] This perverse result is likely because illegal marketers who send spam would use a National Do Not Email Registry as a directory of valid email addresses.[169] In and of itself, a National Do Not Email Registry, regardless of the model, would do nothing to enhance the accountability of bulk-email marketers, or the ability of the Commission and other law enforcement agencies to identify and locate them. Therefore, we do not believe that creating a Registry now would have any beneficial impact on the spam problem.[170]

Each Registry model is largely dependent upon senders' compliance with the law, but spammers have demonstrated and continue to demonstrate that they will do whatever it takes to send out their UCE and will not police themselves. For example, spammers continue systematically to violate ISPs' acceptable use policies by sending unsolicited bulk email. This is true even though ISPs post these policies publicly.[171] Despite ISPs' anti-spam policies, spam accounts for the majority of daily incoming email traffic. For example, spam accounts for 80% of AOL's daily incoming email traffic.[172]

Similarly, spammers ignored state laws requiring that email solicitations contain an "ADV:" label in the subject line of an email message[173] and most are currently not complying with the provisions of the CAN-SPAM Act.[174] Perhaps most tellingly, notwithstanding the CAN-SPAM Act, most spammers continue to disguise their email to bypass filters and engage in

168. While the fact that criminals will not comply with the law does not vitiate the need for laws, Aristotle: Bowles, 17, the crafting of a solution to the spam problem must take into consideration the effectiveness of possible cures.

169. This could not happen with the third-party forwarding service, but the third-party forwarding service is unworkable for other reasons. *See supra* Section IV.D.3.

170. Many have voiced this concern, including anti-spam groups, academics, marketers, and technologists. American Advertising Federation: Rector, 11; Association of National Advertisers-Comment, 2; ASRG: Levine, 39; Comcast: Lewis, 27; Comcast: Lutner, 8, 35, 50; DMA-Comment, 14; Edelman, 12-13, 35; EFF: Cohn, 32-33; ESPC-Comment, 9; ICC: Halpert, 18, 28-29; MCI: Mansourkia, 55, 60; Microsoft: Goodman, 19; NRF: Treanor, 47-48; Piper Rudnick for American Advertising Federation, American Association of Advertising Agencies, Promotion Marketing Association, U.S. Chamber of Commerce-Comment, 1-2; Spamcon: Atkins, 23; Spamcop: Haight, 27; UOL: Popek, 18; USISPA-Comment, 3.

171. *See supra* Section III.B.2.

172. Pew Internet and American Life, *Spam: How it is Hurting Email and Degrading Life on the Internet,* October 22, 2003, p. 8 at http://www.pewinternet.org/reports/pdfs/PIP_Spam_Report.pdf.

173. The Commission's False Claims in Spam Study showed that compliance with the ADV label requirement was "sparse," with only 2% of the spam analyzed following the requirement. False Claims in Spam, 11. *See also* Sorkin, 14, 29; UOL: Skopp, 82.

174. According to one ISP's Section 6(b) Order response, about 30 percent of spam delivered to its subscribers' inboxes in January and February of 2004 purported to contain an opt-out mechanism. Confidential 6(b) Order response. Actual compliance with CAN-SPAM's opt-out mechanism requirement is in all likelihood even lower because the ISP did not test to see if the opt-out mechanisms functioned or whether requests were honored. Spam solution providers offer an even more dismal view of current CAN-SPAM compliance. For instance, MXLogic claims that only three percent of unsolicited commercial email sent during March 2004 complied with the CAN-SPAM Act. http://www.mxlogic.com/news_events/04_09_04.html.

obfuscatory tactics to conceal their identities.[175] As one academic put it:

> [The spammers responsible for the non-CAN-SPAM compliant email] are not likely to comply with what the U.S. government tells them to do either because they're not in the United States or because they think they're doing an awfully good job of hiding who they are and where they are. . . . [T]hey are already outlaws, and you can see it in the sorts of goods and services that they're offering for sale. You can see it in their methods of advertising, the typos, and other tricks. The people are not going to alter their behavior merely because black letter written on a piece of paper somewhere tells them to, but that's a pretty serious problem.[176]

As long as spammers can hide their identity and disguise their emails, they can rarely be held accountable, and spam will continue. As one prosecutor in Virginia stated:

> It's not going to stop. It's too profitable for the people to stop. They're just going to find additional ways to mask the identity of the sender. . . . I think it's just going to create more ways of concealing themselves. But the spam is not going to stop.[177]

A representative from Microsoft believes that the people who are best at getting past Microsoft's filters are the ones who are doing something illegal or unethical and are "willing to do awful things."[178] Spammers have enormous technological skill that they use to conceal themselves and the origins of their emails. ISPs already spend millions of dollars on spam protection,[179] yet spammers continue to reach email users' inboxes through outlaw tactics like hijacking personal computers and customizing each email so that, even though they are actually sent in bulk, each one looks unique.[180] (If email does not appear to be sent in bulk, then the ISPs' filters will not necessarily block it.) So long as there are illegitimate marketers who can disguise their email without being identified, spam will continue.[181]

F. Additional Concerns Regarding a Registry's Impact on Children with Email Accounts

Section 9(a)(3) of the CAN-SPAM Act requires the Commission to explain in this Report "how a National Do Not Email Registry would be applied with respect to children with email accounts." There is cause for concern about spam and its effects on children. According to a study conducted by Symantec Corp., 76 percent of children who use the Internet have one or more email accounts.[182] These email accounts are often bombarded with spam advertising cut-rate mortgages, online dating services, weight loss products, and pharmaceutical products, such as "herbal viagra."[183] Most disturbingly, 47 percent of the children surveyed in this study received spam with links to pornographic websites.[184] Over 20

175. ICC: Halpert, 6; MCI: Mansourkia, 55.

176. Edelman, 12-13.

177. VAOAG: McGuire, 35.

178. Microsoft: Goodman, 19.

179. ICC: Halpert, 14.

180. AT&T: Cade, 45-46.

181. *See supra* Section III.B.2.

182. The study, conducted by Symantec Corp. in June 2003, surveyed 1,000 children between the ages of seven and eighteen. http://www.symantec.com/press/2003/n030609a.html.

183. *Id.*

184. *Id.*

percent of children with email accounts open and read spam messages.[185] Even when children feel uncomfortable, offended, or curious after seeing inappropriate spam, 38 percent of them do not tell their parents.[186]

The Commission has found no data, however, to suggest that spammers currently are targeting children to receive specific types of spam.[187] Rather, children likely receive the same types of offers that adults receive because spammers use indiscriminate marketing techniques.[188] This fact is not surprising because spammers and others currently have no way of knowing that particular email addresses belong to children, unless the children have divulged their ages and email addresses.

It is reasonable to explore a variety of potential approaches to address the spamming of children, including the possibility that a National Do Not Email Registry might provide protection for children's email accounts. Nevertheless, our conclusions with respect to spam in general apply with equal force to spam that children receive: at present, such a Registry would at best be ineffective and at worst could cripple the email system or actually facilitate more spam – including more spam to children.

Furthermore, we conclude that any Do Not Email Registry that earmarked particular email addresses as belonging to or used by children would raise very grave concerns due to the security issues discussed above.[189] The possibility that such a list could fall into the hands of the Internet's most dangerous users, including pedophiles, is truly chilling.

V. Proposed Plan and Timetable for Establishing a National Do Not Email Registry

Given the significant security, enforcement, privacy, technical, and practical concerns identified above, the Commission strongly believes that implementation of a National Do Not Email Registry, particularly in light of the current lack of authentication, would be costly, potentially counter-productive, and without any appreciable benefit from spam reduction or increased law enforcement capabilities. Anti-spam efforts should presently focus on one of the core causes of the problem – the ability of spammers to use obfuscatory techniques such as spoofing, open relays, open proxies, and zombie drones.[190]

185. *Id.*

186. *Id.*

187. When Commission investigators "seeded" 175 different locations on the Internet with 250 undercover email addresses, they found that the content of the resulting spam was unrelated to the location on the Internet from which the address was harvested. http://www.ftc.gov/bcp/online/pubs/alerts/spamalrt.html.

188. According to one ISP's Confidential Section 6(b) Order response, about a quarter of all spam delivered to its subscribers inboxes in January and February 2004 contained sexually explicit material or reference. Confidential 6(b) Order Response. The Commission found that 17 percent of pornographic offers in the spam it analyzed contain "adult imagery." False Claims in Spam Report, 13.

189. Some RFI responders suggested permitting parents to register the email addresses of their children. One RFI responder, however, proposed a system that would collect a child's email address, birthdate, and jurisdiction where the child lives. According to this RFI responder, email marketers could use such data to ensure compliance with the Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501-6506, and state children's protection laws.

190. The Commission's plan does not address the other root cause of spam – the cost structure of email that makes it virtually free to send additional messages. Cost-shifting mechanisms would most likely require a dramatic restructuring of the email system and

The private market is already moving toward creating systems for authenticating that an email message actually comes from a mail server operated by the second-level domain appearing in the message.[191] Even though domain-level authentication cannot necessarily authenticate the particular person who sent an email, it does authenticate the domain from which the email originated. Law enforcement can then contact the domain to obtain information that could identify the individual sender of the email.[192]

While the marketplace should be given adequate time to test and phase-in an authentication standard,[193] Commission support may help accelerate the pace.[194] Moreover, the Commission may be able to help focus efforts so that smaller ISPs and businesses, as well as individuals who operate their own domains, can readily use the ultimate protocol that emerges.[195] Finally, the Commission can lend support to evaluating the international implications of an authentication standard.

The Commission recognizes that, in an area of rapidly developing technology, government intervention can stifle innovation. As one academic has explained:

> [G]enerally the experience we've had with trying to hard code technology into the law has not been successful. The law can't change quickly enough. It may stifle the development of technology, and frequently we just get the technology wrong when we try to put it into the law.[196]

Mindful of the risks inherent in the government attempting to regulate technology, through the following plan, the Commission will encourage the private market to move quickly to develop an authentication standard – an essential preliminary step, without which implementation of a Registry would, in our judgment, fail. The Commission, therefore, proposes the following four-step plan.

A. Conduct an Authentication Summit

To ensure that authentication standards are developed in an open environment and can be easily adopted by smaller ISPs and domain owners, the Commission, in conjunction with other relevant government

pose significant issues (such as who should pay, who should receive payment, and how much should be paid). The development of a new email protocol to support a cost shift that resolves these significant issues is not likely in the near term.

191. *See supra* Section III.C. None of the private market proposals aims to authenticate that messages actually come from the particular email addresses listed in the "From:" line. While domain-level authentication schemes can be imposed without significant adjustments to the architecture of the email system, sender-level authentication may require substantial changes in official email protocols and the software used by both operators of email servers and by individual computer users.

192. Under ECPA, the Commission can issue a CID seeking six types of information to a domain hosting an email account that was used to send spam: (1) name of the email account holder; (2) address of the account holder; (3) records of session times and durations; (4) length of service and types of service utilized; (5) subscriber number or identity, including any temporarily assigned network (IP) address; and (6) means and source of payment for services. 18 U.S.C. § 2703(c)(2). While the name and address of an account holder may often be false, the account holder's IP address and payment records frequently provide useful investigative leads.

193. AT&T: Israel, 79; Comcast: Lutner, 49-50; ICC: Halpert, 29; Microsoft: Goodman, 78-79.

194. ICC: Halpert, 29; NetCreations: Mayor, 24; UOL: Popek, 64.

195. Aristotle: Bowles, 75; Aristotle: Shivers, 74; UOL: Skopp, 78.

196. Sorkin, 28-29; *see also* Microsoft: Goodman, 78-79.

agencies and departments, will conduct a two-day Authentication Summit this Fall.[197] The Commission will invite technologists from ISPs, businesses and individuals that operate their own mail servers, and computer scientists to participate in the Authentication Summit,[198] and encourage participants to begin wide-scale testing and deployment of authentication standards, if this has not already occurred.[199]

B. Convene a Federal Advisory Committee

If, after allowing the private market sufficient time to develop, test, and widely implement market-based authentication standards, no single standard emerges, the Commission could begin the process of convening a Federal Advisory Committee to help it determine an appropriate email authentication system that could be federally required.[200] The system might consist of a Registry of authenticated senders or mandate the use of a particular private-market developed authentication standard. The Commission's decision to convene such a committee would not be made lightly. The Commission is well aware of the risks inherent in regulating technology and in changing the largely hands-off role of the government *vis-a-vis* the Internet.

C. Mandate an Authentication System

If a market-based authentication standard has not yet been widely implemented, six months following the selection of its members, the Federal Advisory Committee could be required to recommend an authentication protocol. An effective mandatory authentication protocol would require legislation to enable the Commission to enforce authentication standards violations against entities outside of its jurisdiction. Regulations to implement the scheme would be proposed soon thereafter.

D. Determine Whether an Authentication System Substantially Reduces Spam and Issue an ANPR Proposing a Registry, if Necessary

After implementation and a reasonable period of time following the effective date of a mandatory authentication standard, the Commission will consider studying whether an authentication system, (whether

197. While we are still investigating the details of and logistics for the Summit, we may be able to hold it as early as September 2004.

198. The Summit would aim to identify potential flaws in the authentication proposals and possible remedies for these flaws. For instance, given the large amount of spam sent through zombie drones, an effective domain-level authentication system would have to address this problem. Ideally, spam sent through zombie drones would not be treated as authenticated email. The Summit would present a forum, not only for identifying such issues, but for aiding the development of solutions.

199. The Commission will also monitor the IETF's efforts in this area since the IETF has developed a working group to study and develop an authentication standard. The working group plans to propose an authentication standard in the Summer of 2004. http://www.nwfusion.com/news/2004/0412marid.html.

200. Through the Summit, the Commission will explore the technological challenges of the various authentication proposals, the ability of small ISPs and business domain owners to participate in the authentication systems, the costs associated with the various proposals, and other issues that impact the time frame for wide-scale adoption of authentication systems. This information will guide the Commission's determination of the appropriate time for convening the Federal Advisory Committee.

market-developed or governmentally-imposed) combined with enforcement or other mechanisms (e.g., better filters) had substantially reduced the burden of spam.[201] If spam continued to be a substantial problem, if a Registry could significantly reduce it once an authentication system is in place, and if other technological developments removed the security and privacy risks associated with a Registry, the Commission will consider issuing an ANPR proposing the creation of a National Do Not Email Registry.

A Registry, if any, maintained by the government would also have to comply with certain procedural and legal requirements before it could be implemented. For example, to the extent the Registry database would compile and create records retrieved by email address or other personal identifier, the Privacy Act of 1974 would require an advance period of public comment and notice to Congress, in addition to other compliance costs and requirements after the system is established. Separately, the E-GOV Act of 2002 requires a privacy impact assessment and certain other security assessments and certifications under Title III of that Act before initiating any online collection of personally identifiable information that could be used to contact an individual. Federal procurement law and regulation would also likely impose competition, clearance, and other requirements before the agency could select a vendor to operate the system. To the extent the Registry, like the Do Not Call Registry, were to be funded by fees, the FTC would need to seek and obtain specific legislative authorization from Congress and conduct public proceedings to establish an appropriate schedule of fees before the system could start operating. In any event, the Commission would need substantial funds to implement and enforce a National Do Not Email Registry.

VI. Conclusion

For the foregoing reasons, the Commission concludes that, under present conditions, a National Do Not Email Registry in any form would not have any beneficial impact on the spam problem. It is clear, based on spammers' abilities to exploit the structure of the email system, that the development of a practical and effective means of authentication is a necessary tool to fight spam. Therefore, the Commission encourages the private market to develop an authentication standard. Authentication is not only required to make a Registry effective, but may even substantially address the underlying problem that prompted Congress to consider the establishment of a Registry.

201. Information obtained by the Commission through the Authentication Summit and Federal Advisory Committee process will impact the time frame for conducting this study.

Appendix 1: Request for Information

Federal Trade Commission's Plan for Establishing a National Do Not E-mail Registry

The Federal Trade Commission ("FTC") is seeking information that may assist in the creation of a plan and timetable for establishing a National Do Not E-mail Registry, as required by the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, Pub. L. No. 108-187 (Dec. 16, 2003) (the "CAN-SPAM Act"). The FTC is also soliciting information to determine the availability of capable contractors that can develop, deploy, and operate such a registry. This is a Request for Information ("RFI") only. It is issued solely for information and planning purposes. It does not constitute a Request for Proposals ("RFP") or a promise to issue an RFP in the future. This RFI does not commit the government to contract for any supply or service whatsoever. The FTC reserves the right to accept, reject, or use without obligation or compensation any information submitted in response to this RFI. The U.S. Government will not pay for any information or administrative cost incurred in response to this RFI.

Part I. Background

Section 9 of the CAN-SPAM Act requires the FTC to transmit to Congress, no later than June 16, 2004, a report that: (1) sets forth a plan and timetable for establishing a National Do Not E-mail Registry; (2) includes an explanation of any practical, technical, security, privacy, enforcement, or other concerns that the Commission has regarding such a registry; and (3) includes an explanation of how the registry would be applied with respect to children with e-mail accounts. Section 9 of the CAN-SPAM Act also authorizes the Commission to establish and implement the plan, but not earlier than September 16, 2004.

Part II. Basic Technical Features of a Registry

The Commission recognizes that a National Do Not E-mail Registry could take one of many possible forms and actively encourages responders to this RFI to propose registry models similar to or different than those described, below. **The model registry you propose may consist of a national registry of consumer (and business) e-mail addresses, a domain-wide registry, a registry of authenticated senders, a combination of these registries, or an entirely different form of registry.** The precise required technical features of a registry will depend upon the types of data collected, the methods of accessing or disseminating the data, and the methods of transforming this data into a usable form.

Parts III of this RFI describes the required technical features for any registry model that involves the registration of either consumer (and business) e-mail addresses (similar to the registry model used in the National Do Not Call Registry) or domains (as in a domain-wide registry). Part IV of this RFI describes the required technical features for any registry model that involves e-mail marketers, domain owners (including ISPs), or third party e-mail forwarding services obtaining access to data appearing in a registry of e-mail addresses or domains. Part V of this RFI describes the required technical features for providing consumers (and businesses) who register their e-mail addresses and/or domain owners that register their domains with the ability to lodge complaints with the Commission that can then be used in enforcement proceedings. Part VI of this RFI describes the required technical features for any registry model that involves a registry of authenticated e-mail marketers and the Internet Protocol ("IP") addresses and domains from which they send e-mail.

If your registry model contains other technical features, you should use the relevant technical features described below when framing your response.

Part III. Registration of E-mail Addresses or Domains

Part III of this RFI identifies required technical features for registries that permit consumers (and businesses) and/or domain owners to register with the Commission their desire not to receive marketing e-mail.

A. Database of Registered E-mail Addresses

If, under the registry model you propose, consumers (and businesses) or domain owners (including ISPs) would register actual e-mail addresses with the Commission – similar to the registry model used in the National Do Not Call Registry – the model described in your response to this RFI should include the following technical features:

1. a web site that would permit consumers (and possibly businesses) to register their e-mail addresses with the Commission;
2. other methods of registration, such as registration via telephone;
3. mechanism(s) for verifying the association between the e-mail addresses registered and the consumers (and businesses) making the registration to ensure that the consumers (and businesses) making the registration are attempting to register their own e-mail addresses (e.g., use a mechanism in which the consumers (and businesses) making the registration are sent confirmation e-mails to which they must respond);
4. mechanism(s) for enabling parents/guardians to register e-mail addresses of children;
5. mechanism(s) for providing consumers (and businesses) with a form of "confirmation" of registration (e.g., a return e-mail from the system);
6. mechanism(s) for providing consumers (and businesses) with the ability to verify whether their e-mail addresses have been registered;
7. mechanism(s) for providing consumers (and businesses) with the ability to remove their registrations and mechanism(s) for providing consumers (and businesses) with the ability to verify whether their e-mail addresses have been removed from the registry;
8. mechanism(s) for periodically deleting closed or inoperable e-mail addresses in the registry;
9. mechanism(s) for logging and tracking when a consumer (or business) registered an e-mail address or accessed, changed, or deleted a registration;
10. mechanism(s) for limiting registrations to consumers (and businesses) located in the United States;
11. the ability to sort registration data by ISP or domain owner in order to facilitate e-mail marketers' access to a subset of registration data;
12. the capacity to process the registration of at least 300 million e-mail addresses;
13. the ability to collect fees from consumers (and businesses) who register their e-mail addresses with the registry;
14. mechanism(s) for accepting e-mail address registrations directly from domain owners (including ISPs) who have verified the authenticity of their subscribers' registration requests;

B. Domain-Wide Registry

If, under the registry model you propose, domain owners (including ISPs) could register their domains as desiring not to receive marketing e-mail (a "domain-wide registry"), the model described in your response to this RFI should include the following technical features, in addition to those relevant features identified above:

1. mechanism(s) that would permit domain owners (including ISPs) to register their domains with the Commission;
2. mechanism(s) for verifying that a request to register a domain are from a person authorized to make such a registration request;
3. mechanism(s) for providing domain owners with a form of "confirmation" of registration (e.g., a return e-mail from the system);
4. mechanism(s) for providing domain owners with the ability to verify whether their domains have been registered;
5. mechanism(s) for providing domain owners with the ability to remove registrations;
6. mechanism(s) for periodically deleting registrations of closed or inoperable domains in the registry;
7. mechanism(s) for logging and tracking when a domain owner registered a domain and accessed, changed, or deleted a registration;
8. mechanism(s) for limiting registrations to domain owners who provide e-mail addresses for consumers (and businesses) located in the United States;
9. mechanism(s) for consumers (and businesses) with e-mail addresses in a registered domain to register their specific addresses as being open to the receipt of marketing e-mail, and mechanisms for verifying and logging such registrations;
10. the capacity to process the registrations of at least 30 million domain owners;
11. the ability to collect fees from ISPs and domain owners who register their domains.

Part IV. Access to Registry Data

Part IV of this RFI identifies the technical features required for providing e-mail marketers, domain owners, or third-party e-mail forwarding services with access to registered e-mail addresses.

A. Database of Registered E-mail Marketers

If, under the registry model you propose, e-mail marketers would have access to a database of registered e-mail addresses, the model described in your response to this RFI should include the following technical features, in addition to those relevant features identified above:

1. method(s) for registering and verifying the identity, ownership, and physical location of e-mail marketers who seek access to or information derived from the database of registered e-mail addresses or the database of registered domains;
2. mechanism(s) for providing registered e-mail marketers with access to or information derived from the database of registered e-mail addresses or database of registered domains;
3. mechanism(s) for logging and tracking when an e-mail marketer registered accessed, changed, or deleted a registration;

4. method(s) for providing each registered e-mail marketer with a unique mark that can be included in the subject line or header information of each e-mail, and ensuring that this unique mark cannot be forged or otherwise misused;
5. method(s) for e-mail marketers to receive updates of registry data on a regular interval (e.g., monthly);
6. the capacity to register, verify, and provide registry information to 500,000 e-mail marketers;
7. the ability to collect fees from e-mail marketers who register to gain access to or otherwise use registry data;
8. mechanism(s) that prevent registered e-mail marketers from sending unsolicited e-mail to consumers (and businesses) or domains that are registered;
9. mechanism(s) that would assist the Commission with identifying the true name and location of an unregistered sender of marketing e-mail;
10. mechanism(s) that would prevent registrations by e-mail marketers located outside the United States;
11. mechanism(s) such as one-way hashes and cryptographic keys for preventing and identifying the misuse of registry data by e-mail marketers and others;
12. mechanism(s) for tracking and logging each access or use of data by registered e-mail marketers;

B. Database of Registered Internet Service Providers and Domain Owners

If, under the registry model you propose, domain owners (including ISPs) would have access to a database of registered e-mail addresses or registered e-mail marketers, the model described in your response to this RFI should include the following technical features, in addition to those relevant features identified above:

1. method(s) for registering and verifying the identity, ownership, and physical location of ISPs and domain owners who seek access to or information from the database of registered e-mail addresses or the database of registered e-mail marketers;
2. mechanism(s) for providing registered domain owners with access to or information derived from the database of registered e-mail addresses or database of registered e-mail marketers;
3. method(s) for domain owners to receive updates of registry data on a regular interval (e.g., monthly);
4. mechanism(s) that enable ISPs and domain owners to incorporate data from the registry of e-mail addresses and registry of e-mail marketers into their anti-spam filters;
5. mechanism(s) for ISPs and domain owners to distinguish between unsolicited commercial e-mail and other forms of e-mail such as non-commercial messages, marketing messages that a consumer (or business) has previously agreed to receive, and transactional messages (such as airline reservation confirmations and bank statements);
6. the ability to collect fees from ISPs and domain owners who register to gain access to or otherwise use registry data;
7. mechanism(s) such as one-way hashes and cryptographic keys for preventing and identifying the misuse of registry data by ISPs and domain owners;

8. mechanism(s) for tracking and logging each access or use of data by registered ISPs and domain owners;

C. E-mail Address and Marketer Registries with Third-Party Forwarding Service

If, under the registry model you propose, all unsolicited commercial e-mail would be required to be delivered by an e-mail marketer to a third party forwarding service that would compare an e-mail marketer's marketing lists to the e-mail addresses appearing on a National Do Not E-mail Registry, your response to this RFI should include the following technical features, in addition to those relevant features identified above:

1. method(s) for registering and verifying the identity, ownership and physical location of third parties who seek to register with the Commission as unsolicited e-mail forwarding services;
2. method(s) for providing each registered forwarding service with a unique mark that can be included in the subject line or header information of each e-mail, and ensuring that this unique mark cannot be forged or otherwise misused;
3. mechanism(s) for providing registered forwarding services with access to or information derived from the database of registered e-mail addresses;
4. mechanism(s) for ensuring the timely delivery of 8 billion e-mail messages per day by registered forwarding services;
5. the ability to collect fees from registered forwarding services;
6. mechanism(s) that prevent registered forwarding services from sending unsolicited e-mail to consumers (and businesses) who have been registered for a period of time to be determined;
7. mechanism(s) such as one-way hashes and cryptographic keys for preventing and identifying the misuse of registry data by registered forwarding services;
8. mechanism(s) for tracking and logging each access or use of data by registered forwarding services.

Part V. Complaint Submission and Review Functions

If the registry model you propose includes a database of e-mail addresses or domains that e-mail marketers, ISPs, domain owners, or forwarding services would access or otherwise use, your response to this RFI should include the following technical features that enable consumers (and businesses) and/or domain owners to lodge complaints and enable the Commission to access complaint data, in addition to those relevant features identified above:

1. mechanism(s) for consumers (and businesses) or domain owners to lodge complaints online with the Commission concerning violations (including the ability to incorporate a copy of an e-mail message, with its complete header information, that is the subject of the complaint);
2. mechanism(s) that ensure that complaints are ripe (i.e., complaints are from consumers (and businesses) who receive e-mail from marketers that had sufficient time to update and remove the complainants' e-mail addresses or domains from their marketing lists;
3. mechanism(s) that ensure that a complaint does not fall within a possible exception to a registry requirement (such as an e-mail from a sender with whom the recipient has an established business relationship, a transactional commercial message, or non-commercial message);

4. mechanism(s) for the Commission to access complaints and complaint data, including the ability to sort complaints substantively (e.g., by subject matter), by sender, by header information, and by ISP or domain owner;
5. mechanism(s) that enable a database of complaints to interface with existing FTC databases.

Part VI. Registry of Authenticated E-mail Marketers

If the registry model you propose consists of or includes as a feature a registry of authenticated senders, your response to this RFI should include the following technical features, in addition to those relevant features identified above. One possible model for a registry of authenticated senders would require a sender of bulk commercial e-mail to obtain a registration number from the Commission, include this registration number in the header information of all marketing e-mail, and register with the Commission the IP addresses and domain names from which it would be sending marketing e-mail. Additional mechanisms would prevent the forgery of registry data, IP addresses, and domain names. Domain owners (including ISPs) would be provided with access to registry information and could adjust their anti-spam filters to reject any marketing e-mail that did not include matching registration numbers, IP addresses, and domain names.

1. method(s) for registering and verifying the identity, ownership and physical location of e-mail marketers, and the creation and maintenance of such a registry of e-mail marketers;
2. method(s) for registering the IP addresses and domains used by registered e-mail marketers;
3. the creation and maintenance of a registry of e-mail marketers, their registration, numbers, verifying information, IP addresses, and domain names;
4. mechanism(s) for ISPs and domain owners to obtain access to e-mail marketers' registry numbers, IP addresses, and domain names;
5. mechanism(s) that enable ISPs and domain owners to incorporate registration number, IP address, and domain name data into their anti-spam filters;
6. the ability to collect fees from registered e-mail marketers and registered ISPs and domain owners;
7. mechanism(s) for preventing the forgery of senders' registration numbers, IP addresses, and domain names;
8. mechanism(s) such as one-way hashes and cryptographic keys for preventing and identifying the misuse of registry data by e-mail marketers, ISPs, domain owners and others;
9. mechanism(s) for tracking and logging each access or use of data by registered e-mail marketers, ISPs, and domain owners.

Part VII. Information Requested

In responding to this RFI, the FTC asks potentially interested parties to submit information on the following subjects. A response to this RFI should be a maximum of 25 pages. Please number your answers to match the question numbers below.

1. Describe the National Do Not E-mail Registry you envision. If your registry model includes a registry of e-mail addresses or domains, explain how your registry would contain the technical features described in Part III of this RFI. If your registry model provides for e-mail marketers, domain owners, e-mail forwarding services, or others to have access to or otherwise use a database of registered e-mail addresses or domains, explain how your registry would contain the technical features described in Part IV of this RFI. If your registry model includes a registry of e-mail addresses or domains, explain how your registry would contain the technical features for accepting and processing complaints of registry violations described in Part V of this RFI. If your registry model includes or consists of a registry of authenticated senders of bulk commercial e-mail, explain how your registry would contain the technical features describe in Part VI of this RFI.

   If your registry model includes the registration of something other than the items described in Parts III, IV, V, and VI of this RFI, include a description of the sources and types of data that the Commission would collect, how and by whom the data would be used, and the methods of verifying the authenticity of entities having access to the data.

2. Describe the technical architecture of your proposed system. Include a description of: (a) the methods used to handle the potential volume of consumer requests to register, and the security measures, including the tracking and accounting of disclosures, you would use to protect the registry information; (b) the methods used to handle the potential volume of e-mail marketer registrations and their need for up-to-date registry information; and (c) the methods used to handle the potential volume of ISP registrations and their need for up-to-date registry information;
3. Provide estimates of the cost of your proposed system, in total and/or per transaction. Indicate the amount of those costs necessary to build or develop the system, including any privacy or other required risk assessments, and the amount necessary to operate it for a five year period. Do any of these cost estimates change based on the volume of transactions that occur? If your system involves the registration of consumer (and business) e-mail addresses, your cost estimate should assume the registration of 300 million e-mail addresses. State the additional costs if there are 450 e-mail addresses registered. If your system involves the registration of domains, your cost estimate should assume the registration of 30 million domains. Finally, provide an estimate of the time necessary for you to implement your proposed system;
4. If your proposed registry model would result in e-mail marketers, e-mail forwarding services, or ISPs learning the specific addresses on the registry, describe security precautions that would: (a) prevent misuse of the registry; (b) enable the Commission to identify persons who misuse the registry; and (c) ensure that e-mail marketers, e-mail forwarding services, ISPs, and domain owners who obtained registry data maintain the data in a secure fashion;
5. Describe how your system would prevent an unregistered e-mail marketer from sending unsolicited commercial e-mail to an e-mail address appearing on the registry and how it would assist the Commission with identifying the true name and location of such an unregistered sender;
6. Describe how the true name and location of an e-mail marketer, e-mail forwarding service, ISP, or domain owner who submitted false information to the Commission when registering as a user of the registry would be identified by the Commission prior to gaining access to the registry;

7. Describe how your system would facilitate identifying misuse of the registry by e-mail marketers, e-mail forwarding services, ISPs, or domain owners that are registered users of the registry;
8. Describe the size of the registry database envisioned by your model and the costs in terms of bandwidth and computational time that your model would impose on e-mail marketers, e-mail forwarding services, ISPs, and domain owners;
9. Describe the technical sophistication (e.g., software and hardware) needed by e-mail marketers, ISPs, domain owners, and consumers under your registry model;
10. Describe how your registry model would ensure the delivery of transactional e-mails, other forms of solicited or permission-based commercial e-mail messages, and personal e-mail messages;
11. Describe how your registry model would ensure the privacy rights of consumers;
12. Describe how your registry model would enable parents/guardians to register the addresses of children;
13. Describe your expectations concerning the rights you would maintain in any part of the proposed system you would develop. The FTC expects that the data collected in the registry would be the government's property and cannot be used for any non-governmental purpose other than ensuring compliance with a National Do Not E-mail Registry. Any registry system would also be expected to comply with the requirements and standards of the Federal Records Act, Rehabilitation Act (e.g., section 508), the Privacy Act, the E-Government Act of 2002, and any other applicable statutes, regulations, or orders;
14. Describe the specific billing and collection mechanisms you would use if fees are charged to access the registry;
15. Provide any additional technical information that will assist in understanding your response to this RFI;
16. Briefly describe your company, products, services, history, ownership and any other information you deem relevant. In particular, describe any projects you have been involved in that are similar in concept to what is described in this RFI, including management and operations approach, security requirements, including policies and practices for personnel background checks or clearances, and any relevant lessons learned;
17. Describe any necessary additions or modifications to rules, standards, or protocols (e.g., FTC rulemaking, E-mail protocol changes (RFC for Sendmail), changes in standards set by ICANN) that would enhance the effectiveness, enforcement, or security of your proposed registry format.
19. Include any suggestions on acquisition strategies that the FTC should use for this project, e.g., performance based statement of work, turn-key approach, two-stepped sealed bidding, etc.;
20. Include any comments on the structure of the requirements for formal Request for Proposals ("RFP") responses and suggestions for the evaluation of such formal responses;
21. Include the relevant information if your services are available on a GSA schedule or other contract vehicle. Identify Special Item Numbers (SIN) under your GSA contract applicable to the services/products required to build the registry.
22. Identify the commercial performance matrix and incentives that should be used.

General Information

Response Date: March 10, 2004

Contracting Office Address:

Federal Trade Commission, Financial Management Office, Acquisitions,
600 Pennsylvania Avenue, NW, Washington, DC 20580

Points of Contact:

Daniel Salsburg
Federal Trade Commission, Division of Marketing Practices
600 Pennsylvania Avenue, NW. Washington, DC 20580
202-326-3402

Five copies of a response to this RFI should be either hand delivered or sent via an overnight courier service to Daniel Salsburg at the above address.

Respondents to the RFI may be contacted for additional information or clarifications concerning their RFI response if the FTC determines it to be necessary.

Appendix 2: List of Interviews

Name	Organization	Date	Transcript?
Ashworth, Bill	Microsoft Corporation	3/10/2004	No
Atkins, Laura	The SpamCon Foundation	2/10/2004	Yes
Atkins, Steve	SamSpade.org	2/10/2004	Yes
Baer, Joshua (“Josh”)	SKYLIST, Inc.	3/9/2004	Yes
Berkower, Elise	Email Service Provider Coalition (ESPC); DoubleClick	1/28/2004	No
Bernard, Ted	Savicom	3/8/2004	Yes
Bowles, Elizabeth	ARISTOTLE.net	3/15/2004	Yes
Boyd, Thomas M.	Email Service Provider Coalition (ESPC); Alston & Bird LLP for the National Business Coalition on Electronic Commerce and Privacy	1/28/2004	No
Brady, Betsy	Microsoft Corporation	3/10/2004	No
Brondmo, Hans Peter	Digital Impact, Inc.	3/9/2004	Yes
Bruening, Paula	Center for Democracy and Technology (CDT)	2/11/2004	Yes
Cade, Marilyn S.	AT&T	3/15/2004	Yes
Castelli, Eric	LashBack LLC	2/17/2004	No
Catlett, Jason	Junkbusters Corp.	2/11/2004	Yes
Cerasale, Jerry	The Direct Marketing Association (DMA)	3/9/2004	Yes
Cohn, Cindy	Electronic Frontier Foundation (EFF)	2/11/2004	Yes
Collingwood, John E.	MBNA America (MBNA)	3/10/2004	Yes
DeGraff, Kenneth	Consumers Union (CU)	3/1/2004	Yes
Delaney, Mark	Yahoo! Inc.	3/25/2004	No
DeLapena, Mike	BigFoot Interactive, Inc.	1/29/2004	No
DiGuido, Al	BigFoot Interactive, Inc.	1/29/2004	No
Dunlap, Leslie	Yahoo! Inc.	3/15/2004	Yes
Edelman, Ben	Harvard Law School	3/3/2004	Yes
Egan, Erin M.	Covington & Burling for Microsoft Corporation	3/15/2004	Yes
Everett-Church, Ray	Coalition Against Unsolicited Commercial Email (CAUCE)	2/10/2004	Yes
Fox, Jean Ann	Consumer Federation of America (CFA)	3/1/2004	Yes
Goodman, Joshua	Microsoft Corporation	3/15/2004	Yes
Grant, Susan	National Consumers League (NCL)	2/26/2004	Yes
Hadley, Tony	Email Service Provider Coalition (ESPC); Experian	1/28/2004	No
Haight, Julian	SpamCop.net, Inc.	3/2/2004	Yes
Halpert, James (“Jim”)	Piper Rudnick for the Internet Commerce Coalition (ICC)	3/8/2004	Yes
Hermanson, Sharon	AARP	2/26/2004	Yes
Hoffman, Adonis	American Association of Advertising Agencies	3/8/2004	Yes
Hoofnagle, Chris Jay	Electronic Privacy Information Center (EPIC)	2/11/2004	Yes
Hughes, J. Trevor	Email Service Provider Coalition (ESPC); Network Advertising Initiative (NAI)	1/28/2004	No
Hughes, J. Trevor	Email Service Provider Coalition (ESPC); Network Advertising Initiative (NAI)	3/9/2004	Yes
Ingis, Stuart (“Stu”)	Piper Rudnick for Time Warner (AOL)	3/15/2004	Yes

Name	Organization	Date	Transcript?
Israel, Susan E.	AT&T	3/15/2004	Yes
Jacobsen, Jennifer	Time Warner Inc. (AOL)	3/15/2004	Yes
Jalli, Quinn	Email Service Provider Coalition (ESPC); Digital Impact, Inc.	1/28/2004	No
Jalli, Quinn	Email Service Provider Coalition (ESPC); Digital Impact, Inc.	2/3/2004	No
Judge, Paul Q.	CipherTrust	2/23/2004	Yes
Kramer, David H.	Wilson, Sonsini, Goodrich, and Rosati	2/23/2004	Yes
Laurant, Cédric	Electronic Privacy Information Center (EPIC)	2/11/2004	Yes
Levine, John R.	Internet Research Task Force, Anti-Spam Research Group (ASRG)	2/26/2004	Yes
Lewis, Chris	Nortel Networks Limited	2/23/2004	Yes
Lewis Jr., Gerard J.	Comcast	3/15/2004	Yes
Libbey, Miles	Yahoo! Inc.	3/25/2004	No
Lutner, Sean	Comcast	3/15/2004	Yes
Maier, Fran	TRUSTe	1/14/2004	No
Mansourkia, Maggie	MCI, Inc.	3/15/2004	Yes
Marshall, Beth T.	MBNA America (MBNA)	3/10/2004	Yes
Mayor, Michael	NetCreations, Inc.	3/8/2004	Yes
McEldowney, Ken	Consumer Action	3/1/2004	Yes
McGilvray, Lana	SKYLIST, Inc.- UnSubCentral	3/9/2004	Yes
McGuire, Russell E. (“Rusty”)	Office of the Attorney General, VA (VAOAG)	3/10/2004	Yes
McLaughlin, Andrew	Google	2/23/2004	Yes
Mesnik, Peter R.	IMN Inc.	3/9/2004	Yes
Mohr, Jeffrey A.	LashBack LLC	2/17/2004	No
Olson, Margaret	Roving Software Inc. d/b/a Constant Contact	3/9/2004	Yes
Park, William	Digital Impact, Inc.	2/3/2004	No
Phillips, Brandon	LashBack LLC	2/17/2004	No
Plesser, Ron	Piper Rudnick for The Direct Marketing Association (DMA)	3/9/2004	Yes
Popek, Gerald	United Online, Inc.	3/15/2004	Yes
Praed, Jon L.	Internet Law Group	2/23/2004	Yes
Randall, Frederick	United Online, Inc.	3/15/2004	Yes
Rector, Clark	American Advertising Federation (AAF)	3/8/2004	Yes
Reed, Jo	AARP	2/26/2004	Yes
Richards, Scott	MBNA America (MBNA)	3/10/2004	Yes
Richards, Rebecca	TRUSTe	1/14/2004	No
Richter, Steve	Email Marketing Association (eMMa)	3/10/2004	Yes
Robinson, Matt	Yahoo! Inc.	3/25/2004	No
Rubin, Joe	U.S. Chamber of Commerce	3/9/2004	Yes
Selis, Paula	Office of the Attorney General, WA (WAOAG)	3/10/2004	Yes
Shafranovich, Yakov	Internet Research Task Force, Anti-Spam Research Group (ASRG)	2/26/2004	Yes
Shivers, Carl	ARISTOTLE.net	3/15/2004	Yes
Silverman, Scott	Shop.org	3/10/2004	Yes
Skopp, Peter	United Online, Inc.	3/15/2004	Yes
Sorkin, David E.	John Marshall Law School	3/3/2004	Yes
Squire, Brooke	United Online, Inc.	3/15/2004	Yes

Name	Organization	Date	Transcript?
Torrie, Beth	BigFoot Interactive, Inc.	1/29/2004	No
Treanor, Elizabeth	National Retail Federation	3/10/2004	Yes
Tuck, Russ	Google	2/23/2004	Yes
Uncapher, Mark	Information Technology Association of America (ITAA)	3/9/2004	Yes
Webb, George	Microsoft Corporation	3/10/2004	No


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