Part III of the

National Do Not Email Registry

A Report to Congress, June 2004

"The Email System and the Resulting Spam Problem"
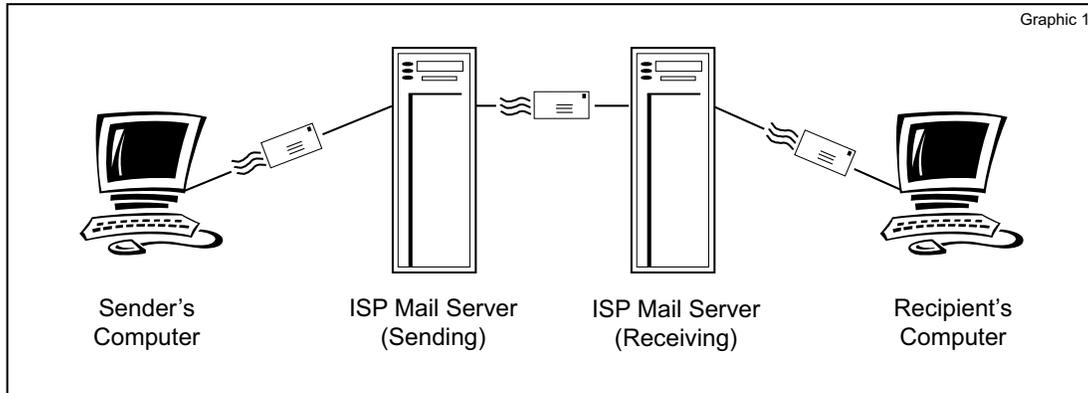
Federal Trade Commission

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

Federal Trade Commission

III. The Email System and the Resulting Spam Problem

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

.

Graphic 1

| Sender's Computer | ISP Mail Server (Sending) | ISP Mail Server (Receiving) | Recipient's Computer |

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."
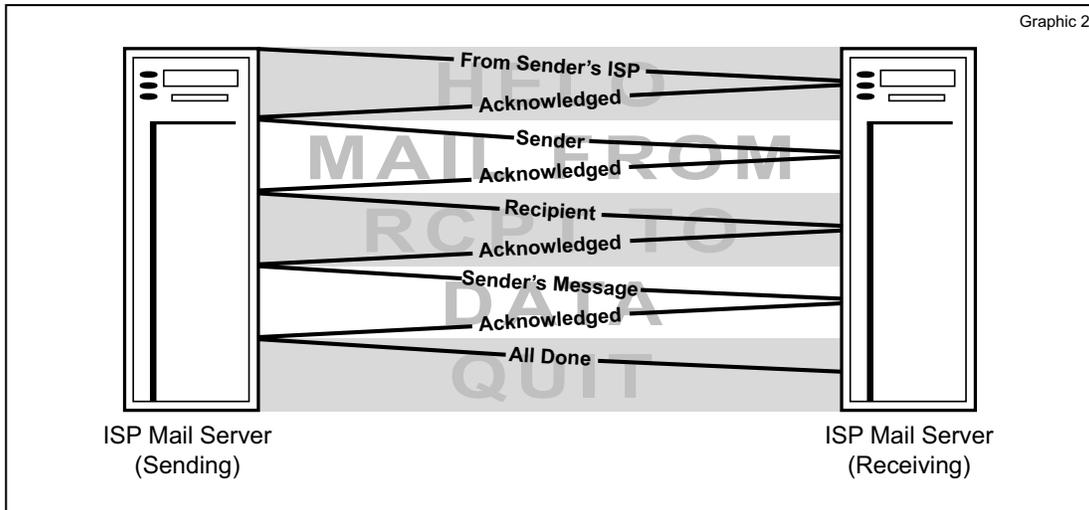
1. The five-part dialogue

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

ISP Mail Server
(Sending)

From Sender's ISP
Acknowledged
Sender
Acknowledged
Recipient
Acknowledged
Sender's Message
Acknowledged
All Done

ISP Mail Server
(Receiving)

(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?contentIte mId=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/43bb6130e5e86e5fc12569fa005d00 4c/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]

---

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.*

---

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

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.