

CANNING SPAM: AN ECONOMIC SOLUTION TO UNWANTED EMAIL

SONIA ARRISON
FEBRUARY 2004



755 Sansome Street, Suite 450
San Francisco, California 94111
Phone: 415-989-0833 / 800-276-7600
www.pacificresearch.org

CANNING SPAM: AN ECONOMIC SOLUTION TO UNWANTED EMAIL

By Sonia Arrison

February 2004

755 Sansome Street, Suite 450
San Francisco, CA 94111
Phone: 415/989-0833
Fax: 415/989-2411
Email: info@pacificresearch.org
WWW.PACIFICRESEARCH.ORG

CANNING SPAM: AN ECONOMIC SOLUTION TO UNWANTED EMAIL

Sonia Arrison

February 2004

Pacific Research Institute
755 Sansome Street, Suite 450
San Francisco, CA 94111
Tel: 415-989-0833 / 800-276-7600
Fax: 415-989-2411
Email: info@pacificresearch.org
www.pacificresearch.org

Additional print copies of this study may be purchased by contacting us at the address above, or download the PDF version at www.PACIFICRESEARCH.ORG.

Nothing contained in this briefing is to be construed as necessarily reflecting the views of the Pacific Research Institute or as an attempt to thwart or aid the passage of any legislation.

©2004 PACIFIC RESEARCH INSTITUTE. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopy, recording, or otherwise, without prior written consent of the publisher.

TABLE OF CONTENTS

- Introduction1
- Identifying Spam1
- Who Sends Spam?3
- Spammer Tricks4
- Legislative and Legal Solutions5
- The Costs of Spam Legislation8
- High-Tech Solutions10
- Money Talks12
- Notes16
- About the Author18
- About PRI19

INTRODUCTION

Anyone who uses email knows that spam, unsolicited commercial messages, is a frustrating and growing problem. Offers of herbal Viagra, miracle organ enhancement schemes, and those “urgent and confidential” financial scams clog inboxes and waste valuable server space.

Spam now accounts for more than 56 percent of all email.¹ That tide of trash has launched a rather frenzied search for answers. Indeed, the problem has become so irritating that even less-technical types in Congress and state legislatures are busy looking for solutions. But the problem doesn’t stop at national boundaries.

Like the Internet itself, spam has an international reach with the potential ability to perturb almost everyone on the planet. As one New Zealand-based writer put it, “for most people the major irritation of the Internet isn’t viruses but spam mail, which is more like pond scum.”² People now complain about spam as they do about the weather, leading multiple research groups to attempt to quantify our collective annoyance and add to it by releasing doom-and-gloom estimates.

For example, according to a Pew Internet & American Life poll, 70 percent of e-mail users say spam makes their online experience unpleasant.³ The Radicati Group predicts that by 2007, 70 percent of all email will be spam and Ferris Research says spam cost U.S. corporations 8.9 billion in 2002.⁴ These numbers naturally lead one to ask who is sending spam and how can we stop them?

The quest for answers was the focus of an April 2003 Federal Trade Commission (FTC) workshop. Instead of finding solutions, however, the hearing demonstrated some of the key roadblocks, starting with the most basic—disagreement over the definition of spam.⁵

This paper makes the case that since people differ over what they consider to be spam, control of spam should rest with the end user. The question then becomes how to give users that control. Technology brings some answers, but the real key is economics.

IDENTIFYING SPAM

Ten years ago, if one asked the average American to define spam, they likely would have started describing the pinkish meat canned and sold by Hormel Foods.⁶ Today, however, spam is more likely to be defined as some sort of unwanted email, but that leaves a lot of room for disagreement.

For instance, many anti-spam activists say that spam is any unwanted commercial email. Marketers, such as Robert Wientzen, president of the Direct Marketing Association, argue that spam is unsolicited email that is also false or misleading.⁷ But spam can be defined even more broadly than simple commercial email.

“For me, spam is those jokes that friends send around,” says Vincent Schiavone of ePrivacy group. And even philanthropic and political messages are thought to be spam by some. For instance, California’s former secretary of state Bill Jones and presidential wannabe Senator Joseph Lieberman have both been accused of spamming, but whether their messages were spam is arguable.

When Jones ran for governor of California in 2002, his staff hired a company to send out unsolicited email to the state’s voters asking for support. The strategy backfired when some people objected to the unexpected messages and it was revealed that the mailing company took advantage of security vulnerabilities to launch the emails from a Korea-based computer.

Indeed, Internet users around the country received Jones’s message, despite the fact that he claims he tried to send it to a targeted list of California addresses.⁸ But not everyone thought Jones acted inappropriately. Mike McCurry, former press secretary for President Clinton, and Larry Purpuro, the former Republican National Committee deputy chief of staff, came to Jones’s defense. They wrote, “Had Jones chosen direct mail, radio or TV, that communication would have been equally ‘unsolicited,’ as defined in the email world. Few voters would have ‘opted in’ to receive campaign information from Jones through any of those channels.”⁹

Senator Joseph Lieberman’s run-in with the anti-spam community was similar, but accompanied by a twist of irony because a few years before sending his unsolicited messages, he positioned himself as an ardent anti-spammer. “Spam is a tremendous nuisance,” he said, “It is not requested by the receiver. It almost never contains any information of substance or value...It is costly, destructive, and an invasion of our privacy.”¹⁰

The message that got Senator Lieberman in hot water was a typical campaign message explaining why he believes he should be president. Of course, the Lieberman campaign didn’t think the message was spam. Whatever Lieberman staffers might have thought was appropriate, John Gilmore, co-founder of the Electronic Frontier Foundation (EFF), was irritated. “For the record,” he said, “I have never sent any money to Joe Lieberman, nor supported either the Republicrat or the Demmican parties...This is spam, not good old Joe getting back to me about my burning concern that he’s not president yet.”¹¹

These two examples show some of the pitfalls of using the Internet in political campaigns, but they also bring up freedom of speech issues. Imagine, for example, if the government were to pass a law banning all spam, and included in the definition any kind of unsolicited political message. It is possible, although perhaps unlikely, to imagine a scenario in which a court accepts this type of restriction as valid.¹²

The idea of banning unsolicited political messages disturbs free-speech advocates but there are others who argue that spam isn’t speech at all but simply an action. For those people, spam is defined by quantity, not content.

For example, Rich Kulawiec, a systems administrator who responded to a conversation on the influential Politech mailing list, said “Spam is conduct: specifically, spam is conduct consisting of a denial-of-service attack which may or may not be targeted at users, systems, networks, mailing lists, or some combination of these, sometimes in small but often in very large quantities.”¹³

Many shared this feeling, including another Politech reader who wrote, “I won’t call it spam until I keep getting it over and over.”¹⁴ Brad Templeton, chairman of EFF, takes the point further. He argues that if political spam were to be exempted from any spam laws, spammers would simply find ways to make their messages political, and he gives a creative and insightful example:

“They’re trying to ban cheap overseas Viagra! People now know if you go to Google and search for “cheap overseas Viagra” you will find good low priced suppliers. But the government wants to make this illegal. Write to your congressman and tell them you want it to be legal.”

Political message? Or ad?¹⁵

With all the different ways to define spam, never has the old adage “one man’s garbage is another man’s treasure” been truer. Alyx Sachs, an email marketer in Los Angeles, hinted at this in reacting to questions about anti-spam tactics.

“70 million people have bad credit.” Sachs told the New York Times, “Guess what? Now I can’t get mail through to help them.” And therein lies one of the problems.

People have different tastes and needs, and it’s difficult to know beforehand who likes what. Who could have predicted, for instance, that the spam messages selling the “Iraqi Most Wanted” deck of playing cards would be so popular?¹⁶ As *Reason* magazine editor Nick Gillespie points out, “clearly the folks who bought over 1 million decks in a matter of days didn’t necessarily find that particular piece of spam insulting.”¹⁷

Indeed, it would be frightening to many if it were possible for someone, other than our friends, family, or true business contacts, to know so much about us that they could easily target their mail to the right people.

WHO SENDS SPAM?

The first known person to ever send a piece of electronic spam was Digital Equipment marketing manager Gary Thuerk. In an interview with *USA Today*, he explained how on May 3, 1978 he sent 397 e-mails pitching technology on Arpanet, the Internet’s predecessor.

“There was negative reaction,” he said “But, on the other hand, a number of people contacted us for information.”¹⁸ Even back in the early days of the Net, where reputation controlled etiquette more strictly, there were messages one might call spam.

Email marketers and legitimate businesses are sometimes accused of sending spam, either because they are sending unsolicited mail or because individuals have forgotten that they signed up to receive information. But these are perhaps some of the least objectionable of society’s spam worries.

The worst are attempts to defraud people of their money, such as the ubiquitous Nigerian scam, or the graphically obscene email that every parent prays doesn’t show up in their children’s inboxes. Many of the people who send these emails are hiding all over the world, in the U.S. and overseas in Eastern Europe and Asia. John Rublaitus, vice president of special projects at email marketing firm Digital Impact, thinks he knows why so much fraudulent and smutty spam comes from overseas.

“I’ve worked with Indian, Latin American, and Russian engineers,” he said, “and many of them who are very clever are often under employed.”¹⁹ What this means is that many of these talented people sometimes get involved in the spam scam business.

“Hackers are a subculture here [in the U.S.]” Rublaitus said, “but over there, it’s a form of entrepreneurship.” But although antispam company Brightmail estimates that 30-50 percent of spam comes from overseas, one cannot blame all pernicious spam on international actors.²⁰ Many are located here in the U.S., and some have hit star-like levels of fame.

“Cajun spammer” Ronald Scelson, an eighth-grade dropout and self-taught computer programmer, is one of the more notorious. At a Senate committee hearing, he said that “he sends between 120 million and 180 million e-mails every 12 hours for products such as insurance, mortgages, vacations, automobiles and software.”²¹

Another infamous spammer is Howard Carmack, the “Buffalo spammer” who was arrested on identity theft and forgery charges in May 2003.²² And, of course, there was Sanford Wallace, who around 1997 was known as the “king of spam” for pumping out 25 million unsolicited emails the day before legal problems drove him from the practice.

Fame, history, and international labor problems aside, pretty much anyone with an Internet connection anywhere in the world can send spam, especially if the definition of spam is as broad as chain letters. This means that your mother and best friends sometimes fall into the nefarious category of “spammer.”

SPAMMER TRICKS

Spammers can be crafty creatures whose techniques include hunting, gathering, and even cajoling in an effort to add new email addresses to their lists. For instance, the more devious

ones harvest email addresses from newsgroup postings, chat sessions, personal web pages, and email directories.

According to an FTC study, 86 percent of email addresses posted at newsgroups and Web pages receive spam, 50 percent of addresses at free personal Web page services get it, 27 percent comes from message board postings, and 9 percent can be attributable to email service directories.²³

There are also automated techniques spammers can use to find addresses, such as the “dictionary attack.” This happens when a spammer connects to a mail server and bombards it with attempts such as abc@hotmail.com, abcd@hotmail.com, and so on.

Ronald Scelson admitted that his target email addresses came from member directories of AOL and other Internet Service Providers (ISPs), and some spammers also send out viruses and worms that suck information from users’ address books. But sometimes these techniques aren’t necessary.

All too often, unwitting individuals give their email addresses away by filling out registration forms at unscrupulous web sites or by responding to a piece of spam in an attempt to get off the list. Because individuals often make these mistakes, many groups have been trying to educate the public on how to avoid spam. In this vein, the FTC lists many good resources at <http://www.ftc.gov/bcp/online/edcams/spam/resources.htm>.

LEGISLATIVE AND LEGAL SOLUTIONS

The Internet community was amused when politicians in Britain appeared confused over whether draft regulations restricting spam referred to unsolicited email or the canned meat product.

According to one news report, Lord Renton asked: “Will the Minister explain how it is that an inedible tinned food can become an unsolicited email, bearing in mind that some of us wish to be protected from having an email?”²⁴

The best answer is that there was a Monty Python skit in which the characters at a breakfast table refer to the tinned spam over and over again (and of course, much of unwanted email arrives over and over). But humor aside, legislators around the country, and the world, are focusing on laws and regulations as a way to stem the tide of unwanted electronic messages. As of this writing, 36 U.S. states have spam laws, the U.S. Congress passed a federal spam law, and there are a number of laws in the European Union and other countries around the world.²⁵ In December 2003, the U.S. Congress approved the Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM).

CAN-SPAM dictates, among other things, that spam be truthful, that spammers cannot disguise themselves with false email addresses or misleading subject lines, that pornography be labeled, and that the FTC investigate the possibility of a “do not spam” list, similar to the “do

not call” list for telephone marketers. CAN-SPAM also pre-empts state spam laws, much to the chagrin of some who support the more draconian laws, such as California’s, at the state level. There are also a handful of other proposed bills in Congress and the FTC has already entered the fray using existing federal consumer protection laws.

States with spam laws:

Alaska	Louisiana	Oregon
Arizona	Maine	Pennsylvania
Arkansas	Maryland	Rhode Island
California	Michigan	South Dakota
Colorado	Minnesota	Tennessee
Connecticut	Missouri	Texas
Delaware	Nevada	Utah
Idaho	New Mexico	Virginia
Illinois	North Carolina	Washington
Indiana	North Dakota	West Virginia
Iowa	Ohio	Wisconsin
Kansas	Oklahoma	Wyoming

By May 2003, the FTC had already taken 53 law enforcement actions against spammers, including those who used deceptive content, phony “from” and “subject” lines, and those who created fictitious “remove me” options.²⁶ That’s a good thing, too, because the FTC estimates that 66 percent of what they define as spam is deceptive, either in the content or in the “subject” and “from” lines.²⁷ What more could a federal spam law such as CAN-SPAM or other proposed laws do to quell the flow? As it turns out, not much.

“Tracking down spammers is not so easy,” email pioneer Vint Cerf said recently.²⁸ One of the problems is that spammers are very good at hiding themselves. By forging information on the email they send out, or even by hijacking someone else’s email account, spammers can make themselves pretty much impossible to find.

The other problem is that American legislation can only be effectively enforced on American firms alone, and much unsolicited email originates from outside the country. The distributed nature of the Internet makes it easy for people to send spam from jurisdictions where laws are not in force. Many have recognized this limitation and some, such as Australia’s technology agency, have suggested entering into international treaties.²⁹

One step taken towards such an international stand is a letter, signed by Canadian, Japanese, Australian, and American agencies, to operators of open relays (servers that allow anyone to

connect to them and send email).³⁰ Open relays, the agencies wrote, “create problems” because they allow people, including spammers, to ““bounce” or route email through them to other Internet mail addresses.”³¹

But there are good reasons for open relays, including the principle of allowing anonymous speech on the Internet and the more practical: allowing people to check their mail from the road. John Gilmore makes this point: “Nobody mentions how painful authenticated networks are to operate and administer, particularly for occasional traveling guests whom you can barely communicate with because their outgoing email isn’t working.”³²

An international law would be both arduous to negotiate and likely impossible to enforce. As *Cnet News*’s Declan McCullagh points out, with the way spam levels are growing, “we can’t wait a decade for an international treaty to be drafted, ratified, and implemented.”³³ And then there’s the nagging fact that there are already a number of laws that address the spam issue, but the problem is still growing exponentially. Never mind that the new federal law will make it illegal to forge an email address, that an older California law required advertisers to put “ADV” in their subject lines, or that EU has an opt-in policy. Spammers just don’t care, and they don’t have to.

The thrust of many legal initiatives is to permit consumers to readily identify unsolicited commercial email and delete it. These attempts to require spammers to identify themselves are doomed as spammers have little incentive to do so and it is so easy for them to hide. Granted, there have been a few successes under current laws.

For instance, in May 2003, Earthlink won a \$16.4 million lawsuit against “Buffalo Spammer” Howard Carmack. And the FTC has been successful in settling some cases against cyber thieves. But as enforcement grows, so does the problem.

And spam victims are not the only ones initiating court cases. Some so-called spammers are using courts to fight back. For example, eMarketersAmerica.org, a group of anonymous e-mail marketers, argued that some blacklist sites—sites that list suspected spammers—“have published false, misleading, and libelous information about their business practices.”³⁴

While court victories might make spam-haters happy, it is clearly not a long-term answer to unsolicited email woes. Since it’s not possible to force spammers to identify themselves; what must be done instead is to permit the legitimate personal emailer to identify him or herself, in a way that the spammer cannot imitate without incurring substantial cost. Before getting too steeped in how that can be done, it is worth noting that while laws might make some feel better, poorly crafted ones could drain the economy and reduce consumer choice.

THE COSTS OF SPAM LEGISLATION

Poorly conceived laws could pose unnecessary costs on legitimate businesses that are already being forced by the market into following proper etiquette. Because this is the case, policymakers, especially at the federal level, should be careful acting in this area.

For example, laws that make it illegal to send mail to someone unless they specifically opted in, such as those in California and Delaware, erect barriers for businesses trying to find new customers or indeed even get off the ground.

A number of companies in America rely on direct mail to get their start and attract new customers. At its core, business is about communicating needs, and if government steps in to halt that communication, it could bring disastrous results. Consider the following testimony from Silicon Valley entrepreneur Dave Gehring, Enterprise and Channel Sales Director, Aeroprise.

Our sales got a kick start with spam, or rather, what some people might call spam. We started with a list of people who use software that our offering compliments. We sent them all emails explaining how our product increases their productivity, as much as 100 percent with minimal effort. Some of them responded and from there we gathered several of our first customers. This inexpensive tactic for new customer acquisition enabled us to gather our “lighthouse” customers as a young company with minimal funding and virtually no marketing budget. Now that the bubble has burst, and young companies don’t have millions of venture dollars to spend marketing new products and offerings, this is how young companies start. If that’s taken away, innovation and ultimately the economy could really suffer.³⁵

Many around the nation echo this idea. Peterson Conway, founding partner of Goodwyn/Powell, an executive recruiting firm, says that unsolicited email communication has been important in his business. “It’s been pretty successful for us. I don’t know if you’d call it spam, though.”³⁶ Maybe he wouldn’t call it spam, but anti-spam activists who believe that any unsolicited message is a problem certainly would. And it’s not just software and other companies that could be harmed.

Consider that a freelance writer submitting a story idea could potentially be considered unsolicited commercial email. Individual communication could suffer dramatically under the wrong kind of law. Even a law that just says unsolicited commercial mail must be labeled with “ADV,” such as those in Arizona and Michigan, could have serious repercussions.

“If someone wants to pitch his new book to an academic discussion list or to some friends, then to keep his nose clean, he’s got to mark it with an ADV,” says UCLA law professor Eugene Volokh. “It puts honest law-abiding people at a substantial disadvantage whenever they send in resumes and whenever they want to engage in normal commercial behavior. They’ll take a course of behavior that will lead to their e-mail being thrown out.”³⁷

In attempting to force spammers to identify themselves, a law therefore has to define spam and what actions make one a spammer. But a general law really doesn’t make a lot of sense when everyone has different ideas of spam, and could mean that some people will lose the ability to communicate.

Short of outlawing fraud, then, it might seem as though a federal law is a bad idea. But not all is always as it seems. There is one potential benefit of a federal law that many in Congress have obviously recognized: the pre-emption of poorly crafted state laws.

A minimal federal spam law like CAN-SPAM is perhaps justified as a way of saving legitimate businesses from overly restrictive state laws. Although there are other potential options for fighting bad state regulations, a federal pre-emption does go a long way towards saving the Net as a medium of communication from overly zealous states whose reach does not, and should not, extend beyond their borders.³⁸

If CAN-SPAM helps stymie political meddling in the communications affairs of others, it will be a great accomplishment, but whether that will happen remains to be seen.

CAN-SPAM Highlights

- Commercial email must contain notice that it is an advertisement or solicitation and it must allow recipients to opt-out from future mail.
- Deceptive or misleading practices are prohibited.
- Preempts state spam laws.
- FTC directed to investigate a “do not spam” list.
- To be enforced by FTC, state AGs, and ISPs.

HIGH-TECH SOLUTIONS

Back in the heady days before the Internet bubble burst, technology was thought of as a solution to almost everything. Need some pet food? No problem, just go online to Pets.com! A few years later, it was fairly clear that there are some things technology alone can't solve, including one's need for buying bulk dog food. So goes the story with spam.

There are a number of different technical responses to battling spam, such as filters at the ISP, corporate, and consumer levels, but none of these is a satisfying solution.

Filters are a little like chaperones at a teenage party—they often misinterpret legitimate actions (false positives) and they sometimes miss the naughty behavior (false negatives). And spammers are a bit like teenagers, who will change their strategies to foil the watchers.

Add to this the problems already mentioned in defining spam, and it seems an impossible situation. Nevertheless, there are a number of technologies available to battle spam. While they do not work as well as they could if economics were part of the equation, at least they have more of an effect than legislation that is slow and difficult to enforce.

For their part, spam filters attempt to recognize spam based on indicators in the message—inconsistencies in the header, character of the text, and so on. One basic example searches for keywords in the message text, such as “herbal Viagra.” These content-based filters are vulnerable to both false negative and false positive errors. That is, offensive keywords can appear in an innocent message, and it's relatively easy for a spammer to disguise provoking language. That's why messages advertising “Nlarge your Pen!s” stuff mailboxes around the nation.

Some content-based filters, such as one provided by “Spam Sleuth,” have become smarter in recent times. Learning to predict from users' classifications what category a message falls into, these “bayesian” filters are a step in the right direction. But they still make mistakes and take up user time because they need to be “trained.”³⁹

According to a category search on Yahoo, there are approximately 45 filters available.⁴⁰ One of the most popular services is a software program called “SpamAssassin,” which employs different filtering techniques. According to the web page, the product's spam-identification tactics include: header analysis (the header is the part of the email that comes before the message text), text analysis, blocking emails that come from ISPs that have been blacklisted, and “signature blocking.”

Signature blocking works by interoperating with a database of user-reported spam. As previously noted, one of the usual characteristics of spam is that it is sent to a large number of people, and each email can be said to have a “signature.” Therefore, signature filtering happens by allowing “the first person to receive a spam to add it to the database—at which point everyone else will automatically block it.”⁴¹

Cloudmark's SpamNet is a peer-to-peer program that works on the signature-based filtering idea, Mailwasher filters on content, albeit using "heuristics," and SpamBouncer checks email headers for likely spam messages. The techniques have come a long way but filters don't stamp out all spam. And some of the new bells and whistles, like the bayesian option and spam reporting, can take just as much time as hitting the delete key.

Suspected spammers, meanwhile, can land on a blacklist. Typically, an ISP will use a blacklist of Internet Protocol (IP) addresses as a simple filter and will reject any message from anyone on the list, but it's also possible to create blacklists for email addresses. Almost as old as spam itself, blacklists are useful, but also fairly controversial. That's because there are so many false positives—people accused of spamming when they haven't.

It's fairly easy for a spammer to substitute a false name in the "from" field of an email, for instance, getting an innocent person's email address blacklisted. And sometimes over-eager folks who run the blacklists target people who are simply going about their regular business. Some of the most well known blacklists include MAPS, Spam Prevention Early Warning System (SPEWS), and the Open Relay Database (ORDB).

Blacklists, which are privately run, can be frustrating for those who accidentally get flagged as spam, as it is often difficult and time-consuming to get off the list. Indeed, this author was accidentally blacklisted by the FTC's spam prevention system, which she discovered when, ironically, she tried to email the FTC a document on how to limit spam.⁴²

A whitelist is the inverse of a blacklist—only mail from known senders is accepted. This, by definition, is subject to false positives—mail from new senders is rejected or, depending on how the system is set up, slowed down. Think of white lists as "priority services" or a "trusted seal" for email. Direct marketers are the ones mainly driving this concept, and a whole host of companies have sprung up around the idea.

Ironport, for example, is a company that runs a whitelist program called "bonded sender."⁴³ Companies who promise to send only legitimate mail are on the list and can reach customers using Ironport's services more quickly and with less hassle. If the companies ever get caught spamming, they have to pay a fine.

Legitimate marketers like this approach because they believe it will help to distinguish them from those who send fraudulent messages. Similar initiatives include Project Lumos by the email service provider coalition and EPrivacy's Trusted Email Open Standard (TEOS).⁴⁴

While these whitelist programs certainly help direct marketers, they are ineffective in stopping material people might not want. And since the list is compiled by a middleman with the goal of delivering mail, the consumer isn't really in control.

A challenge/response system, on the other hand, tries to inject some cost to spammers for their actions by trying to force them to spend time. It acts as a sort of consumer-created

whitelist that is meant to verify that the sender is human (as opposed to a robot) and that the human has time to respond to the challenge (unlike a spammer who would have difficulty manually responding to each email they send out).

When email arrives, it's held in a pending folder and a return email is sent to the sender, with a challenge such as asking the person to answer a question, recognize a word in colored dots, or fill out a form. A correct response results in the mail being taken from the pending folder and placed in the user's inbox. This type of system for fighting spam got a huge boost in May 2003 when Earthlink announced that it would offer the system to its five million subscribers.⁴⁵ While challenge/response systems are very good at filtering spam, they are subject to at least one major flaw.

There are many legitimate occasions for machines to email people. Individuals may have signed up for mailing lists, customer-relationship management lists, or travel notifications. Because of this problem, challenge/response will have only limited success.

MONEY TALKS

The reason spam is such a problem is that it travels for free. This creates incentives to send as much unsolicited email to as many people as possible. The solution, therefore, is to create conditions to make spammers pay for their follies. One way would be for software companies like Microsoft to team up with a micropayment firm like iPIN to create a system that allows users to charge anyone they don't know to send them email.

A plug-in to Outlook could be created to allow users to start charging people they don't know for sending them email. A way of authenticating people would be necessary for this system to work, so digital signatures would have to be woven into the system—something not only possible but already a goal for many companies. For instance, in a June 2003 *Wall Street Journal* op-ed, Bill Gates wrote that Microsoft is already “creating a system to verify sender addresses, much as recipients' addresses are verified today.”⁴⁶ And in December 2003, Yahoo announced the development of a new system to authenticate email senders called “Domain Keys” that will be implemented by 2004.⁴⁷ Such a costing system wouldn't necessarily mean giving up free communications.

Family and friends would be put on the do-not-charge list and their emails would arrive in the user's in-box for free. But for anyone the user doesn't know, a charge of \$.50 (or whatever price the user wanted) could be levied. If, after the payment and the email from the unknown mailer is received, the user decides that he wants to communicate with the previously unknown person, he can put them on the free list and give back their money.

The first articulation of this idea appears to be from Michael Rothschild who wrote about it in *Forbes ASAP* in 1994.⁴⁸ Others include EFF's Brad Templeton, IBM's Scott Fahlman, and Todd Sundsted who won a patent in 1997 on using estamps.⁴⁹

As to whether this type of system is feasible, Colin Birge, program manager for Microsoft's MS Office group, was upbeat. "It's an interesting idea." He said, "Outlook already includes an extensibility model. It's an idea we can certainly float." And, of course, Microsoft and iPIN certainly aren't the only ones capable of creating such a system.

Another way to implement an estamps system would be for ISPs to allow the service at the server level. Indeed, they may want to do the payments off of a monthly bill in order to avoid the hassle of many small micropayments and refunds. ISPs are the most obvious economic victims of spam because it clogs their servers and wastes bandwidth, so it would make sense for them to take the lead. At least one Silicon Valley company has recognized this and has designed a system that approximates the true estamps model.

An estamps model works just like it sounds. In order to send mail, the sender would have to attach an electronic stamp; corporations or mass-senders would pay for their stamps and individuals would get them free. The idea is perfect in theory, but many have attacked it on practical grounds. How would people get stamps and who would run the system? Would it be hard for consumers to use?

These questions appear to be answered by Silicon Valley-based Goodmail Systems, which plans to implement the program through the consumer's ISP so that the transition is seamless.⁵⁰ One service provider—Yahoo—has already indicated interest in using the system, so time will tell how well it will work. In the beginning, Goodmail says it will set a default price of one cent to enter a user's box.

"We will introduce a new class of email that addresses the root economic causes of spam and restores email to a medium consumers can rely on," said Goodmail CEO Richard Gingras, "It guarantees that legitimate commercial and personal mail often mistakenly lost to spam prevention methods will be delivered, and consumer requests to unsubscribe from email sources will be respected. By shifting the economics of email, providers can continue to provide low-cost access and enhanced service to their members."

According to Gingras, the program will be implemented in two phases. In phase one, bulk mailers like the Gap, J.Crew, or other retailers would buy stamps to guarantee delivery into the user's mailbox. On first glance, this might sound like a license to spam, but it's not.

If a user gets an email he doesn't want, he can simply click on the opt-out button on the bottom of the message. Unlike current arrangements, the opt-out lists will be enforced because the system, not humans, will enforce it.

This is good news for consumers because they will have more control and avoid the perpetual false positives associated with current spam filters. The plan is also valuable because its content-neutral nature steers it away from free-speech problems that arise with other solutions. Legitimate mailers will like this system because although they will pay to send messages, they will have better guarantees that delivery actually occurred.

“Our biggest surprise was how much the mass senders liked this idea,” said Gingras, “but it turns out they really want to distinguish themselves from illegitimate spammers. They also want to make sure their messages get through without having to stop using words like ‘free’ and ‘discount’ in order to escape spam filters.”

Perhaps ISPs have the greatest reason to embrace this system, as they will get paid through stamp revenue for their infrastructure costs and the bandwidth that bulk mail sucks from their networks. They could also make their customers happy by sharing stamp profits while stopping spam. Of course, phase one of the program is not enough to eliminate spam.

In phase two, ISPs will issue free “person-to-person” stamps to consumers so that every email is automatically stamped without effort. This takes care of confusion over how to use the stamps. It also puts an end to spam as the ISPs will allow consumers to reject any incoming mail that doesn't have a stamp or at least subject non-stamped email to spam filters at their strongest settings.

But what about consumers at ISPs who are not part of the stamping system? When they attempt to send email to someone on the system, a message would come back directing them to a page where they can buy a stamp. Not a perfect solution at first, but if the system works, most ISPs will offer the stamps themselves.

Spammers could, of course, buy stamps and send mail, but that is unlikely to be profitable. And Goodmail's opt-out system doesn't allow for a piece of mail to be sent more than once if the recipient has chosen to opt-out. More nefarious spammers could try to hijack an email account and send spam using the free stamps, but Goodmail says that trick will be foiled by monitoring the volume of email sent, based on historical sending patterns.

Although Goodmail representatives are wary about discussing any additional phases, founder Daniel Dreymann speculated about a possible phase three that would complete the original estamps idea by giving consumers the ability to set their own stamp prices.

For example, a high-profile CEO might make it more expensive for people to enter her mailbox as her time is extremely limited and she only wants important messages to get through. On the other hand, a college student interested in talking with all sorts of people might set a low price to facilitate communication. The system, if implemented with this third phase, would go a long way towards both eliminating spam and giving users freedom of choice.

This is the first time consumers have come close to obtaining a spam solution that effectively implements the pure estamps theory that many, including this author, have been advocating for years. If Goodmail and its test-case ISP hold true to the estamp model, consumers could very well see a spam-free Internet in the near future. Legislators itching to pass more spam laws should hold off and let the marketplace deliver the solution.

The marriage of economics with technology is the best solution to deal with the problem of spam. It preserves individual choice and does not require mammoth enforcement machines. It is a solution that follows the simple rules of the marketplace to fix what seems now to be an unmanageable problem.

That's not to say that law and filters are completely useless. But they are not nearly as effective, and inexpensive to implement, as the estamps solution.

NOTES

- ¹ According to Brightmail http://www.brightmail.com/pressreleases/121803_spam_2003.html
- ² “Spam: how to attract it and how to kill it,” by Stephen Ballantyne, *The National Business Review* (New Zealand) April 17, 2003.
- ³ <http://www.pewinternet.org/reports/reports.asp?Report=102&Section=ReportLevel1&Field=Level1ID&ID=443>
- ⁴ ePrivacy group compilation.
- ⁵ <http://www.ftc.gov/bcp/workshops/spam/index.html>
- ⁶ See: <http://www.spam.com/>
- ⁷ “Can Spam be Stopped,” by Grant Gross, *Computerworld*, May 1, 2003.
- ⁸ “CAMPAIGNS: California Candidate Chastised For E-mail To Voters,” by *National Journal’s Tech Daily*, March 1, 2002.
- ⁹ “But Cut Political Email Some Slack,” by Mike McCurry and Larry Purpuro, *LA Times*, p. 15, August 15, 2002.
- ¹⁰ “Hail to the...spammer-in-chief?,” by Declan McCullagh, *Cnet news*, January 20, 2003. <http://news.com.com/2010-1071-981258.html>
- ¹¹ “Hail to the ...Spammer in Chief,” by Declan McCullagh, *Cnet news*, January 20, 2003. <http://news.com.com/2010-1071-981258.html>
- ¹² See: “Political E-Mail: Protected Speech or Unwelcome Spam?” by Mark Sweet in the *Duke Law Review*, January 14, 2003. <http://www.law.duke.edu/journals/dltr/articles/2003dltr0001.html>
- ¹³ <http://www.politechbot.com/p-04371.html>
- ¹⁴ “Some defenses of political spam and Sen. Lieberman’s bulk mail,” *Politech* mailing list, January 25, 2003.
- ¹⁵ <http://www.politechbot.com/p-04337.html>
- ¹⁶ See “E-mail Message Blitz Creates What May Be Fastest Fad Ever,” by Saul Hansell, *New York Times*, June 9, 2003.
- ¹⁷ “Why I Love Spam,” by Nick Gillespie, *TechCentralStation*, June 16, 2003.
- ¹⁸ “Spam thrives despite effort to screen it out,” by Jon Swartz and Paul Davidson, *USA Today*, May 8, 2003.
- ¹⁹ Interview with Sonia Arrison, May 29, 2003.
- ²⁰ “A Modest Proposal to End Spam,” by Declan McCullagh, *Cnet News*, April 28, 2003. <http://news.com.com/2010-1071-998513.html>
- ²¹ “Congressional bill to kill spam would do the opposite,” *San Jose Mercury News*, June 3, 2003.
- ²² http://www.oag.state.ny.us/press/2003/may/may14a_03.html
- ²³ “Spam Harvest study” <http://www.ftc.gov/opa/2003/05/spamtestimony.htm>
- ²⁴ “House of Lords email debate reveals ‘spam’ confusion,” by Will Sturgeon, *Silicon.com*, May 7, 2003.
- ²⁵ For a concise summary of laws see: David Sorkin, www.spamlaws.com.
- ²⁶ “No “Silver Bullet” to Limit Spam, FTC Tells Congress”, FTC press release, May 21, 2003. <http://www.ftc.gov/opa/2003/05/spamtestimony.htm>
- ²⁷ “No “Silver Bullet” to Limit Spam, FTC Tells Congress”, FTC press release, May 21, 2003. <http://www.ftc.gov/opa/2003/05/spamtestimony.htm>
- ²⁸ “Internet pioneer discourages legislation to curb spam,” by Steve Alexander, *Star Tribune*, April 26, 2003.
- ²⁹ “Australia Mulls Global Anti-spam Effort,” by Declan McCullagh, *Cnet news*, April 16, 2003. <http://news.com.com/2010-1071-981258.html>
- ³⁰ <http://www.ftc.gov/bcp/online/edcams/spam/openrelay/pdf/EnglishLetter.pdf>
- ³¹ <http://www.ftc.gov/bcp/online/edcams/spam/openrelay/pdf/EnglishLetter.pdf>
- ³² “Verio censored John Gilmore’s email under pressure from anti-spammers,” by John Gilmore, various dates. <http://www.toad.com/gnu/verio-censorship.html>

- 33 “Want to Stop Spammers? Charge ‘em.” By Declan McCullagh, *Cnet news*, May 5, 2003.
<http://news.com.com/2010-1071-999561.html>
- 34 “Spammers Fight Back in Court,” by Joanna Glasner, *Wired News*, May 14, 2003.
- 35 Interview with Sonia Arrison, May 30, 2003.
- 36 Interview with Sonia Arrison, June 5, 2003.
- 37 “A Modest Proposal to End Spam,” by Declan McCullagh, *Cnet News*, April 28, 2003.
<http://news.com.com/2010-1071-998513.html>
- 38 And some states are worried that this may very well happen. In April, Washington attorney general Christine Gregoire and 43 other attorneys general urged Congress to avoid unnecessary pre-emption. See: “A National Solution at Center of Debate,” by Gary Young, *National Law Journal*, May 19, 2003.
- 39 <http://email.about.com/cs/bayesianfilters/>
- 40 http://dir.yahoo.com/Business_and_Economy/Business_to_Business/Computers/Communications_and_Networking/Software/Email/Junk_Email_Removal_and_Filtering/
- 41 <http://www.spamassassin.org/index.html>
- 42 “Public Access to FTC Hurt by Spam Lists,” by Declan McCullagh, *Cnet news*, November 26, 2002.
<http://news.com.com/2100-1023-975473.html?tag=rn>
- 43 <http://www.bondedsender.com/>
- 44 http://www.e-businessworld.com/ic_1309734_10402_1-5041.html and
<http://www.eprivacygroup.com/article/articlestatic/62/1/6>
- 45 “Earthlink to offer Anti-Spam E-mail System,” by Johnathan Krim, *Washington Post*, May 7, 2003, P. E 01.
<http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A22390-2003May6¬Found=true>
- 46 “Why I Hate Spam,” by Bill Gates, *Wall Street Journal*, June 23, 2003.
- 47 “Yahoo proposes new Internet anti-spam structure,” by Ben Berkowitz, Reuters, December 5, 2003.
- 48 “When You’re Gagging on Email,” by Michael Rothschild, *Forbes ASAP*, June 1994.
http://www.bionomics.org/text/resource/articles/ar_014.html
- 49 See Templeton: <http://www.templetons.com/brad/spam/estamps.html>, Sundsted patent:
<http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PALL&p=1&u=/netahtml/srchnum.htm&r=1&f=G&l=50&s1=5,999,967.WKU.&OS=PN/5,999,967&RS=PN/5,999,967>
- 50 <http://www.goodmailsystems.com/>

ABOUT THE AUTHOR

SONIA ARRISON

Director, Technology Studies

Sonia Arrison is director of Technology Studies at the California-based Pacific Research Institute where she researches and writes on the intersection of new technologies and public policy. Specific areas of interest include privacy policy, e-government, intellectual property, nanotechnology, evolutionary theory, and telecommunications.

She is a regular columnist for TechCentralStation.com and her work has appeared in many publications including CBS MarketWatch, CNNfn, LA Times, Sacramento Bee, San Francisco Chronicle, San Jose Mercury News, The National Post, Washington Times, and Consumer Research Magazine. She is author of *Consumer Privacy: A Free Choice Approach*, co-author of *Internet Taxes: What California Legislators Should Know*, and editor of *Telecrisis: How Regulation Stifles High Speed Internet Access*. A frequent media guest and National Press Club First Amendment Scholar, Ms. Arrison has appeared on National Public Radio's "Forum," Tech TV, CBC's "The National," and CNN's *Headline News*.

Prior to joining PRI, Ms. Arrison focused on Canadian-U.S. regulatory and political issues at the Donner Canadian Foundation. She also worked at the Fraser Institute in Vancouver, where she specialized in regulatory policy and privatization. She received her BA from the University of Calgary and an MA from the University of British Columbia.

ABOUT PRI

The Pacific Research Institute champions freedom, opportunity, and personal responsibility for all individuals by advancing free-market policy solutions. It provides practical solutions for the policy issues that impact the daily lives of all Americans. And it demonstrates why the free market is more effective than the government at providing the important results we all seek—good schools, quality health care, a clean environment, and economic growth.

Founded in 1979 and based in San Francisco, PRI is a non-profit, non-partisan organization supported by private contributions. Its activities include publications, public events, media commentary, community leadership, legislative testimony, and academic outreach.

EDUCATION STUDIES

PRI works to restore to all parents the basic right to choose the best educational opportunities for their children. Through research and grassroots outreach, PRI promotes parental choice in education, high academic standards, teacher quality, charter schools, and school finance reform.

BUSINESS AND ECONOMIC STUDIES

PRI examines how the entrepreneurial spirit, the engine of economic growth and opportunity, is stifled by onerous taxes and regulations. It recommends comprehensive public-policy reforms that would maintain a robust economy, ensure consumer choice, and spur creativity and innovation.

HEALTH CARE STUDIES

PRI reveals the failure of the single-payer model for health care, drawing particularly on the dramatic problems within the Canadian system. It proposes market-based policy reforms that would provide greater access to care, improve quality, and increase affordability.

TECHNOLOGY STUDIES

PRI is dedicated to defending individual liberties, fostering high-tech growth and innovation, and limiting harmful government intervention in the digital world.

ENVIRONMENTAL STUDIES

PRI reveals the dramatic and long-term trend towards a cleaner, healthier environment. It also examines and promotes the essential ingredients for abundant resources and environmental quality property rights, markets, local action, and private initiative.