Junk email—yes, it's annoying, but it can also be overwhelming. A new study evaluates the current extent of the spamming problem and suggests there are no quick fixes to solve the situation.

Spam!

Lorrie Faith Cranor and Brian A. LaMacchia

Concern about the proliferation of unsolicited bulk email, commonly referred to as "spam," has been steadily increasing. When received in small quantities, spam may annoy recipients, but rarely poses a significant problem. However, some recipients of large quantities of spam find themselves so overwhelmed with unwanted email that it is time-consuming or difficult for them to ferret out their desired correspondence. Furthermore, unlike most junk postal mail, junk email frequently contains explicit sexual language and attached photographs that many recipients find offensive. With the advent of HTML-enabled email clients, some bulk emailers now send lengthy HTML-formatted email, complete with images and links to Java applets that may execute automatically when the email is read using some clients.

As spam recipients become increasingly annoyed, ISPs have been deluged with complaints. Furthermore, some ISPs report that spam places a considerable burden on their systems.

A variety of technical countermeasures to spam have been proposed: the simplest are already being implemented; some of the more extreme could require dramatic changes to the ways we communicate electronically. In addition, there has been growing support in the U.S. for laws that would restrict the sending of spam.

Prior to the commercialization of the Internet in the mid-1990s, the spam problem was quite limited. Unsolicited mail consisted mostly of messages from pranksters, chain letters, and inappropriate messages sent to established email lists by individuals who were either unaware their message would go to the entire list or unaware their messages were inappropriate for that forum. However, unsolicited *commercial* email messages were quite rare. Nonetheless, unwanted email messages were recognized as a problem in an Internet Request For Comments as early as 1975 [8] and in the pages of *Communications* as early as 1982 [2].

ILLUSTRATIONS BY BEATA SZPURA

After large-scale commercial spam made its public debut on Usenet in the infamous Canter and Siegel "green card lawyers" incident of 1994 [1], the proliferation of unsolicited commercial email began to pick up speed. By the spring of 1996 spam made up a significant portion of the email received by customers of the major Internet service providers, and some providers began to take action. In June 1997, the U.S. Federal Trade Commission held hearings on spam that resulted in the launching of a "Scamspam" effort to go after the senders of fraudulent spam and in the creation of an ad-hoc working group to address the issue [4].

According to Jill Lesser, a lawyer for America On-Line, at times as much of 50% of the email coming into the AOL system was spam before technical countermeasures were actively pursued. At the FTC spam hearings Lesser reported that during the spring and early summer of 1997, spam rates on most days hovered near 30%.

Our study (see the Case Study sidebar) suggests the volume of spam received by AOL may not be indicative of the overall extent of the problem. Possibly due to the ease with which bulk emailers can harvest the addresses of AOL subscribers (a practice that is against AOL's policies), AOL appears to receive an unusually large volume of spam. By comparison, during July 1997 our study found spam rates around 10% for a corporate network (selected AT&T and Lucent subdomains used by employees of those companies) and spam rates under 2% for a large pure ISP (that is, a service provider that offers only Internet access, not online services).

While AOL's spam rates may not be typical, our study indicates the spam problem has been increasing rapidly and it may only be a matter of time before all ISPs experience similar rates. It remains to be seen whether technical countermeasures can curb the increasing spam rate over the long term.

In addition to technical countermeasures, some ISPs have sought legal relief. Early cases centered on attempts by ISPs to block or limit spam generated by Cyber Promotions, perhaps the largest generator of spam on the Internet. In *Cyber Promotions, Inc. v. America Online, Inc.*,[1] Cyber Promotions was found not to have a First Amendment right to send spam to AOL subscribers and thus AOL could attempt to block such messages via technical means. Cyber Promotions and Compuserve entered into a consent decree limiting the methods by which the former could communicate with the latter's subscribers.[2] (Cyber Promotions entered into similar agreements with Prodigy[3] and Concentric Networks.[4]) More recently, because generators of spam often use false return addresses containing the trademarked names of other businesses, several ISPs have sought injunctions preventing the use of their electronic addresses within spam generated by others.[5]

Contributing Factors

Before discussing possible solutions to the spam problem, it is instructive to examine the major factors that contribute to the problem: the low price of bulk email, and cheap pseudonyms.

Bulk email is inexpensive to send. Some bulk email services will send 100,000 email messages for under $200, and do-it-yourselfers can

[1] 948 F. Supp. 436 (E.D. Pa. Nov. 4, 1996).
[2] *CompuServe Inc. v. Cyber Promotions, Inc.*, No. C2-96-1070 (S.D. Ohio) (final consent order filed in E.D. Pa. May 9, 1997).
[3] *Prodigy Services Corp. v. Cyber Promotions*, Inc., (S.D.N.Y. filed Oct. 18, 1996.)
[4] *Concentric Network Corp. v. Wallace*, No. C-96 20829-RMW(EAI) (N.D. Cal. Nov. 5, 1996).
[5] See for example *Parker v. C.N. Enterprises*, No. 97-06273, (Tex. Travis County Dist. Ct., 1997), *Strong Capital Management, Inc. v. Smith*, No. 97-C-0371 (E.D. Wis., 1997), *Typhoon, Inc. v. Kentech Enterprises* (S.D. Cal., 1997), *Web Systems Corp. v. Cyber Promotions, Inc.* (Tex. Harris County Dist. Ct., 1997).

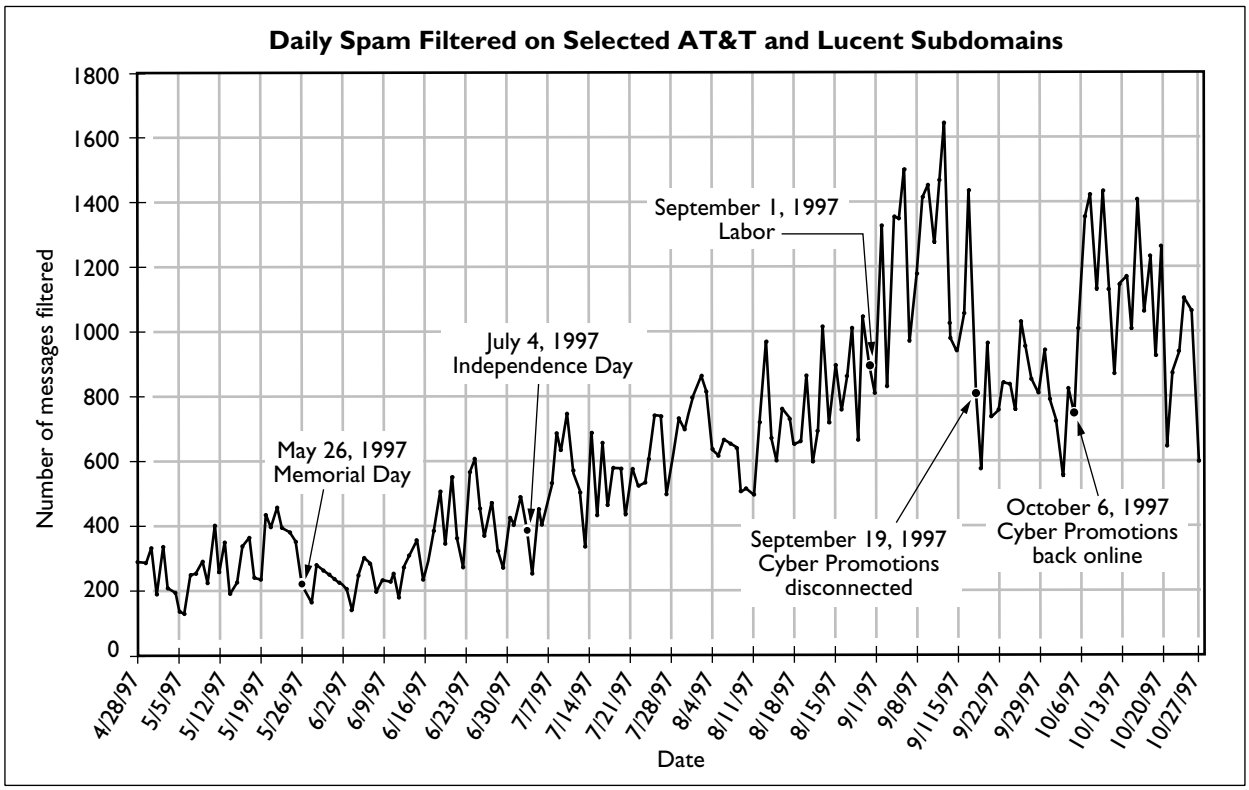
buy a million email addresses for under $100. A plain vanilla personal computer, dial-up Internet account, and free email client software will do for the amateur bulk mailer. But serious bulk mailers invest a few hundred dollars in specialized software capable of sending 250,000 messages with forged headers per hour and harvesting email addresses from Usenet, the Web, and online services. After making the initial investment in a personal computer and software, a bulk mailer can send out hundreds of thousands of messages a day with minimal work and monthly service fees. With such low expenses, bulk mailers can recoup their costs even if only a tiny fraction of the messages they send out result in sales.

A CASE STUDY

In order to better understand the extent of the spam problem, we analyzed mailer logs for selected AT&T and Lucent subdomains for a six-month period beginning at the end of April 1997. These domains receive about 70,000 email messages from the Internet during a typical week. We also studied the spam problem for an ISP during a two-week period in July 1997 in which the service processed over 13 million email messages from the Internet.

During the study period, email administrators at AT&T and Lucent used a variety of automated and semi-automated filtering mechanisms to identify and block spam messages intended for their employees. The filters were updated on a regular basis (often daily), a process that generally consumed between 4 and 20 hours of administrator time each week. We compiled statistics on the number of messages blocked each day for all the subdomains under study. For one subdomain we compiled the number of addresses for which spam was blocked each day, and the number of messages blocked for each address. Using information reported by employees who voluntarily saved all the spam messages they received, we monitored the accuracy of the spam filters. We estimate that the filters blocked at least half the spam messages received during the entire study period. During the last half of the study period, we estimate the filters blocked between 60% and 80% of the spam messages.

At the beginning of the study period at the end of April, we blocked 2.5% of the messages received from the Internet on the subdomains under study. Thus, we estimate that spam comprised no more than 5% of the total messages received from the Internet at that time. This percentage had doubled by the end of June. At



However, it is important to remember that while the cost of sending bulk mail is low, the cost of receiving it may not be. The cost of receiving a single piece of bulk mail is minimal, but the cost of receiving many pieces can be considerable. Even if individuals are not paying per-message or per-minute fees, spam may be expensive in terms of time. Individuals may waste minutes or hours transferring unwanted messages from their ISPs to their computers and sorting through those messages once transferred. Furthermore, unwanted messages place a burden on ISPs, requiring them to spend time and money implementing filters, responding to subscriber complaints, and increasing their email system

its peak, we estimate the weekly spam percentage exceeded 15%. The percentage of spam received dipped significantly at the end of September through the beginning of October during the period when Cyber Promotions lost its Internet connectivity. The spam rate began increasing again after the first week of October. The number of messages blocked each day during the study period are shown in the figure.

Because the majority of email received in a business setting is received during the work week rather than on weekends, the spam percentage on weekends was consistently significantly higher than the spam percentage on weekdays. The actual number of spam messages received each day on weekends was generally about the same as the number of spam messages received each day during the work week. While we observed that fewer email messages were received on U.S. national holidays, we did not observe a decrease in the number of spam messages received on those days.

In addition to increases in the total number of spam messages, the number of addresses that received spam messages also increased substantially during the study period. At the end of April, approximately 14% of the addresses receiving mail during a given week received some spam mail. This percentage increased to over 31% by the week of October 20. Furthermore, while no single address received more than an estimated 20 spam messages each week at the end of April, just prior to the Cyber Promotions outage some addresses were receiving an estimated 80 spam messages each week.

In order to gain some insight into why some people were receiving an ever increasing quantity of spam while others were receiving none, we examined the 55 addresses that received the most spam during the first half of our study and compared them with 55 addresses randomly selected from those that received at least 50 email messages during that period. We looked up the high spam and random address in two online Web indexes—AltaVista and HotBot—and in Deja News, an index of Usenet news. We recorded the number of hits returned for each address. The random address had an average of 3 hits in AltaVista, 6 hits in HotBot, and 7 hits in Deja News, while the high spam addresses had an average of 13 hits in AltaVista, 30 hits in HotBot, and 99 hits in Deja News. Furthermore, the high spam addresses were 1.5 times more likely than the random addresses to have any hits in either of the Web indexes, and 3.2 times more likely to have any hits in Deja News. The high spam addresses were 4.6 times more likely than the random addresses to have hits in all three indexes.

This data suggests that people who have indexed Web pages or post frequently to Usenet are more likely to receive spam than those who do not. Although we have not demonstrated a causal relationship with this data, the existence of automated tools to harvest email addresses from the Web and Usenet suggests that having an indexed Web page or posting frequently may actually cause one to receive spam, rather than simply being a characteristic of those who receive spam. However, Web page owners and frequent posters may also be likely to engage in other online activities that may trigger spam. Also, it is not clear whether having an indexed Web page is really a major contributing factor for receiving spam, or whether having an indexed Web page is simply a characteristic of many people who post frequently to Usenet.

While it was not possible to track down the creation date for all the addresses in the subdomains under study, the addresses in one subdomain were known to be mostly obsolete, and the addresses in another were known to have been created within the past two years. The highest levels of spam were generally received on the oldest subdomain, while the lowest levels of spam were generally received on the newest subdomain. Several employees who have multiple email addresses reported to us that they tended to receive more spam at their older addresses.

Preliminary analysis of data collected after the end of our six-month study period indicates the performance of our filters has degraded considerably over the past few months, apparently due to spammers' changing tactics (and little effort on our part to keep up). In addition, the amount of spam we receive each day appears to be leveling off.

—Lorrie Faith Cranor, Bob Flandrena, Danielle Gallo, Brian A. LaMacchia, and Tom Scola

capacity more frequently than would otherwise be necessary. In addition many ISPs are burdened by spam not destined for their own subscribers, but relayed through their system by spammers who are attempting to hide the true origin of their messages. One ISP estimated that before installing anti-relay technology in March 1997, 15% of their total mail traffic was relayed spam.

Pseudonyms are inexpensive to obtain. The most straightforward techniques for filtering unwanted email involve filtering messages based on the name or address of the sender. But it is inexpensive for senders to obtain new valid or forged email addresses, phone numbers, post office boxes, or other identifiers that serve as pseudonyms in cyberspace. As long as their business does not rely on building a positive reputation over time, it costs bulk mailers little to repeatedly change pseudonyms, thus thwarting many filtering efforts.

Technical Solutions

Here, we focus on the technical and regulatory solutions that are currently available or proposed to solve the spam problem. Legal countermeasures have also been used with mixed results. When the spam generator has a significant business presence it may be possible (at the cost of hiring counsel and filing a lawsuit) for recipient ISPs to pursue restraining orders and injunctions. These costs can be prohibitive, though, for individual spam recipients. Furthermore, the advent of do-it-yourself spam kits has encouraged many small-time bulk emailers who are more difficult to pursue in court. Most of these small-timers contribute very little to the problem individually, but together they can churn out huge quantities of spam. Identifying these senders and suing each one individually is not likely to be practical.

Filtering solutions. Automated and semiautomated filtering solutions are widely used by ISPs, corporate email administrators, and individuals. Completely automated solutions bounce or delete all suspected spam, while semi-automated solutions put suspected spam aside for a human to examine. The most straightforward filtering solutions involve filtering messages from known spam senders based on information in message headers. In addition, pattern matchers can sometimes identify spam based on information within the body of an email message. Our experience with the use of pattern matchers on the subdomains we studied suggests it is still difficult to use them with 100% accuracy. While an automated filter that misses a small percentage of spam may be acceptable to most people, fewer people are likely to accept an automated filter that incorrectly identifies a small percentage of desired mail as spam. In addition, the presence of thousands of identical copies of a single message can be an indication of spam. However, there are some legitimate messages sent to thousands of people (for example, many frequent travelers sign up to receive email notification of airfare sales), so automatic filtering based on the number of recipients also requires some manual supervision. Updating filters and supervising a semi-automated filter can be a time-consuming endeavor for an email administrator and too complicated for unsophisticated end users.

Serious bulk mailers invest a few hundred dollars in specialized software capable of sending 250,000 messages with forged headers per hour and harvesting email addresses from Usenet, the Web, and online services.

The manual effort required to facilitate filtering solutions can be reduced by taking advantage of economies of scale. Once one copy of an unsolicited commercial message is identified, setting filters to detect additional copies is easier. Collaborative filtering techniques and systems for easily sharing filtering lists can reduce the effort required by any one individual. Furthermore, semi-automated filtering techniques in which filters are run by administrators but the review of suspected spam is done by each recipient, may require less manual effort by an administrator without substantially increasing the burden on the recipient. However, some semi-automated solutions may pose problems for individuals who download all of their email using a modem as they still have to wait for the unwanted mail to download. This problem is reduced by email systems that allow clients to preview email headers.

Some ISPs have experimented with filters that reject all messages from nonregistered domains. When a message is received for delivery to an account on the ISP the mail agent tries to resolve the SMTP envelope address in the inbound message. If the domain name contained within the address does not have a valid record in the domain name service the message is silently rejected. Such filtering can

weed out messages with deliberately faked addresses but it may also drop legitimate messages from misconfigured mail servers. Alternatively, SMTP mail agents could require authenticated connections for inbound mail; spam messages could then be traced back through the chain of transfer agents.

Some ISPs now perform filtering on outbound messages as well as inbound messages, or place daily limits on the number of outbound messages each subscriber can send, in an attempt to prevent their subscribers from contributing to the spam problem.

If bulk emailers do not significantly change their techniques, filtering solutions will probably become increasingly more successful and less time-consuming to administer. However, while some bulk mailers continue to use primitive techniques, many are purchasing increasingly sophisticated software packages that help them thwart filters. Bulk emailers can increase the difficulty of detecting their messages by sending out a bulk solicitation in which the message sent to each recipient has been customized or otherwise modified so that the messages are not identical. Furthermore, sophisticated bulk mailers might try other tactics—such as encrypting each message with the recipient's public key—that might prove difficult to filter by anyone except the recipient. It remains to be seen which side will ultimately prevail in this arms race.

Counterattack solutions. Some people have responded to spam by bombarding the sender or the sender's ISP with complaints or false inquiries about the advertised product. Such tactics can be automated, and can sometimes pose an inconvenience for the spam sender. Many ISPs will revoke the accounts of those who are the subject of spam complaints. However, as it is often difficult to determine the true sender of spam messages, technical counterattacks sometimes go nowhere (often leaving a substantial trail of bounced message notices) or land in the mail boxes of innocent victims whose email addresses were misappropriated by unscrupulous spam senders. Thus, the effectiveness of such tactics is increasingly limited.

Opt-out lists. Several email opt-out lists were established in 1997. Individuals who do not wish to receive spam can ask to have their email addresses included on these lists. The list maintainers ask bulk emailers to cleanse their lists and remove all addresses that appear on the opt-out lists. However, many people are suspicious of the opt-out lists (in part, due to the fact that some are run by bulk email companies), and there is little evidence that these lists are widely used by bulk emailers to cleanse their lists. Should companies with established brand names begin using spam as a marketing tool, they would be more likely to use opt-out lists than the companies that typically market with spam today.

Channels. The spam problem might be addressed through technologies that sort incoming email according to sender, rejecting email from unknown senders, or placing it in a separate mailbox. Robert Hall, a researcher at AT&T Labs, developed a system of channelized electronic mail in which individuals may assign a different channel to each of their correspondents by giving each correspondent a unique email address at which to contact them [6]. Individuals can establish public channels, for example to use on business cards, when submitting an email address to a Web site, or when posting messages to public forums. Channels may be revoked and all further messages sent to them bounced if they are used for spam. A *personal channel agent* can help generate and keep track of an individual's own channels as well as the addresses needed to contact other channel users that the individual corresponds with. A similar tool is built into the Lucent Personal Web Assistant [7] to help users manage target-revocable email addresses

used when posting to newsgroups or submitting an email address to a Web site.

Individuals who adopt a channelized email system might find themselves receiving significant amounts of spam on public channels but be unwilling to revoke those channels because they are also used for unanticipated, but desired, correspondence. As the amount of spam received on those channels increases, it may not be practical to sort through the various channels to find desired messages. Even so, these individuals would still benefit from having mail from known senders sorted into separate channels.

Payments. A channelized email system might be augmented so that individuals may require payments before they read messages arriving on certain channels. Such a payment might be in the form of electronic cash. Optionally, if a message is from someone the individual

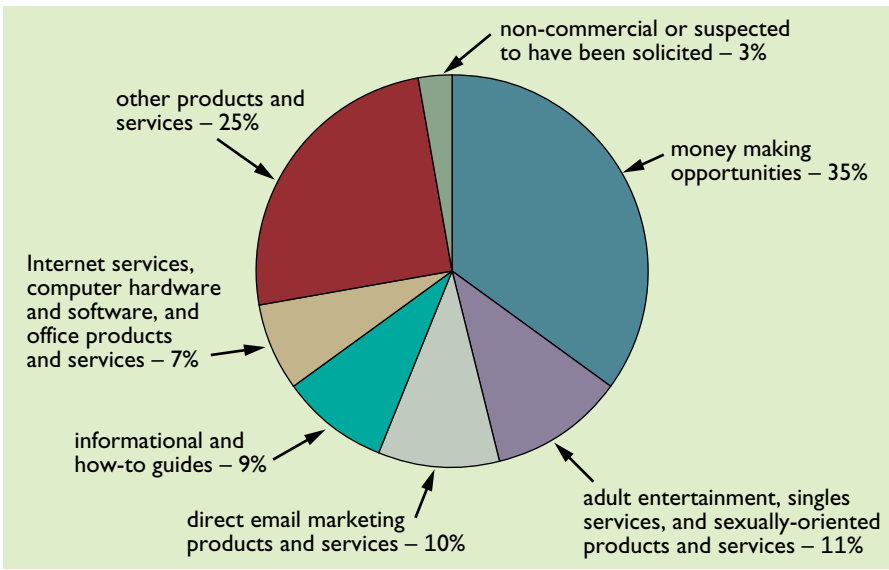
WHAT DOES SPAM ADVERTISE?

As part of our study, we analyzed a collection of 400 unique messages sent to the AT&T and Lucent subdomains under study during March, April, and May 1997 and identified by email administrators as spam. We classified the messages in this collection according to the types of products or services they advertised and recorded several other characteristics of each message. Fifty of the messages were then classified by another rater. The classifications by the two raters agreed 82% of the time.

The figure shows the types of products advertised by the spam we analyzed. Thirty-six percent of the messages in our collection advertised money-making opportunities, including pyramid-style schemes, multilevel marketing systems, and investment opportunities. Eleven percent advertised adult entertainment, singles services, and sexually oriented products and services. Ten percent advertised direct email marketing products and services, including bulk email services, lists of email addresses, and software for harvesting email addresses or sending out bulk mailings. Nine percent advertised informational and how-to guides. Seven percent advertised Internet services and various computer hardware and software products, office supplies and machinery, and related services. Three percent were either non-commercial messages or suspected to have been solicited by the recipient. The remaining messages advertised other products and services, including phone services, vacation packages, nutritional supplements, weight loss products, credit cards, cable descramblers, and online newsletters.

Only 36% of the messages contained instructions for being removed from the mailing list—and reports from email administrators suggest that many of these instructions are likely faulty or deliberately misleading. Perhaps most telling about the nature of these messages was the fact that fewer than 10% identified the name, postal address, phone number, and email address of the sender, as per the Direct Marketing Association guidelines (see www.the-dma.org/home_pages/business-affairs/onlinebd.html). Such identification would be required by Title III of S. 1618.

The low percentage of identified senders and our observations about the types of products and services being offered support the general perception among spam recipients that most spam is not coming from legitimate businesses. Indeed, spam recipients often complain that spam is particularly annoying to them because so much of it advertises adult entertainment and possibly fraudulent schemes.



Types of products and services advertising in analyzed spam samples

wishes to correspond with, such as a long lost friend, the individual might refund the payment. This would make it more costly to send unsolicited email, and it would compensate people for spending time reading this mail. To be practical, however, this system would require the widespread adoption of compatible digital payment systems. Another way to make it costly to send spam would be to require payments of computation. Cynthia Dwork and Moni Naor [3] have proposed a scheme that would require email senders "to compute a moderately hard, but not intractable, function." Such computations could place a significant burden on the computer resources of bulk mailers.

A problem with the payment schemes described here as well as other proposals is they generally require additional or augmented protocols between both the email sender and the recipient and thus create an *incremental adoption* problem. Any given sender-recipient pair can implement these schemes using specialized software, but guaranteed support for any scheme requires a change in Internet mail standards and global adoption by every mail client. Incremental adoption will always leave some users out in the cold; users who do decide to adopt such a systems may discover that many of their correspondents who send them desirable email have not adopted the system and thus cannot easily comply with the payment request. This problem might be reduced in a system that allows senders to cut and paste a computation payment from a Java applet or other such software easily downloaded and installed on the senders' computer.

Recently, Bell Labs researchers proposed a novel twist on email payment schemes in which email senders perform time-consuming computations as part of a handshake necessary to receive an extended email address (similar to a channel address) for someone they wish to correspond with [5]. The handshake is initiated by sending mail to the user's email address without any extensions. Once an extended email address is received, it may be used repeatedly without need for the sender to engage in further computation or use specialized email software. However, should the sender use the extended email address to send unwanted mail, the recipient can configure his or her client software to reject all future messages sent to that address.

Referral networks. Another possible augmentation to a channelized system would be a system of referral networks that would provide an automated way for senders to be introduced or referred to people with whom they have not previously corresponded. Referrals could be made in a variety of ways. For example, senders who know someone who knows the intended recipient could ask for a referral certificate from the common acquaintance, or professional societies or clubs might provide certificates to refer their members to each other. Individuals could configure their email software to accept some types of referrals but not others, or prioritize messages according to their referrals. We can also imagine special-purpose referral certificates that might be usable only a finite number of times or that expire at a certain time. However, in order for a referral system to be useful it must be adopted by a critical mass of people.

Fee restructuring. Another proposed solution involves restructuring the way fees are charged for Internet services. It has been suggested that ISPs that generate large volumes of email pay the ISPs that receive that email. The email generators would then have incentives to charge their customers for sending large volumes of email. This solution would require a lot of cooperation among ISPs and backbone providers, and may pose problems for bulk mailers who send solicited email. It remains to be seen whether fees can be structured such that a significant cost burden can be placed on bulk mailers without making email prohibitively expensive for individuals.

Regulatory Solutions

Solutions to the spam problem are also being sought in the legislative realm. Four bills have been introduced in Congress this session (two each in the House of Representatives and the Senate); each suggests a different approach to using Federal power to address the problem. The first spam bill submitted this session, the "Netizens Protection Act of 1997" (H.R. 1748) would amend the Telephone Consumer Protection Act of 1991 (which prohibits unsolicited facsimile communications) and make spam subject to the same regulations as junk fax. Unsolicited commercial email would be banned and senders of solicited commercial email would be required to identify themselves on all communications. The constitutionality of this approach is questionable, however; though commercial speech may be regulated in limited cases[6] the TCPA was found not to violate the First Amendment in part because of the actual costs shifted from advertiser to recipient by junk fax and the technological alternatives available at the time.[7] Spam presents a different economic model with different costs and available remedies.

The "Unsolicited Commercial Electronic Mail Choice Act of 1997" (S. 771) does not attempt to ban

[6] See *Central Hudson Gas and Electric Corp. v. Public Service Comm'n*, 447 U.S. 557, 100 S. Ct. 2343 (1980), *Board of Trustees v. Fox*, 492 U.S. 469, 109 S. Ct. 3028 (1989).

spam but rather force it to be uniformly labeled and identified in an easily filtered manner. (Since labels amount to compelled speech this approach also raises constitutional questions.) Commercial messages would be required to be labeled as advertisements and senders of spam would have to provide opt-out methods under this proposal. ISPs would be required to provide their users with email filtering software sensitive to these labels. The bill would also grant the FTC the power to seek injunctions and/or fines against spam generators that did not properly label their message, and spam recipients would gain a private cause of action.

Another possible regulatory approach is to ban particular bad-faith actions bulk mailers use to protect themselves. This is the goal of the "Electronic Mailbox Protection Act of 1997" (S. 875), which targets particular practices instead of attempting to ban all spam. The bill would prohibit the transmission of unsolicited messages from unregistered or fictitious domains and disguising the source of an unsolicited message in order to prevent replies. Bulk mailers would be required to comply with opt-out requests, prohibited from sending spam via third-party mail agents or from harvesting names and email addresses from third-party systems in contravention to their respective policies and terms of service agreements.

Most recently, the "Data Privacy Act of 1997" (H.R. 2368) suggests that spam be controlled via the establishment of voluntary guidelines for the behavior of bulk mailers. The guidelines would be established by an industry working group (chartered by the legislation itself). Incentives for adhering to the guidelines include safe harbor provisions with respect to claims of unfair or deceptive trade practices on the part of the bulk mailers and the right to identify oneself with an icon or logo as complying with the guidelines. This approach obviously raises two questions: whether the guidelines would be significant and whether anyone would actually choose to adhere to them. Some anti-spam forces counter that this approach (and, indeed, anything short of a total ban) may actually lead to an *increase* in spam as such legislation will legitimize the practice of sending spam and remove the associated stigma.

When this article went to press, the U.S. Senate added anti-spam provisions to legislation concerning telephone fraud (S. 1618) which was subsequently passed and introduced into the House of Representatives (H.R. 3888). Title III of S. 1618 includes some of the notice requirements of S. 771 (compelled identification of the sender and maintenance of valid routing information), but does not require any action on the part of ISPs. Opponents of this legislation argue that its passage would not only legitimize the practice of sending unsolicited mail but would also allow each spammer "one free shot" at Internet users as it requires only that spammers support an opt-out procedure such as a "remove/no further" contact list.

[7]See *Destination Ventures, Ltd. v. F.C.C.*, 844 F.Supp. 632, affirmed 46 F.3d 54.

WHAT YOU CAN DO ABOUT SPAM?

If you are annoyed or inconvenienced by spam, you might want to take action to reduce the amount of spam you receive. There is a growing number of spam filtering tools available for sale and for free. Check the Web page for your email client to see if there are any tools designed specifically to work with that client. Yahoo has a list of anti-spam software at www.yahoo. com/Computers_and_Internet/Communications_and_Networking/Electronic_Mail/Junk_Email/Software.

If your email client has built-in filtering capabilities, you might try some simple spam filtering tricks such as identifying messages that are not addressed directly to you and sending them to a separate junk folder. This will catch a large percentage of spam messages, but it will also catch some legitimate messages, so make sure you look through your junk folder periodically before emptying it. You can improve the accuracy of this filter by setting up other folders for your legitimate mailing list mail and adding new filtering rules as you discover misfiled messages.

If you can't filter all the spam you receive, complaining about spam might help you feel better, and it might ultimately lead to legal action against some spammers. For information on identifying the source of spam messages and tips on who to complain to about spam, see Phil Agre's "How to Complain About Spam, or, Put a Spammer in the Slammer" at weber.ucsd.edu/~pagre/spam.html. This essay also includes an extensive list of online resources for spam-related information.

Other good online sources for information (and opinions) about spam include: spam.abuse.net/; www.cauce.org/; www.junkemail.org.

Recommendations and Conclusions

There is growing concern that the volume of spam sent each day may increase substantially and that bulk mailers may adopt increasingly sophisticated techniques to thwart automated filtering tools. If this occurs, current filtering solutions are likely to become largely ineffective and many individuals will likely become overwhelmed by spam to the point their electronic mailboxes are useless to them.

Efforts to enforce existing laws as they apply to fraudulent practices of some bulk emailers should be pursued, and the impacts of these efforts should be studied. While proposed new laws may help slow the onset of a severe spam problem, we do not believe they will be effective in the long term and they are likely to cause undesirable side effects. On the other hand, technical solutions that may have limited effectiveness right now may prove quite useful should a severe problem arise. In addition to continued filtering efforts by ISPs, we recommend that user-friendly email software be developed that supports a multipronged technical solution that includes filters, channels, payments, and referral networks. Those features that do not cause people to risk missing desired messages can be activated immediately. As the spam problem gets worse, more risky features can be activated by individuals who find the cost of spam exceeds the costs of potentially missing some desired messages.

We end with a cautionary note. In selecting solutions to pursue, it is important to keep in mind possible side effects. For example, per-message fees could make email prohibitively expensive for a variety of desirable applications, legal requirements on identifying email senders might limit legitimate anonymous communications, and channelized email and referral networks might result in increased entry barriers to social networks. The properties that make email so appealing to marketers have also served to make email an effective tool for political organizers, academic communities, social networks, and individuals. In attempting to prevent spam from destroying email as a useful medium, we should be careful not to adopt solutions that will undermine the very aspects of email that we value. C

References

1. Campbell, K.K. A NET.CONSPIRACY SO IMMENSE...Chatting With Martha Siegel of the Internet's Infamous Canter & Siegel. CuD 6.89, Oct. 1, 1994; www.eff.org/pub/Legal/Cases/ Canter_Siegel/c-and-s_summary.article
2. Denning, P. Electronic junk. *Commun. ACM 3*, 25 (Mar. 1982), 163–165.
3. Dwork, C. and Naor, M. Pricing via processing or combating junk mail. *Advances in Cryptology—Crypto '92*. E. Brickell, Ed. Lecture notes in computer science 740. Springer–Verlag, NY (1993), 139–147.
4. Federal Trade Commission Consumer Information Privacy Workshop. Transcripts and public comments available at www.ftc.gov/bcp/privacy2/index.html (June 10–13, 1997).
5. Gabber, E., Jakobsson, M., Matias, Y., and Mayer, A. Curbing junk E-mail via secure classification. In *Proceedings of Financial Cryptography '98.* (Feb. 23–25, 1998, Anguilla, BWI).
6. Hall, R.J. How to avoid unwanted email. *Commun. ACM 3*, 41 (Mar. 1998). Also available from ftp://ftp.research.att.com/dist/hall/papers/agents/channels-long.ps.
7. Lucent Personal Web Assistant. lpwa.com.
8. Postel, J. On the junk mail problem. Network Working Group Request for Comments: 706, NIC #33861. Nov. 1975. ftp://ftp.internic.net /rfc/rfc706.txt

Lorrie Faith Cranor (lorrie@acm.org) is a senior technical staff member at AT&T Labs–Research in Florham Park, N.J.; www.research.att.com/~lorrie/

Brian A. LaMacchia (bal@acm.org) is a program manager in the public key security group at Microsoft Corporation, in Redmond, Wash.; www.farcaster.com.