

S. HRG. 108-968

SPAM (UNSOLICITED COMMERCIAL E-MAIL)

HEARING

BEFORE THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION UNITED STATES SENATE

ONE HUNDRED EIGHTH CONGRESS

FIRST SESSION

—————
MAY 21, 2003
—————

Printed for the use of the Committee on Commerce, Science, and Transportation



U.S. GOVERNMENT PRINTING OFFICE

85-548 PDF

WASHINGTON : 2013

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512-1800; DC area (202) 512-1800
Fax: (202) 512-2104 Mail: Stop IDCC, Washington, DC 20402-0001

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED EIGHTH CONGRESS

FIRST SESSION

JOHN McCAIN, Arizona, *Chairman*

TED STEVENS, Alaska	ERNEST F. HOLLINGS, South Carolina,
CONRAD BURNS, Montana	<i>Ranking</i>
TRENT LOTT, Mississippi	DANIEL K. INOUE, Hawaii
KAY BAILEY HUTCHISON, Texas	JOHN D. ROCKEFELLER IV, West Virginia
OLYMPIA J. SNOWE, Maine	JOHN F. KERRY, Massachusetts
SAM BROWNBACK, Kansas	JOHN B. BREAUX, Louisiana
GORDON H. SMITH, Oregon	BYRON L. DORGAN, North Dakota
PETER G. FITZGERALD, Illinois	RON WYDEN, Oregon
JOHN ENSIGN, Nevada	BARBARA BOXER, California
GEORGE ALLEN, Virginia	BILL NELSON, Florida
JOHN E. SUNUNU, New Hampshire	MARIA CANTWELL, Washington
	FRANK R. LAUTENBERG, New Jersey

JEANNE BUMPUS, *Republican Staff Director and General Counsel*

ROBERT W. CHAMBERLIN, *Republican Chief Counsel*

KEVIN D. KAYES, *Democratic Staff Director and Chief Counsel*

GREGG ELIAS, *Democratic General Counsel*

CONTENTS

	Page
Hearing held on May 21, 2003	1
Statement of Senator Allen	10
Statement of Senator Burns	8
Statement of Senator Cantwell	55
Statement of Senator McCain	1
Letter dated May 21, 2003 from Bill Gates, Chairman and Chief Software Architect, Microsoft	3
Letter dated May 20, 2003 from Jerry Berman, President, Center for Democracy & Technology	4
Statement of Senator Nelson	17
Statement of Senator Wyden	9

WITNESSES

Dayton, Hon. Mark, U.S. Senator from Minnesota	15
Hughes, J. Trevor, Executive Director, Network Advertising Initiative	76
Prepared statement	78
Leonsis, Ted, Vice Chairman, America Online, Inc. and President, AOL Core Service	58
Prepared statement	61
Rotenberg, Marc, Executive Director, Electronic Privacy Information Center and Adjunct Professor, Georgetown University Law Center	83
Prepared statement	85
Salem, Enrique, President and CEO, Brightmail Inc.	63
Prepared statement	64
Scelson, Ronald, Scelson Online Marketing	89
Prepared statement	92
Schumer, Hon. Charles E., U.S. Senator from New York	11
Prepared statement	14
Swindle, Hon. Orson, Commissioner, Federal Trade Commission	18
Report dated April 30, 2003 from the Federal Trade Commission's Division of Marketing Practices entitled "False Claims in Spam"	20
Prepared statement	37
Thompson, Hon. Mozelle W., Commissioner, Federal Trade Commission	38
Prepared statement	40

SPAM (UNSOLICITED COMMERCIAL E-MAIL)

WEDNESDAY, MAY 21, 2003

U.S. SENATE,
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION,
Washington, DC.

The Committee met, pursuant to notice, at 9:35 a.m. in room SR-253, Russell Senate Office Building, Hon. John McCain, Chairman of the Committee, presiding.

OPENING STATEMENT OF HON. JOHN MCCAIN, U.S. SENATOR FROM ARIZONA

The CHAIRMAN. Good morning. Today, the Committee will examine whether there are ways we can effectively deal with the increasing proliferation of spam in America. I commend the Federal Trade Commission for its dedication to the complex policy and technical issues involved in putting an end to unwanted spam. I also want to strongly commend Senators Burns and Wyden for their continued work over the years in trying to address this issue through legislation. Literally hundreds of hours have been spent by these two Senators and their staffs in trying to address this very, very difficult issue.

Spam means different things to different people. The FTC defines spam generally as unsolicited commercial e-mail, and some Americans do not want any of it, other consumers like to receive unsolicited offers by e-mail. To them, spam means only unwanted, fraudulent or pornographic e-mail that floods their in-box. Many American businesses view e-mail as a new medium through which to market or communicate more efficiently with consumers. To them, that is not spam, but commercial speech protected by the First Amendment.

Internet service providers are caught in the middle, often drawing a distinction between what they, but not necessarily consumers perceive as good or bad actors, and permitting some unsolicited e-mails to pass through their networks to consumers while blocking others in their spam filters. Regardless of whether you call all unsolicited commercial e-mail spam, it is rapidly on the rise, and its sheer volume is affecting how consumers and businesses use e-mail. E-mail messaging has fundamentally changed the way we communicate with family and friends, the way we communicate with businesses that provide goods and services, and the way that businesses market products to consumers.

The growing affliction of spam, however, may threaten all of us. Less than 2 years ago, spam made up only 8 percent of all e-mail. Today, industry experts estimate that more than 45 percent of all

global e-mail traffic is spam, and many expect it to reach the 50 percent mark by this summer. AOL estimates that it blocks 80 percent of all its inbound e-mail, nearly 2.4 billion messages each day. Managing this influx adds real cost to consumers and businesses. There are other costs to Americans, such as the cost to our children, who may be victimized by the nearly 20 percent of spam that contains pornographic material, some including graphic sexual images.

The FTC also tells us that two-thirds of all spam contains deceptive information, much of it peddling get-rich-quick schemes, dubious financial or health care offers, and questionable products and services. While most agree that something should be done about spam, it is clear that legislation alone will not solve the problem.

Yesterday's *New York Times* had a very interesting article. It says—and I will not, obviously, quote the whole article. I will include it in the record, but it said at first, it looked as if some students at the Flint Hill School, a prep academy in Oakton, Virginia, had found a lucrative alternative to an after-school job. Late last year, technicians at America Online traced a new torrent of spam, or unsolicited e-mail advertisements, to the school's computer network. On further inquiry, though, AOL determined the spammers were not enterprising students. Instead, a spam-flinging hacker who has still not been found exploited a software vulnerability to use Flint Hill's computers to relay spam while hiding the e-mails' true origins.

I mention that story because the complexity of this issue is challenging to all of us, and the complexity and the innovative ways that spammers are employing make this to some degree an issue that has ever-changing challenges. The fact that there may be—keeping up with resourceful spammers' latest technology is not the only challenge. Jurisdictional barriers only complicate enforcement, and up to 90 percent of all spam may pass through mail servers outside of the United States.

The fact that there may be no silver bullet to the problem of spam does not mean, however, that we should stand idly by and do nothing at all about it. It is clear we must act, but I ask the witnesses to help us define the problem and tell us how, whether by technical, legislative, or other means we can be most effective. For Congress' part, we should make no mistake, unless we can effectively enforce the laws we write, those laws will have little meaning or deterrent effect on any would-be purveyor of spam.

Finally, I ask industry to continue to respond to the demands of American consumers in doing all that it can to stop the worst part of spam. Parents should not have to think twice before encouraging their children to use the computer.

I thank the witnesses, and look forward to the testimony.

Also, I would like to enter into the record, letters from Mr. Bill Gates and also Jerry Berman of the Center for Democracy and Technology, basically stating their commitment to working with us to try to eliminate this issue.

[The information referred to follows:]

MICROSOFT
May 21, 2003

LETTER FROM BILL GATES TO THE U.S. SENATE COMMERCE COMMITTEE REGARDING
SPAM HEARINGS

Dear Chairman McCain and Ranking Member Hollings:

Thank you for holding this important and timely hearing on spam. I greatly appreciate the leadership of both you and your Commerce Committee colleagues. I regret that we are unable to participate directly, but would like to take the opportunity to share Microsoft's perspective on this critical e-commerce and consumer issue.

The torrent of unwanted, unsolicited, often offensive and sometimes fraudulent e-mail is eroding trust in technology, costing business billions of dollars a year, and decreasing our collective ability to realize technology's full potential. According to some industry estimates, spam now makes up more than 50 percent of all e-mail. To make matters worse, spam often preys on less sophisticated e-mail users, such as our children, posing a genuine threat to personal security and privacy and threatening the very utility of e-mail as a viable communication tool.

Microsoft firmly believes that spam can be dramatically reduced, and that the solution rests squarely on the shoulders of industry and government. There is no silver bullet solution to the problem. Rather, we believe that fully addressing this problem for the long-run requires a coordinated, multi-faceted approach that includes technology, industry self-regulation, effective legislation, and targeted enforcement against the most egregious spammers.

In terms of technology, Microsoft is committed to providing customers with the best solutions available, and engaging on every level to find new and better technical means to stop spam. To date, Microsoft's investments in anti-spam technologies have already paid off for businesses and consumers through innovations available in new versions of our products, such as MSN, Hotmail, Exchange and Outlook.

The industry is building better filters every day, and is investing heavily in research and development to open the door to greater innovation. We need filtering technologies that are easier for consumers to use, and more effective at determining which e-mail messages are spam and which are desired communications. This differentiation will greatly reduce the risk of falsely misidentifying legitimate e-mail as spam.

While we and others have made significant advances in anti-spam technology, we recognize there is still much work to be done. But technology is not the only answer. Effective and complementary self-regulation efforts by the industry are crucial.

Specifically, we support the establishment of an independent trust authority or authorities around the globe that could spearhead industry best practices, and then serve as an ongoing resource for e-mail certification and customer dispute resolution. In short, these authorities could provide mechanisms to identify legitimate e-mail, making it easier for consumers and businesses to distinguish wanted mail from unwanted mail. Of course, any technology designed to establish the identity of legitimate commercial firms and associate them with a trusted sender "seal" should be based on open standards and developed with broad input from affected industries.

But in order for the self-regulation and technology efforts to be successful, they need to be supported by strong Federal legislation that prohibits fraudulent and deceptive spamming practices, and empowers consumers without threatening the vitality of legitimate e-commerce.

Specifically, Federal legislation should create incentives for e-mail marketers to adopt best practices, and to certify themselves as trusted senders who can be more easily identified by consumers and filters alike. One way to encourage marketers to adopt e-mail best practices is to provide a Safe Harbor for those companies who are members of an FTC-approved self-regulatory organization. Under this approach, safe harbor participants would be entitled to avoid the burden of additional labeling requirements (such as "ADV:" to identify e-mail advertisers) while enjoying other regulatory benefits based upon their compliance with specific sender guidelines.

Thus, Federal legislation should identify the basic components that industry guidelines must address, such as notice and choice obligations, but permit the industry to take the lead in developing the specific guidelines within these parameters.

Microsoft believes other elements of Federal legislation should include:

- Effective Internet service provider (ISP) enforcement that allows ISPs to prosecute spammers on behalf of their customers;
- Meaningful definitions to capture all bad actors involved in sending unlawful spam, including those who knowingly assist in the transmission of unlawful spam;
- Provisions that permit state Attorneys General to enforce violations of Federal law, as well as existing state contract and trespass laws, in order to further increase the pressure on persistent spammers;
- Express language that preserves the right of ISPs to combat spam (*i.e.*, provisions that make it clear that the Federal anti-spam law does not impose an obligation on ISPs to block or carry certain types of e-mail messages, and does not impair an ISP's ability to enforce its anti-spam policies); and
- Federal preemption of state statutes that regulate the sending of commercial e-mail messages provided the Federal anti-spam law contains strong substantive requirements. Because ISPs rely heavily on state contract and trespass laws, as well as laws relating to computer fraud and theft, in their fight against spammers, Federal preemption in any anti-spam law should include a carve-out for such state laws.

The recent increase in anti-spam legislative activity both domestically and internationally is encouraging, and we commend you for the important work you are doing in this area. Current U.S. state laws already make it possible for the industry to begin taking action against spammers who are illegally targeting customers. Enforcement efforts across the industry to date have been successful, and more will come. ISPs including Microsoft, AOL and Earthlink have already begun to file lawsuits, as have the Federal Trade Commission and many state Attorneys General, in an effort to increase the costs of sending spam, thereby reducing its volume.

As a leader in the industry, Microsoft is committed to using its resources to help address this problem from every perspective: technology, self-regulation, legislation and enforcement. We have started to see progress on all fronts, but much more work needs to be done.

We pledge our support to your legislative effort, and look forward to sharing our proposals and working with others toward a viable solution. When industry, government and technology come together to solve the spam problem, we will truly be able to offer consumers a trustworthy, safe and more productive e-mail experience.

Sincerely,

BILL GATES,
Chairman and Chief Software Architect.

CENTER FOR DEMOCRACY & TECHNOLOGY
Washington, DC, May 20, 2003

Chairman JOHN MCCAIN,
Senate Committee on Commerce, Science, and Transportation,
United States Senate,
Washington, DC.

Dear Chairman McCain:

The Center for Democracy and Technology is continuing its activity to help find effective solutions to the problem of unsolicited commercial e-mail—also known as “spam.” We welcome the Committee’s inquiry into this important issue, and look forward to working together towards a solution that will protect the Internet and its users from the choking effects of unwanted e-mail, while maintaining the openness and innovation that makes the Internet so valuable.

As per your request, we have attached our recent report “Why Am I Getting All This Spam?” which we ask you to consider in the Committee’s hearings on this issue. In the report, CDT explored the ways in which spam was received by over two hundred and fifty e-mail addresses spread all over the Internet. In six months, we received over eight thousand unsolicited e-mail messages to addresses that had been posted on the Web, used in newsgroups, or disclosed to Internet businesses.

From that research, CDT created a series of tips for users to take steps to shield themselves from spam. Those tips, as well as the rest of our report, are attached.

Based on our research and further discussions, CDT believes that the spam problem merits targeted Federal legislation to help alleviate the burdens spam causes for consumers, businesses, and ISPs. While spam is undeniably a major problem for the future of the Internet, we must be careful to craft legislation that can be effective and does not run counter to freedom of speech and other concerns.

A prerequisite to narrow and effective spam legislation is open dialogue among policymakers, industry, and Internet users—a dialogue that is only beginning to occur. This committee has an important role to play in creating the kind of open discussion that will lead to the best path forward. We look forward to continued work with you on this important issue.

Sincerely,

JERRY BERMAN,
President.

LexisNexis

Copyright 2003 The New York Times Company

The New York Times—May 20, 2003 Tuesday Correction Appended Late Edition—Final

SECTION: Section A; Column 1; Business/Financial Desk; Pg. 1

LENGTH: 1835 words

HEADLINE: TECHNOLOGY; E-MAIL'S BACKDOOR OPEN TO SPAMMERS

BYLINE: By SAUL HANSELL

BODY:

At first, it looked as if some students at the Flint Hills School, a prep academy in Oakton, Va., had found a lucrative alternative to an after-school job. Late last year, technicians at America Online traced a new torrent of *spam*, or unsolicited e-mail advertisements, to the school's computer network.

On further inquiry, though, AOL determined that the spammers were not enterprising students. Instead, a *spam*-flinging hacker—who still has not been found—had exploited a software vulnerability to use Flint Hills' computers to relay *spam* while hiding the e-mail's true origins.

It was not an isolated incident. The remote hijacking of the Flint Hills computer system is but one example among hundreds of thousands of a nefarious technique that has become the most common way for spammers to send billions of junk e-mail messages coursing through the global Internet each day.

As *spam* has proliferated—and with it the attempts by big Internet providers to block messages sent from the addresses of known spammers—many mass e-mailers have become more clever in avoiding the blockades by aggressively bouncing messages off the computers of unaware third parties.

In the last two years, more than 200,000 computers worldwide have been hijacked without the owners' knowledge and are currently being used to forward *spam*, according to AOL and other Internet service providers. And each day thousands of additional PC's are compromised at companies, institutions and—most commonly of all—homes with high-speed Internet connections shared by two or more computers.

"The spammers have mutated their techniques," said Ronald F. Guilmette, a computer consultant in Roseville, Calif., who has developed a list of computers that are forwarding *spam*. "Today, if you are trying to do a really mass spamming, it is de rigueur to do it in an underhanded manner."

Just last Thursday, 17 law enforcement agencies and the Federal Trade Commission issued a public warning about some of the ways spammers now commandeer computers to evade detection. The officials translated the warning into 11 languages because many of the exploited computers are known to be in China, South Korea, Japan and other countries with heavy Internet use.

Mostly, the spammers are exploiting security holes in existing software, but increasingly they are covertly installing e-mail forwarding software, much like a computer virus. For some, hacking is no longer about pranks, but making a profit.

"This is not about a hacker trying to show off, or give you a hard time," said William Hancock, chief security officer for Cable and Wireless, the British telecommunications company. "This is about money. As long as there are people who want *spam* to go out, this is not going to go away."

Spam fighters say that some software is too easy to exploit and should be fixed. Moreover, computer users can take technical precautions to safeguard their machines. But not everyone will bother to take those steps, even if he or she discovers having been dragooned into the spammers' global army.

To begin with, most users do not see much effect when their computer has been co-opted. Surfing the Web from the victimized computer may be slower than usual but that is not always easy to detect. In most cases, the owners' e-mail addresses are not added to the spammed messages, so there is no need to worry that friends

and associates will think the PC owners have suddenly started peddling herbal Viagra.

Indeed, the only way most users even become aware of such hijackings is when they receive telephone calls or e-mail from their Internet service providers saying a piece of *spam* was traced back to their machines.

"People are shocked," said Bobby Arnold, a network abuse engineer at Earthlink, the big Internet provider. "Someone will say, 'I thought my computer was running a little slow, but I had no idea it was being used to send *spam*.'"

Some of the victims of the hidden spammers are revolted to learn, Mr. Arnold said, that they are aiding the hucksters and pornographers responsible for what many Internet users consider the medium's great blight. The truly offended rush to safeguard their machines.

But others, who see no direct impact to themselves, simply shrug off the problem, Internet providers say. Intent on reducing their network clutter, the providers then often try to cajole them into cooperating—and, if that fails, will sometimes cut off a user's service.

Sometimes people do find that someone has been sending *spam* and using their e-mail address as the sender, but this does not mean that their computers were used. Nothing on the Internet verifies that an e-mail message was actually sent by the person listed in the "From" address, which is one reason fighting *spam* is so hard.

And spammers like to send e-mail that appears to be from their enemies or names chosen at random. The legitimate owners of those addresses are often left to clean out hundreds or thousands of complaints from their e-mailboxes.

When a computer receives an e-mail message, it does record a code number, called an Internet protocol address, that can be traced to the computer that is connecting to it. But often e-mail is passed from one machine to another and the identity of the original sender cannot be verified.

Indeed, the rapid rise in the number of spammers trying to hijack innocent computers is a direct result of their desire to hide their own Internet protocol addresses from *spam* blockers. Most commonly, they are taking advantage of a backdoor in much of the software that office users or people with high-speed connections at home often install to share an Internet link among several computers—or so-called proxy servers. Some other types of e-mail and Web surfing software, typically run by larger companies, can also be taken advantage of if security features are not properly set up.

Because it essentially enables one computer to masquerade as another, a proxy server is an ideal tool for anyone seeking to use the Internet anonymously. So proxy servers are used by people in some countries to visit websites blocked by government censors. They are also used by hackers trying to attack other machines. And they are perfect for spammers trying to avoid filters.

None of these uses would be possible if the owners of the proxy servers made sure to configure them for access only by authorized users. But whether from laziness or ignorance, many users of proxy servers leave them open to anyone on the Internet.

AnalogX Proxy, a free proxy-server program that has been downloaded by more than a million people, is automatically in the open state when it is first installed. Mark Thompson, the author of AnalogX, said he had rebuffed the requests of many antispam activists to distribute the software with the security features already activated because doing so would make it harder to set up.

"The biggest plug for the proxy is it is really easy to get it running," he explained. Mr. Thompson said he did try to achieve a compromise by revising the program to give people a warning about security problems every time it starts.

Even so, Wirehub, a Dutch Internet service provider, says that 45,000 of the 150,000 open proxy servers it has identified as sending *spam* appear to be using AnalogX.

To find all these vulnerable machines, spammers and other hackers deploy computers that do nothing more than try to connect to millions of computers across the Internet, looking for open proxy servers to exploit.

At the Flint Hills School, "it was pretty amazing how fast our vulnerability was picked up by the spammers," Robert Hampton, the school's director of technology, said recently. Once the problem was identified, the school was able to fix it immediately.

Spammers and hackers trade or sell lists of open proxy servers on dozens of websites. And other sites sell software a would-be spammer can use to find new servers.

In the last six months, an increasingly common trick has been for spammers to attach rogue e-mail-forwarding software to other e-mail messages or hide it in files that are meant to emulate songs on music sharing sites like KaZaA.

As with all such hacker contraptions, and much *spam*, it is difficult to figure out who is behind these programs. But there is some evidence that one of the major *spam*-sending programs, known as Jeem, originated in Russia, which has been a fertile ground for both spammers and hackers.

Last October, Michael Tokarev, a Russian computer programmer active in the worldwide antispam effort, noticed a lot of *spam* in Russian that offered bulk-mailing services. The messages were identical, but they came from many different computers. He investigated and found they were forwarded by a program, calling itself Jeem, that had not been seen before.

Mr. Tokarev said that in December, a Russian forum for spammers called *Carderplanet.com* contained a posting offering to sell the Internet addresses of open proxy servers, for \$1 each, that appeared to be machines infected with Jeem. "Since the last week of December, several big U.S. spammers started to use those Jeems, too," Mr. Tokarev wrote in an instant message interview last week.

Machines infected with Jeem, which is especially hard to find because it keeps switching its identity on the computers it borrows, seem to be used these days mostly by spammers selling pornography, David Ritz, a volunteer *spam* fighter, said. Using a software monitoring tool he helps run, Mr. Ritz last week examined the messages sent to Internet news groups from just one home computer infected with Jeem. On one day last week, this computer sent 773 pornographic news postings with subjects like "Lolita paradise" and "N.U.D.E—L,O,L,I,T,A,S."

"Open proxies are the single greatest threat to the integrity of the network that we see now," he said.

AOL, which has made fighting *spam* a central part of its marketing thrust, is taking what some see as radical action against open proxy servers. It will no longer accept any incoming e-mail sent directly from the computers of individual home users with high-speed service. This will not affect most home users because they typically do not run e-mail servers on their own computers but connect their e-mail programs to servers run by their Internet providers. But a handful of advanced users and small businesses do run their own e-mail servers connected to high-speed lines, and they no longer can send e-mail to AOL users.

Road Runner, the high-speed service of Time Warner cable, is taking a different approach. It is actively running the same sort of scanning program used by the spammers to find out whether any of its customers have open proxy servers. Those that do are asked to close them. Many other service providers shy away from such scanning because it appears to be an invasion of privacy.

"It's a race," said Mark Harrick, Road Runner's director of network security. "There are malicious individuals scanning our users looking for vulnerabilities every day, and we want to find them first."

CORRECTION-DATE: May 21, 2003

CORRECTION:

A front-page article yesterday about mass e-mailers who bounce *spam* off the computers of unwitting third parties misspelled the name of a prep school in Virginia whose network was used to send *spam*. It is Flint Hill, not Hills.

The article also misspelled the surname of the director of security for Road Runner, which is scanning its customers' systems to determine whether they are vulnerable. He is W. Mark Herrick Jr., not Harrick.

GRAPHIC: Chart: "Close the Door To Spammers" To avoid having their e-mail ads blocked, spammers are increasingly relaying their messages covertly through computers of home and office Internet users. The users are often unaware that their computers have been hijacked. Measures to prevent spammers from commandeering a computer will also make for a safer Internet connection. **ERECT A FIREWALL** A firewall program governs what programs may connect to the Internet and can block the forwarding of rogue e-mails. Firewalls come both as software programs and built into routers, devices used to share a connection. **USE ANTIVIRUS PROTECTION** This software protects against infiltration by a covert *spam*-relaying program. Keep this software updated, as hackers are prolific. **BEWARE OF DOWNLOADS** Many malicious programs are distributed in the form of attachments to e-mails, or files to download, as from a music-sharing website. **LIMIT PROXY SERVERS** If using proxy-server software instead of a router to share an Internet connection, make sure it is set to share only with computers on the local area network, not the entire Internet. Common proxy-server programs include AnalogX Proxy and Wingate. (pg. C6)

The CHAIRMAN. I would like to ask Senator Burns, if that is OK, Senator Burns and then Senator Wyden, and then we will welcome our two colleagues.

**STATEMENT OF HON. CONRAD BURNS,
U.S. SENATOR FROM MONTANA**

Senator BURNS. Thank you, Mr. Chairman, and I think you hit the nail on the head a little while ago. I want to thank my colleague, Senator Wyden, and you mentioned him spending many hours on this issue, and we have for the last 4 or 5 years, but I also want to commend you for your patience in putting up with us. We have been involved in this issue quite a while now, and now we are finally coming down to a product I think we can present to the American people with pride, and I think also the Chairman's acknowledgement that legislation alone will not take care of this problem. It will, however, facilitate industry and law enforcement people, especially the FTC, to get down to business and look at it seriously, as if we have the technology to prevent this unwanted commercial e-mail, if you want to call it that, and do something about it, because it is the cost to businesses and individuals are escalating, and they are wide-ranging.

Businesses lose money when employees take more time to wade through their e-mails, individuals who pay long distance charging to ISPs end up footing the bill while their inbox is filled with unsolicited messages. Servers all over the country have difficulty blocking spam, all while spammers work to find more and more ways to circumvent the latest software server or individual blocking systems.

I want to specifically, really, at this point thank my colleague, Senator Wyden, who has been working tirelessly for years. Last month, Senator Wyden and I reintroduced the CAN-SPAM bill, which passed unanimously out of this Committee last year. I thank the cosponsors of the bill, particularly those on this Committee and here today, including Senators Stevens, Breaux, Nelson, and, of course, Senator Schumer, and we will hear from him later.

The CAN-SPAM bill empowers consumers and grants additional enforcement authority to the FTC to take action against spammers. The bill will provide additional tools to end this online harassment by allowing users to remove themselves from the mass e-mail lists and impose steep fines up to \$1.5 million on those spammers. For particularly flagrant offenders, the CAN-SPAM bill carries criminal penalties, including up to a year in jail for those who disguise their identities and use false and misleading subject lines. In short, this bill provides broad consumer protection against bad actors, while still allowing legitimate Internet advertising as a justified means of flourishing.

While it is obvious to anyone with an e-mail account that the scourge of spam has continued to worsen, the trends are becoming more apparent by the day, and even more alarming. According to a recent article in *The Washington Post*, spam currently accounts for 40 percent of all the e-mail traffic. The number is estimated to exceed that this summer. America Online alone is blocking 2.4 billion spam messages every day. That seems almost unbelievable. If

current trends continue and nothing is done, the toxic sea of spam is threatening to drown the very medium of e-mail.

The digital dreck of spam is particularly poisonous in rural areas. Because of the vast distances in Montana, many of my constituents are forced to pay long distance charges for their time on the Internet. Spam makes it nearly impossible for those in rural America to realize the tremendous economic and educational benefits of the online era. In today's information age, where beating the competitor to the next sale is absolutely critical to survival, spam-related slow-downs and shutdowns are causing real economic damage. According to one study done by a consulting group, spam will cost U.S. businesses \$10 billion this year alone.

The true impact of spam is seen in individual stories. A constituent of mine, Jeff Smith, who built a cutting-edge cyber hotel in Missoula, Montana, he has calculated that spam has cost his business \$300,000 a year. Nearly half of the bandwidth he buys is sucked up by unwanted messages. His entire company is only worth \$2.5 million, so clearly, a loud clarion call for Federal legislation has gone forth, and the Committee should heed this call.

Just weeks ago the *New York Times* mentioned it, as was cited by our Chairman today, and understanding the peril that we are in is drowning something that actually a lot of folks have thought to be one of the great tools that we have in this country especially in areas we might call remote.

So thank you, Mr. Chairman, for having this hearing. Thank you for your patience. Thank you for understanding the problem that we are facing.

The CHAIRMAN. Thank you, Senator Burns. Senator Wyden.

**STATEMENT OF HON. RON WYDEN,
U.S. SENATOR FROM OREGON**

Senator WYDEN. Thank you, Mr. Chairman. I will just make a few comments. Senator Burns and I have been prosecuting this case against spam now for more than 4 years, and he has said it very well, and I have been really proud to have been his junior partner in this cause all these years, and we appreciate the fact that you are willing to hold this hearing.

Mr. Chairman, it just seems to me what this issue is all about is giving consumers control over their inbox. At this point, there are few, if any, consequences for those who have chosen to abuse the open and low-cost nature of e-mail, and that is what Senator Burns and I have been trying to change all these years, and I wanted to take just a minute to put a bit of perspective on this, because as we have been at this now for several Congresses, what would always happen is that we would get favorable reactions from people, citizens and others who are frustrated with spam, but we always heard a number of arguments that now was not the time for congressional action.

People would say, well, the problem is not so serious, it is just an annoyance. They would say, you can use the delete key, that is the only solution that anybody needs, it is overkill to have a variety of enforcement tools, and what seemed particularly ironic in this Committee, since we led the effort for the Internet Tax Freedom Act, people said that spam legislation would stunt the growth of E-

commerce. Well, I do not think those arguments hold much weight any more, given the fact that we have got this tidal wave of spam, and the question now is to look at the good ideas.

Senator Burns and I think that we have come up with an approach that is going to work, but we know our colleagues have a number of good ideas, and we are anxious to look at those as well, but begin to change the odds. The people who are spamming are not technological simpletons. These are very sophisticated, savvy people, and what we need to do is to change the odds, and we believe in our legislation, by producing a tiered approach on enforcement—Senator Burns and I have criminal penalties, we give the Federal Trade Commission civil authority to bring action, we give the state Attorneys General the authority to bring action, and we give the ISPs, the Internet service providers the authority to bring action, and we believe that if you bring a modest number of enforcement actions using that kind of authority, you send a message to those scamming spammers and people who want to abuse the system that the odds are going to change. The odds are more likely that this is going to be treated as a serious problem and you are going to have some consequences.

The last point that I would make, Mr. Chairman, is that I think you absolutely have to have a tough enforceable national law, because the alternative is, the country will have a crazy quilt of state laws. The spammers will play the states off against each other, and I think the problems will continue to proliferate. What this really comes down to is, in our country, we think that the consumer ought to have a right to know where e-mail is coming from, and they ought to have a right to tell the spammer to stop. We are anxious to move forward finally, welcome our colleagues. They have good ideas, and several of our other colleagues do as well. Let us move to examine them and then pass legislation here in this Committee.

And I thank you.

The CHAIRMAN. Thank you. I would like to welcome both of our colleagues, Senator Schumer and—Senator Allen, did you have an opening comment?

**STATEMENT OF HON. GEORGE ALLEN,
U.S. SENATOR FROM VIRGINIA**

Senator ALLEN. If I may, Mr. Chairman. Thank you, and I want to thank all of our witnesses for appearing this morning on this important topic. In fact, I was with a group of people—I will not mention who; it is political, but I said we have to leave here because we have got a hearing on spam, and everyone said go, great, get rid of it, and so this is a good bipartisan issue that I think all Americans care about. Obviously, for e-mail and Internet to continue, it has to be efficient, and unfortunately—and you will get all the testimony here—it is becoming that you spend more time deleting unwanted messages, and that is one thing personally, it is another thing for a business, and I will also speak briefly on a few points here.

I know that Commissioners Swindle and Thompson will be testifying, the FTC Commissioners, and I want to commend you all for the effort you have been making particularly enforcing against e-

mail that is fraudulent or containing deceptive information. That is very important, and I commend you. The goal here, as we see it, is to empower consumers or provide them with a choice while preserving legitimate E-commerce business activities that are important for the growth of our economy and businesses. I do think that the costs, though, associated with spam far outweigh the benefits of it.

This is a balance we have to strike here, and consumers—and I will say this as a parent—are becoming increasingly concerned about the spam that is coming through to our children, not just disruptive to the family, but children, and people will talk about that. I will say from personal experience now, using AOL as my Internet service provider compared to previous ISPs, it is much better in blocking this unwanted spam. You may have to click off a few ads, which you have always had to do, but as far as blocking this unwanted spam, it is far, far better in that regard, and I know that Mr. Leonsis will testify on AOL's efforts.

Finally, I want to commend this legislation that Senator Burns and Senator Wyden have. I think it is a good bill pending before our Committee, Mr. Chairman, as it relates to the issue of state preemption, which is an important matter for Virginia, and we have just passed a very good law. It strikes the right balance as far as enforcement and preserving certain causes of action as far as fraud, so I think ultimately, an approach which incorporates the good legislation like the Burns-Wyden legislation, as well as effective Government enforcement, and let us also couple it with technology advancements and solutions, and improved business practices. We will strike that appropriate balance needed to empower consumers while maintaining e-mail as a viable commercial communications tool, and I thank you, Mr. Chairman, for having this very timely, needed hearing.

I thank all the leaders and our colleagues for their leadership, and look forward to reading and hearing the testimony of our witnesses.

The CHAIRMAN. Thank you. Welcome to our colleagues, Senator Schumer and Senator Dayton.

Senator Schumer.

**STATEMENT OF HON. CHARLES E. SCHUMER,
U.S. SENATOR FROM NEW YORK**

Senator SCHUMER. Thank you, Mr. Chairman. First, I want to thank you for holding these timely hearings and for your leadership on so many consumer issues. I think people who have problems with all sorts of different new technological and other industry problems look to you as a beacon, and once again, you are Johnny-on-the-spot, and we very much appreciate it. I also want to—I did not even—the double entendre was not intended.

[Laughter.]

Senator SCHUMER. Sometimes these things just slip out. It is not so bad. Worse things have been said about people.

In any case, I also want to thank Senators Burns and Wyden. They have been true trailblazers and leaders on this issue, and I know as we try to come together on legislation that their proposals

and their thoughts on this will help us dramatically in Congress solve this problem.

Now, it is no secret, Mr. Chairman, we are under siege. Armies of online marketers have overrun e-mail inboxes across the country with ads for herbal remedies, get-rich-quick schemes, and pornography. Today's spam traffic is growing at a geometric rate, causing the superhighway to enter a state of virtual gridlock. What was a simple annoyance last year has become a major concern this year, and could cripple one of the greatest inventions of the 20th Century next year if we do nothing.

As a result, Mr. Chairman, a revolution against spam is brewing as the epidemic of junk e-mail exacts an ever-increasing toll on families, businesses, and the economy. A number of us in the Senate have proposed legislation aimed at curbing the spread of spam. I have proposed a no-spam list, criminal penalties for spammers, and several other initiatives geared toward reducing the number of unwanted e-mails we get in our inboxes, and obviously there are many other solutions out there, and we know that there is no silver bullet; that not any one solution is going to solve this problem, because as you mentioned, the technology—you have offensive and defensive warfare, and every time a defensive warfare does some good, the offense uses the same technology to get ahead.

But there is one fact that is very encouraging, and that is that 90 percent of spam, it is estimated, is caused by about 250 users, such as the fellow they just caught in my state, in Buffalo. That means that legislation, while it will not eliminate spam, can really go after the worst users. So can enforcement, and we can make a real dent and turn the tide, so instead of the number of spam messages every one of us gets going up each week, it will go down and down until it is back to being just an annoyance.

So today I am going to discuss these measures, but I also want to talk about one other thing, because spam grows so exponentially, and that is the need for an international effort in the war on spam to occur at the same time we seek to deal with the problem here in the United States. The simple fact of the matter is that so many of the problems that have come about in the digital age are inherently global. Spam is no exception.

Spam is truly an international issue, because the Internet is a global resource, and stemming the rising tide of spam is essential if the Internet is to continue to be an effective medium of communication and commerce. It would not do us much good if we went after the spammers here in the United States and they set up shop in another country and just did the same thing.

Other countries are beginning to deal with spam, Korea and Australia among them. Their governments are considering anti-spam measures, and collaboration with these and other Nations is crucial if the U.S. is to be effective, so that is why today I am proposing an international agreement, a treaty to fight spam. A global agreement will ensure that anti-spam standards protecting American computers are enforceable both here and abroad.

An international agreement will become more important as new regulations and law enforcement efforts in the U.S. cause the most prolific spammers to flee to other countries. We know that is what they do. We have experience with money laundering, digital piracy,

child pornography. We know that as soon as we tighten up our laws here and institute vigorous enforcement, those who want to violate our laws move abroad to avoid prosecution.

The bottom line is that the second we tighten up enforcement here at home, rogue actors go overseas to continue their activities. If we are just focused on curbing spam here at home, we will be unsuccessful, but that does not mean we should sit on our hands until we get our fellow countries on board with these efforts. There is a lot of work that needs to be done here, and that is why so many interested parties, including the Direct Marketing Association, have come around to the view that the Federal Government can play a meaningful role in stopping spam. They know that effective anti-spam legislation makes it more likely that consumers will read legitimate marketing messages.

We also have the problem of pornography, which is really a serious one. Let me illustrate this point with a story. My wife and I have two wonderful children, one of whom is just about to complete her first year at college, and the other, a 14-year-old girl, Alison, is an absolute whiz on the Internet. She spends far more time on the Internet than she does watching television, which until recently we thought was great, considering what is on television.

Well, as parents we do our best to make sure the Internet is a positive experience for her, a device to help her with her school work, learn about events taking place around the world, maybe even a way to order the latest N Sync CD. You can imagine my wife's and my anger and dismay when we discovered that not only was she a victim of spam, but like all e-mail users, much of the junk mail she was receiving advertised pornographic websites, things I would not want to see, let alone have my child see. That is another reason that we have to move, and we have to move quickly.

So let me just discuss the solution that I have proposed. Criminal penalties, and we really need stiff jail time for repeat offenders. We can warn them once, fine them significantly second, but if they keep doing this, we should give them jail time, and I am working with my colleagues on the Judiciary Committee. We will have to work in concert with the Commerce Committee, which has primary jurisdiction, in terms of criminal penalties. We can hunt down the spammers one by one using these penalties, and again, because so much of spam is caused by so few people, it should make a real difference.

Another idea I have offered is the national no-spam registry. A list maintained by the FTC would be a gigantic database of people who can call in or e-mail in and opt out of receiving unwanted spam by submitting their mail addresses to the list. The list is modeled on the highly successful do-not-call registries that have been used to ward off telemarketers. It has been very successful in telemarketing. Admittedly, it is a little harder with spam, because it is a lot cheaper than having somebody make a phone call, but again, given the small number of people who do this, it can make a real and dramatic difference.

Although a similar list for e-mail addresses poses security challenges that must be addressed before implementation, I am hopeful that this list, in conjunction with ADV labeling, safeguards for

those who employ best practices, might be one way we can give consumers control over their inboxes.

In conclusion, Mr. Chairman, this is a very important issue. The technology which has blessed our lives and accounted for so much of the prosperity we have seen in the last two decades is at risk, a very real part of it, and I am glad that you are Chairman of this Committee and look forward to working with you, Senator Burns, and Senator Wyden to come up with a good, strong, comprehensive bill. At the same time, I hope we can all work together to get our country to start talking to other countries about a treaty, so when we solve things here, they do not just go right overseas and we have to start all over again.

Thank you, Mr. Chairman.

[The prepared statement of Senator Schumer follows:]

PREPARED STATEMENT OF HON. CHARLES E. SCHUMER,
U.S. SENATOR FROM NEW YORK

Chairman McCain, Senator Hollings, Colleagues, Good morning.

Mr. Chairman, I want to thank you for holding this hearing to address Unsolicited Commercial e-Mail or spam. I also want to commend Senators Burns and Wyden for their leadership and hard work on this issue.

I believe we are under siege. Armies of online marketers have overrun e-mail inboxes across the country with advertisements for herbal remedies, get-rich-quick schemes and pornography.

As you are all aware, spam traffic is growing at a geometric rate, causing the Superhighway to enter a state of virtual gridlock.

What was a simple annoyance last year has become a major concern this year and could cripple one of the greatest inventions of the 20th century next year if nothing is done.

Way back in 1999, the average e-mail user received just 40 pieces of unsolicited commercial e-mail—what we call spam—each year. This year, the number is expected to pass 2,500. I know that I'm lucky if I don't get 40 pieces of spam every couple of days!

As a result, a revolution against spam is brewing as the epidemic of junk e-mail exacts an ever increasing toll on families, businesses and the economy.

Let me illustrate this point with a story. My wife and I have two wonderful children, one of whom is just about to complete her first year at college. The other, a 14 year-old girl, is an absolute whiz on the Internet who loves sending and receiving e-mail.

As parents, we do our best to make sure she has good values and that the Internet is a positive experience for her—a device to help her with her schoolwork or learn about events taking place around the world and, maybe even a way to order the latest N Sync CD.

You can imagine my anger and dismay when I discovered that not only was she a victim of spam like myself, but, like all e-mail users, much of the junk e-mail she was receiving advertised pornographic websites.

I was and remain virtually powerless to prevent such garbage from reaching my daughter's inbox.

The frustration I feel in the battle against spam is one that I think business owners and Internet Service Providers across that nation can identify with.

According to Ferris Research, spam costs businesses in the United States \$10 billion each year in lost productivity, consumption of Information Technology resources and help-desk time.

With surveys showing that over 40 percent of e-mail traffic qualifies as spam, ISPs spend millions of dollars each year on research, filtering software and new servers to deal with the ever expanding volume of junk e-mail being sent through their pipes.

And, if the spam itself isn't enough, spammers often engage in crimes such as identity theft and fraud to secure e-mail addresses and domain names from which to send millions of pieces of junk e-mail.

All of this demonstrates that it's time to take back the Internet from the spammers. And why I am joining you today in saying that enough is enough.

We all know that spammers use a variety of tools and methods to send millions of e-mail messages each day. In order to be effective, I believe spam solutions will have to be as creative and varied as the spammers' efforts.

We should give law enforcement officials, ISPs and others a wide variety of tools to fight spam.

Among the possible solutions that are exist—and this is not an exhaustive list—are pending legislation in the Senate and the House the would enact anti-e-mail harvesting provisions and special e-mail labeling requirements; stipulate valid unsubscribe features; and prohibit false and fraudulent header, router and subject line information.

And that's just a start. As I said before, because of the dramatic challenges we face in stemming the spam flood, we need a multi-pronged approach.

In particular, I believe stiff criminal penalties—including jail time for repeat offenders—are warranted. I am working with my colleagues on the Judiciary Committee on a bill to create these new penalties.

We will hunt down spammers one by one, using criminal penalties to show what will happen to those who continue to send junk e-mail.

Another idea I have offered is a National No-Spam Registry. This list, maintained by the Federal Trade Commission, would be a gigantic database of people who have "opted out" of receiving spam by submitting their e-mail addresses to the list.

The list is modeled on the highly successful Do-Not-Call registries that have been used to ward off telemarketers.

Although a similar list for e-mail addresses poses security challenges that must be addressed before implementation, I am hopeful that this list might be one way we can give consumers control over their in-boxes.

None of these solutions will be the silver bullet that stops all spam. But a multi-faceted approach has a better chance of reducing the ever-growing amount of spam than a solitary solution.

And stemming this rising tide is essential if the Internet is to continue to be an effective medium of communication and commerce.

If spam continues to grow, people will rely on their e-mail less and less. Right now, consumers are becoming so frustrated at the junk e-mail bombardment that they delete legitimate commercial e-mail as if it were spam.

This is why so many interested parties, including the Direct Marketing Association, have come around to the view that the Federal Government can play a meaningful role in stopping spam.

They know that effective Federal anti-spam legislation will make it is more likely that consumers will read legitimate marketing messages.

I think we can all agree that spammers must not be allowed to bog down the vast potential of e-mail and the Internet.

It is my hope that the impressive roster of panelists you have assembled here today will stimulate ideas to stop spammers in their tracks. I look forward to hearing their testimony and working with all of you to bring and end to the current junk e-mail epidemic.

The CHAIRMAN. Thank you very much, Mr. Schumer. Thank you for coming.

Senator Dayton.

**STATEMENT OF HON. MARK DAYTON,
U.S. SENATOR FROM MINNESOTA**

Senator DAYTON. Thank you, Mr. Chairman. I thank you for the opportunity to testify before you this morning, and I commend you for your leadership in this whole area, and I certainly commend Senators Burns and Wyden also for their leadership and the legislation that they have introduced.

I want to just at the outset, on behalf of the state of Minnesota and the good Minnesota Company, Hormel, voice an objection to the use of the word, "spam" to characterize all of this activity. You know that spam was, for a half-century, the bane of existence of servicemen and women and others, and it came to define a certain low point in some people's view of things, but I think it has actually gotten much lower if that is the case.

Senator Burns and I had the opportunity—I ate over in South Korea at the DMZ—to eat my third MRE, and I must say, Spam at any temperature is a lot better than the MRE that I ate—

[Laughter.]

Senator DAYTON.—however automatically warmed in its pouch, and now we have this form of spam, which is, you know, very, very different from the Hormel version. For one, with Hormel, you get to choose whether or not you want it. Second, it is not forced down anyone's throat.

[Laughter.]

Senator DAYTON. The source is clearly identified, and the contents, too. You can ask Hormel what they put in their Spam, and they will just tell you right up front it is everything but the kitchen sink.

[Laughter.]

Senator DAYTON. And in what proportions, and what—it is left to your imagination, but my anti-spam proposals are incorporated in the legislation I have introduced as 563, which is the Consumer/Owner's Bill of Rights, and it is broader than just the anti-spam, but I will focus on that point alone this morning, and it is a starting point, not an end product at all, and I recognize going into this that the great appeal of the Internet is that it has been unregulated and it has been free.

I have met many who have enjoyed it that way and used it that way and want to keep it that way, but unfortunately, individual freedom becomes, in a larger and ever-larger social system, a form of anarchy. In that process comes a form of Darwinism, where everyone is on his or her own. The strongest, the smartest, the most aggressive tend to take over and dominate, and that is the situation with spam today.

There are 31 billion messages being transmitted through cyberspace today, each day. That is an estimate, but it is enormous and ever-expanding, and these 31 billion messages are transmitted freely and free. They are unregulated, they are unrestricted, and they are largely unwatched, and everyone who is involved in that system must individually then protect themselves; the individuals, businesses, and the like, which is great for the software industry, who has not created this problem, but has tried to help deal with it.

There are all sorts of software that you can buy to prevent spam and pop-ups and ads and all sorts of things, which range from nuisances at best, but then increasingly, invasions of people's lives, spies, identity theft, credit card theft, and spam also becomes a carrier of viruses, worms, trojan horses, which are even more destructive and costly to individuals and to businesses.

McAfee's anti-virus unit estimates that there are 62,000 virus threats today, and these numbers that I am throwing out are ones that other sources would have quite different, which is part of the function of the expansion of this, and rapidly growing aspect of this whole realm, is that I have seen numbers that deviate quite a bit from one another, but one virus alone, the Code Red worm in the year 2001 was estimated by Computer Economics, an independent research firm, to have a worldwide cost of \$2.62 billion, one virus, and it is expanding, and some would say it is even exploding. Sen-

ator Schumer referenced Howard Carmack, who was recently arrested. It is estimated that he issued himself 825 million pieces of spam last year, one individual in 1 year.

Write Mail, the spam blocker firm, estimates, and others have said, some 40 percent of all Internet e-mail today is spam. I have seen figures that estimate that percentage is higher, but the percent share of the e-mail is increasing, I think everyone would agree. Legislation will not solve this, as others have said, but the situation will not improve without legislation. In fact, it will get worse, and I think this is a case where the perfect becomes the enemy of the good. This is going to be a moving target. It is going to be ongoing. It is sort of going to be like the *Mad Magazine Spy v. Spy*, where they will be ever-dueling, one escalating and outsmarting and outwitting the other, and the other needing to respond.

So whatever we design has to be flexible, the process must be nimble, and it has to be dynamic. It has to keep up with these ever-new developments, and so I would recommend something along the lines of what Robert Kennedy said up in the Department of Justice years ago, the Anti-Organized Crime Task Force, a SWAT team, a team that would drive this effort, carry out congressional mandates, and would interact with industry, with users, with leaders in Congress, but we have to have something that is as dynamic as the industry itself, and as inventive as the spam producers themselves.

My own legislation suggests a national registry, where people can opt out one time. Another is to make every e-mail sent to someone in the United States be identified as to its source, and finally, I think it is worth looking at—I am not prepared to propose this now, but some very, very small charge to every e-mail that is sent, so small that it would not be onerous for an individual or a business that has regular use, but it would add up and be a financial deterrent for those who are sending millions and even billions of these e-mails all over the world.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you very much, Mr. Dayton. Senator Nelson has an opening comment, and we will leave and go vote and come right back. As soon as you finish, we will take a quick break.

**STATEMENT OF HON. BILL NELSON,
U.S. SENATOR FROM FLORIDA**

Senator NELSON. And it will be short, Mr. Chairman. I just want to throw on the table another approach, and the approach would be to have an opt-out provision—

If all of you leave, that means I am chairing the Committee.

[Laughter.]

Senator NELSON. We will take up the Nelson bill right now.

[Laughter.]

Senator NELSON. The approach is virtually along the same lines. It would be more, instead of the implied consent that Senator Wyden's bill indicates, there would be more of a consumer protection. The message would have to have an opt-out provision where the consumer could say, I do not want any more of this, and if we are really going to put teeth into this, that this violation, both criminal

penalty with jail time and/or fines, would be the first element showing the conspiracy or continuum of activities that would activate the RICO Act, which is the Racketeer Influenced and Corrupt Organization Act, which then gives prosecutors the tools to go after the criminal enterprise and to confiscate the assets.

Now, that is starting to put some bite into the legislation, and so I want to offer that, and that will be a part of the discussion as we get in and tinker with this legislation, trying to fit and design a solution so that consumers can start using their e-mail. I mean, it is just unbelievable.

A week ago, I was in my Tampa office. The press had come in. We were just going to shoot the breeze, and I happened to punch up on the computer to see what messages were there. In 1 day, I had a normal letter-size piece of paper, single-spaced, full of unwanted e-mail messages, two of which were pornographic. Now, if that is happening to a United States Senator, you can imagine what is happening to our citizens all across the country, and they do not want this, and it is time for the Government to do something to stop it.

Another interesting change is that the major network providers in the past have been quite skittish about any kind of interference with this new form of communication, but they have come around now because we are starting to see that there is so much of an interference with the normal communication lines that the Government is going to have to step in and do something about this, perhaps with the FTC, but also very likely with legislation.

And I will just close my comments and dash off to vote, to say this. Since I had that conversation in my Tampa office, the media wrote about it, and that has been in Florida, and I will tell you, everywhere I have gone in Florida since, people keep coming up to me and saying, thank you for being willing to do something about this, because it has gotten to the point that we are fed up and we have had enough, so I hope that we will do something about it.

The Committee will stand in recess.

[Recess.]

The CHAIRMAN. We will resume the hearing. The witnesses in the first panel are Hon. Orson Swindle of the Federal Trade Commission and Hon. Mozelle Thompson, also with the Federal Trade Commission. Welcome, gentlemen. Since one of you has white hair and one of you has no hair, we will begin with the white-haired Mr. Swindle.

[Laughter.]

Mr. THOMPSON. I am just follically challenged.

[Laughter.]

Mr. SWINDLE. I would win if we did this on looks, too.

[Laughter.]

The CHAIRMAN. Mr. Thompson.

[Laughter.]

**STATEMENT OF HON. ORSON SWINDLE, COMMISSIONER,
FEDERAL TRADE COMMISSION**

Mr. SWINDLE. Thank you, Mr. Chairman and Members of the Committee, for this timely discussion of spam and the threat it poses to potential benefits of information technology. Consumers

must have trust and confidence and comfort with technology and its uses, particularly when it comes to their privacy and security of personal and sensitive information. Spam undermines consumer trust and confidence. It represents a significant and rapidly growing threat to web-based services. The Commission's prepared testimony provides the Committee with an excellent overview of our efforts to combat spam.

What is spam? We have heard it discussed several times this morning. The FTC defines spam as any commercial electronic mail message that is sent, typically in bulk, to consumers without the consumers' prior request or consent. I think the Chairman's term, unwanted, may be perfect.

There are at least four major concerns caused by spam. First, the volume is increasing at astonishing rates. Current estimates indicate that at least 40 percent of all e-mail is spam. Second, recent studies by the FTC indicate that spam has become the weapon of choice of those engaged in fraud and deception. Nearly 66 percent of the spam we examined appeared to contain falsity and deception. I would ask that our False Claims in Spam Report be included as part of the record, Mr. Chairman.

The CHAIRMAN. Without objection.

[The information referred to follows:]



FALSE CLAIMS IN SPAM

A report by the FTC's Division of
Marketing Practices

April 30, 2003

FALSE CLAIMS IN SPAM


I. OVERVIEW


In this report, staff of the Federal Trade Commission's ("FTC") Division of Marketing Practices describes the results of its review of approximately 1,000 pieces of unsolicited commercial email (UCE), commonly known as "spam." This random sample was drawn from a pool of over 11,000,000 pieces of spam. This study, which focuses on the likely truth or falsity of claims contained in the messages, supplements two previous FTC studies of spam – the "Spam Harvest" (finding that 86% of addresses posted to web pages and newsgroups received spam) and the "Remove Me Surf" (finding that 63% of email list removal requests were not honored).

This study represents the first extensive review of false claims appearing in UCE.¹ FTC staff who are trained to spot deceptive and unfair practices identified indicators of falsity for several types of offers likely to appear in spam. These indicators of falsity were based on representations found to be false in previous law enforcement actions brought by the Commission and on staff research. Staff then analyzed each piece of spam to determine whether the "From" line, "Subject" line, or message content contained any of these signs of falsity. The presence of signs of falsity in a message reviewed in this study does not mean that the message satisfies the legal standard of deception under the FTC Act; further investigation would be necessary to make such a determination. Staff also reviewed each piece of spam to determine whether the message contained pornographic images (in order to determine whether the nature of the images was disclosed in the "Subject" line), a request for personal information, or a label indicating that the message was an advertisement.

The messages reviewed by FTC staff consist of random samples from three FTC data sets – the UCE Database (consisting of spam forwarded to the FTC by members of the public), the Harvest Database (consisting of messages received by undercover FTC email boxes seeded on Internet web pages and in chat rooms), and spam received by FTC employees in their official FTC inboxes. A full description of the data sets, the sampling ratios, and likely biases of each data set are discussed in Section XI. (Methodology).

¹ Studies by others have focused on the economic costs resulting from spam (*see, e.g.*, <http://www.ferris.com> (April 8, 2003)), the volume of UCE (*see, e.g.*, http://www.brightmail.com/pressreleases/122302_holiday_spam_alert.html (Dec. 23, 2002)), and consumer attitudes regarding spam (*see, e.g.*, http://www.harrisinteractive.com/harris_poll/index.asp (Jan. 3, 2003)).

 **About 1,000 pieces of spam were analyzed to determine whether they bore the hallmarks of falsity.**

 **FTC staff analyzed false claims appearing in "From" and "Subject" lines and in the body of messages.**

II. TYPES OF OFFERS MADE VIA SPAM

FTC staff began its analysis by determining the type of offer being made in each spam message. The messages fell into eight general categories, with a catch-all category included for types of offers that appeared infrequently:

Type of Offer	Description
Investment/Business Opportunity	work-at-home, franchise, chain letters, etc.
Adult	pornography, dating services, etc.
Finance	credit cards, refinancing, insurance, foreign money offers, etc.
Products/Services	products and services, other than those coded with greater specificity.
Health	dietary supplements, disease prevention, organ enlargement, etc.
Computers/Internet	web hosting, domain name registration, email marketing, etc.
Leisure/Travel	vacation properties, etc.
Education	diplomas, job training, etc.
Other	catch-all for types of offers not captured by specific categories listed above.


✉ **Investment/
Business
Opportunity**
offers account for **20%** of spam studied. The majority of these are work-at-home, franchise, chain letter, and other non-securities offers.

The following illustration sets forth the prevalence of different types of offers in the random sample of spam analyzed by FTC staff:



✉ **Investment/
Business
Opportunity,
Adult, and Finance**
offers together comprise over half of spam in sample.

Together, Investment/Business Opportunity, Adult, and Finance offers comprised 55% of the random sample of spam analyzed by FTC staff. Surprisingly, given that UCE inherently targets consumers with computers and Internet connections, only 7% of the spam analyzed concerned offers for computer or Internet-related products or services.

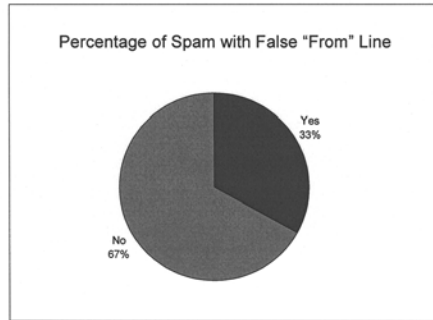
 Only 7% of spam analyzed concerned Computer or Internet-related goods or services.


III. FALSITY IN "FROM" LINE

The "From" line in each UCE message was examined to determine whether the information obscured the true identity of the sender. FTC staff determined whether the "From" line contained any of the following indicators of falsity:

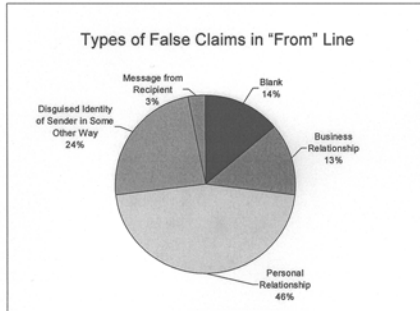
Type of "From" Line Falsity	Description
Blank	Sender's identity has been stripped from "From" line
Connotes Business Relationship	Name of sender suggests a business relationship between sender and recipient (e.g., "youraccount@vendortex.com")
Connotes Personal Relationship	Name of sender suggests a personal relationship between sender and recipient (e.g., use of first name only, which may suggest that the message is from someone in the recipient's address book.)
Message from Recipient	Sender's identifying information has been stripped from message and replaced with recipient's email address
Disguised in Other Way	Catch-all for other methods used to disguise the sender's true email address (e.g., sender, as identified in the message text, uses another person or entity's name or email address in the from line)


One-third of the spam messages contained false information in the "From" line.



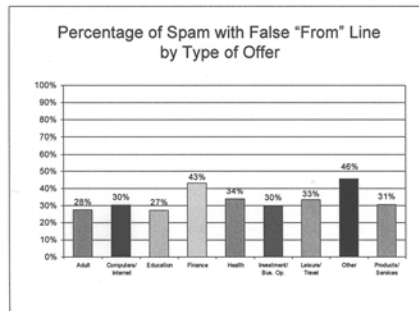
 Thirty-three percent of spam analyzed contained false information in the "From" line.


Of the messages containing indicators of falsity in the "From" line, nearly half claimed to be from someone with a personal relationship with the recipient. Such a personal relationship was typically manifested by the use of only a first name in the "From" line, suggesting that the message was coming from someone whose name was in the recipient's email address book.



 Of the spam containing false information in the "From" line, 46% suggested a personal relationship between the sender and recipient.

"From" lines with signs of falsity appeared in UCE for all types of offers, with incidence rates ranging from a low of 27.2% for education-related spam to a high of 45.8% for spam coded as "Other," and 43.1% for finance-related spam. No matter the type of offer contained in the UCE, senders of the UCE reviewed by FTC staff frequently obscured their identity by manipulating the information in the "From" line.



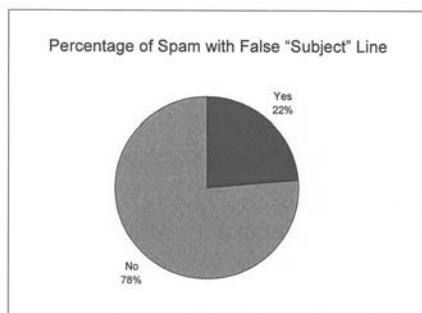
 Senders of all types of spam analyzed frequently obscure their identities in the "From" line.

IV. FALSITY IN "SUBJECT" LINE

FTC staff examined the "Subject" line in each spam message in the sample to determine whether the information appeared to be false. "Subject" lines were analyzed to determine whether they contained any of the following characteristics:

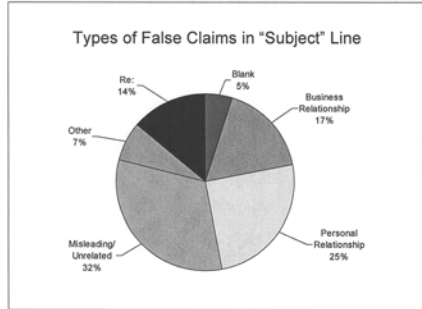
Type of Subject Line Falsity	Description
Blank	Contains no information about the subject of the message
Connotes Business Relationship	Suggests existence of business relationship between sender and recipient (e.g., "your order's status")
Connotes Personal Relationship	Suggests existence of personal relationship between sender and recipient (e.g., "Bob says 'hi'")
Unrelated to Content of Message	Content of message differs from description in "Subject" line
Re:	Suggests that the message is in reply to a message previously sent by recipient
Other	Catch-all for other methods used to disguise the true content of the message (e.g., "Subject" line indicates that the message is "extremely urgent.")

Twenty-two percent of UCE in the sample contained false information in the "Subject" line.

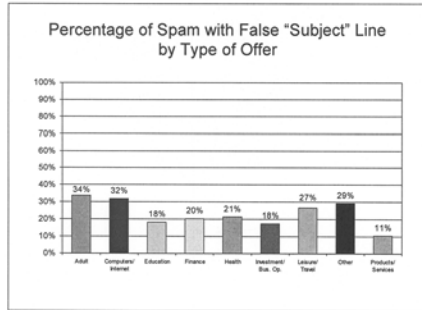



✉ **Twenty-two percent of spam analyzed contained false information in the "Subject" line.**


Of the spam containing signs of falsity in their "Subject" lines, nearly one-third contained a "Subject" line that bore no relationship to the content of the message. These false "Subject" lines were designed to lure consumers into opening the messages, expecting to see content related to the representations in the "Subject" lines. Forty-two percent of the spam containing false "Subject" lines misrepresented that the sender had a personal or business relationship with the recipient.



While false "Subject" lines were found in all types of offers, over one-third of "adult" offers appeared to misrepresent the content of the message.

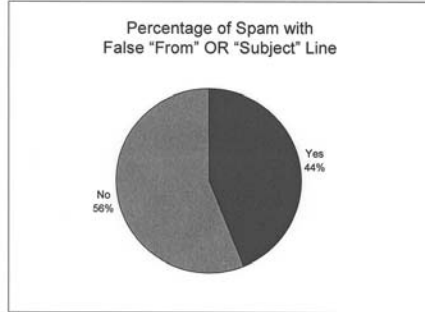


 **Forty-two percent of spam containing misleading "Subject" lines misrepresented that the sender had a personal or business relationship with the recipient.**

 **One in every three "adult" spam messages reviewed by the FTC contained false information in the "Subject" line.**

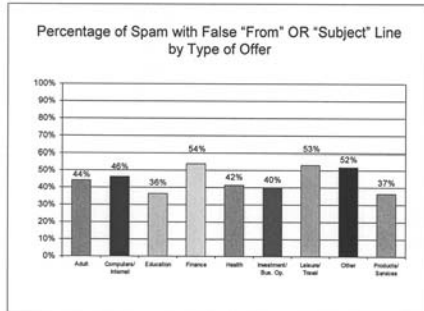
V. FALSITY IN "FROM" OR "SUBJECT" LINES

Forty-four percent of spam analyzed by FTC staff contained hallmarks of falsity in either the "From" line or "Subject" line.



✉ Forty-four percent of spam reviewed by FTC staff contained false information in the "From" or "Subject" lines.

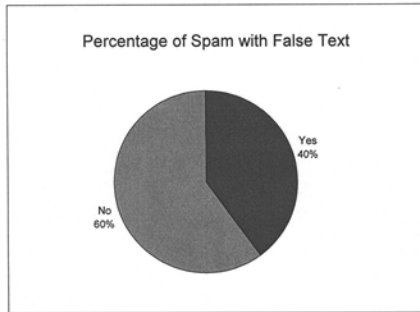
All types of spam in the sample analyzed by FTC staff contained indicators of falsity in the "From" or "Subject" line, with incidence rates ranging from a low of 36.4% for education-related UCE to a high of 53.9% for finance-related spam.



✉ Over half of finance-related spam analyzed by the FTC contained false "From" or "Subject" lines.

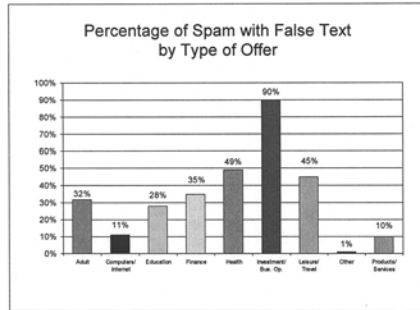
VI. FALSITY IN MESSAGE TEXT

Using expertise gleaned from past law enforcement actions and its own research, FTC staff identified specific representations that were likely to be false. Staff then analyzed each spam message in the sample to determine whether its text bore any of the enumerated hallmarks of falsity. Approximately 40% of the messages had at least one indication of falsity.



Forty percent of spam studied contained signs of falsity in the body of the message.


The incidence of likely false claims in the text of spam varied considerably among types of offers. Ninety percent of UCE in the sample that advertised investment and business opportunities contained signs of falsity.



Ninety percent of spam concerning investment and business opportunity offers analyzed by the FTC contained likely false claims.

Many of the Investment/Business Opportunity messages analyzed for this study could be categorized as “chain letter” messages, and many others advertised some other form of “effortless income.”

Spotlight on:



“Chain Letter” Spam

What the “chain letters” say:

- “Read on. It’s true. Every word of it. It is legal. I checked.”

What to watch out for:

- Chain letters may try to win your confidence by claiming that they’re legal, and even that they’re endorsed by the government. Nothing is further from the truth.

Other topics generating a significant percentage of messages with indicators of falsity included those involving health (48%) and leisure/travel (47%). Common “health” spam messages advertised weight loss products and intimacy aids; common “leisure/travel” spam messages offered prize and vacation promotions.

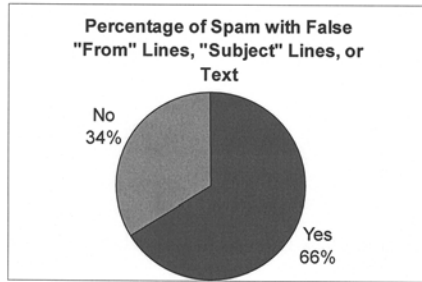
VII. FALSITY IN “FROM” LINE, “SUBJECT” LINE,

 **Chain letter and effortless income offers are frequently marketed through UCE.**

 **Of the spam analyzed, 48% marketing healthcare products and 47% marketing travel or leisure products contained signs of falsity in the text of their messages.**

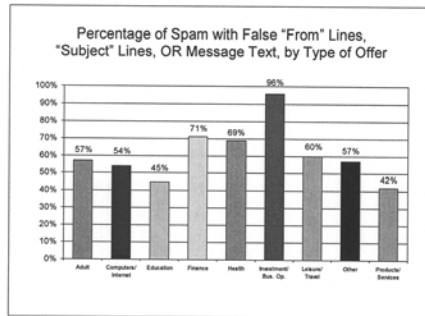
OR MESSAGE TEXT

Sixty-six percent of spam analyzed by FTC staff contained indications of falsity in their "From" lines, "Subject" lines, or message text.



Sixty-six percent of spam analyzed contained false "From" lines, "Subject" lines, or message text.

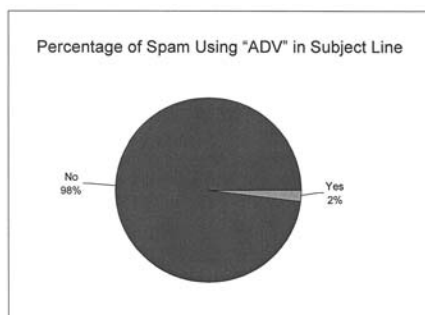
All types of spam in the sample contained indications of falsity in the "From" or "Subject" line or in the message text, with falsity rates ranging from a low of 42% for spam involving the sale of products and services to 96% for spam offering investment and business opportunities.



Ninety-six percent of spam concerning investment and business opportunities contained false "From" lines, "Subject" lines, or message text.

VIII. USE OF THE "ADV:" LABEL IN "SUBJECT" LINES OF MESSAGES STUDIED

Several states have enacted laws in recent years requiring senders of spam to begin every subject line with the phrase "ADV:" (an abbreviation used to identify advertising) in messages sent to recipients of those states. FTC staff's study of a sample of messages found that compliance with this labeling requirement was sparse.




IX. MESSAGES REQUESTING RECIPIENTS' PERSONAL INFORMATION

The spam study showed that messages rarely requested recipients to submit personal information in responding to the senders' offers. In analyzing spam regarding this feature, staff distinguished between information that is public and readily available, such as the sender's name and address, and information that is not public or is not readily available, such as the sender's bank account number. The latter type of personal information consists of data that can lead to identity theft or other monetary harm if it falls into the wrong hands; the FTC advises consumers to guard this information carefully. Only 14 of the UCE in the sample requested such personal information. Ten of these 14 messages also contained indicators of falsity in the "From" line, "Subject" line, or body of the message.

✉ **Two percent of the spam analyzed contained the "ADV" label in the subject line, which is required by several state laws.**

✉ **While relatively few spam in the study asked the recipient to submit personal information, those messages requesting such information typically contained signs of falsity.**

Spotlight on:



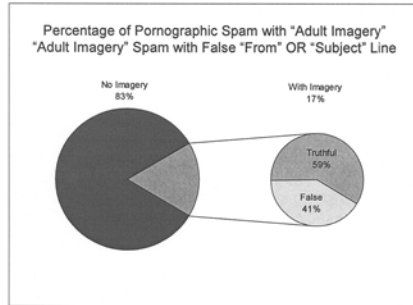
“Nigerian” Spam & Personal Information

- These messages may ask for your bank account number—purportedly so the sender can wire you millions of dollars.
- If you respond and provide your account information, you will receive nothing—and the sender will have access to funds in that account.

X. USE OF ADULT IMAGERY IN OFFERS FOR PORNOGRAPHY

Consumers and lawmakers have repeatedly expressed concern over sexually explicit images contained in spam, principally because the images may be accessible to children. To help determine the scope of this issue, FTC staff analyzed the prevalence of pornographic imagery in the Harvest Database and the database of spam received in FTC employees’ inboxes. (Because many consumers who forwarded their spam to the UCE Database did not send the spam in an HTML-enabled format, the UCE Database sub-sample was excluded from this particular analysis). A message was considered to have “adult imagery” if the image appeared automatically (without requiring the consumer to hyperlink to a web page) and the image contained nudity.

Seventeen percent of pornographic offers in the spam analyzed by FTC staff contained "adult imagery." Over 40% of these pornographic spam messages contained false statements in their "From" or "Subject" lines, making it more likely that recipients would open the messages without knowing that pornographic images will appear.



XI. METHODOLOGY

For this study, FTC staff analyzed UCE from three sources – the UCE Database (approximately 450 sample messages), the Harvest Database (approximately 450 sample messages), and spam received in official FTC inboxes (approximately 100 sample messages). The UCE Database and Harvest Database samples were drawn from messages received during the last six months of 2002. The UCE messages were collected for this study using random selection protocols established by the FTC Bureau of Economics. To enable future internal analysis of spam not blocked by the FTC's internal computer systems, the data sample was supplemented with 100 pieces of randomly-selected UCE received by FTC employees during March 2003.

The UCE Database contains spam forwarded to the Commission by members of the public. Consumers currently contribute about 130,000 messages per day to the UCE Database, and a total of 11,184,139 messages were forwarded to the FTC's UCE Database during the time period from which the study's sample was drawn. The volume of messages in the UCE Database makes it likely that this data source provides a fairly representative look at the

✉ **Seventeen percent of spam advertising pornographic websites included "adult images" in the body of the message.**

✉ **Forty-one percent of spam containing "adult imagery" contained false information in their "From" or "Subject" lines.**

types of messages that many consumers receive. Nonetheless, the email in the database may be skewed because contributors are likely to be knowledgeable about spam or have a dismal view of UCE.

The Harvest Database consists of 3,651 messages received by FTC undercover email accounts that were established as part of its email harvesting study. As part of the Harvest study, the FTC and its law enforcement partners established 250 email accounts and posted these email addresses to 175 different locations on the Internet. Specific email addresses were posted on newsgroups, message boards, chat rooms, instant messaging services, email service directories, web pages, domain name "whois" information, online resume services, and online dating services. FTC staff then tracked email received by each of the 250 email accounts.

While spam contained in the Harvest Database does not suffer from the same potential "contributor" biases as the UCE Database, it may not be fairly representative of the range of spam offers that consumers receive. The database contains messages sent by marketers who use harvesting programs to obtain email addresses. Many marketers eschew using harvesting programs and obtain email address lists in other fashions.

The internal FTC spam database may suffer from the same potential biases as the UCE Database. Commission staff voluntarily contributed the spam they received in their FTC inboxes for analyses. Contributors may be those employees most annoyed with spam. Moreover, the FTC employs email filtering mechanisms that likely affect the representativeness of this sample.

To overcome the potential biases in each of these data sets, the data was combined into a single database. The study's results provide a snapshot of approximately 1,000 pieces of spam drawn from a variety of sources available to FTC staff. It is unknown whether a random sample of all spam sent in the stream of commerce would yield the same findings.

XII. CONCLUSION

This study represents a snapshot of spam, as viewed through random samples of three data sets available to FTC staff. Because all vehicles of commerce, including spam, are in constant motion, this snapshot may not provide a complete picture of the incidence of false claims in spam.

Reviewing this snapshot, FTC staff found that UCE for Investment/Business Opportunity, Financial, and Adult offers accounted for over half of all messages. When analyzing the prevalence of false claims, FTC staff found indicators of falsity in the "From" lines, "Subject" lines, or content of two-

thirds of the messages. Furthermore, this study found that the use of the "adv" (advertising) label by senders of spam was almost non-existent. Finally, the study found that 41% of spam depicting nudity contained indicators of falsity in their "From" or "Subject" lines.

Future studies should be designed to identify changes in the types of offers being made through spam and the frequency of signs of falsity appearing in the "From" lines, "Subject" lines, and content of UCE.

Mr. SWINDLE. Third, the sheer volume of spam, coupled with its capacity to transmit viruses, trojan horses and other damaging code, threatens to do major damage to the Internet and our critical infrastructure.

Fourth, there is no easy solution. No one silver bullet that will solve the problem. Solutions must be pursued from many directions. These concerns represent enormous cost to businesses, the economy, consumers, and society.

Two specific problems demand attention by policymakers and industry leaders. First, there is the complex combination of technology, market forces, and public policy that will be evolving for years to come. The second problem is one that I characterize as being heavily influenced by the emotions of consumers, small businesses, and home users by the millions who are literally fed up with spam. I am concerned that spam is about to kill the killer app of the Internet, specifically consumer use of e-mail and E-commerce. If consumers lose confidence in web-based services and turn away, tremendous harm will be done to the economic potential of information technology. Solving these problems will require innovation, resources, and time.

However, dealing with the emotional reaction to spam by millions of users will demand immediate attention before it gets out of hand. Internet service providers, software manufacturers, and those engaged in designing operating systems must empower consumers with better control over their incoming e-mail. Easing the spam burden on consumers would help to shore up trust and confidence.

Surely consumer empowerment is possible today. Why has industry not solved this problem? Frankly, to date I am not convinced that industry has made the commitment or really wants to empower consumers by giving them easy-to-use tools for personal control.

I read a book last summer, *Tuxedo Park*, by Jennet Conant, a fascinating account of Alfred Loomis, a wealthy financier from the 1920s. He funded a private research laboratory at his Tuxedo Park estate, attracting the greatest scientists of the day. They were instrumental in the rapid development of radar, which enabled us to keep the supply lines open to England in early World War II. Wartime crisis demanded that creative minds quickly find technical solutions to complex problems. Loomis and his friends were up to the task. It occurs to me that we have a crisis today. We must avoid major setbacks to the potential of information technology. We need great minds to quickly find solutions to spam. Empowering consumers would be a good first step. Is industry motivated to do the right thing, and do it now?

The FTC's law enforcement efforts against spam are aggressive, but finding the guilty parties is resource-intensive and a difficult technical challenge. We give consumer education high priority at the commission. Our information security website and private sector partnerships continue to expand our reach. Recently, we released findings from three studies to better understand the magnitude of the spam problem, how spam is proliferated, and how consumers and users are victimized.

Our recent 3-day spam forum aimed to better inform the dialogue and find the best possible solutions to the spam problem. The forum was remarkable in its discussions and participation, over 400 participants and some 80 or so panelists. I would like to share some of the forum's revelations, as well as some personal observations about the realities of spam. First and foremost, the private sector must lead the way to finding the solution. We likely will not find the perfect solution. The target will be constantly moving as technology evolves. More laws are not necessarily the right answer.

I heard little universal enthusiasm from participants for currently proposed legislation. Laws bestowing competitive advantage to larger firms over smaller firms are questionable. Unenforceable laws will have little real effect. Overreaching laws will have unintended adverse consequences. Passing legislation to mandate best practices for the good actors will not help us track down the bad actors engaged in fraud and deception. We must work together.

Consumers, users, and civil society organizations must be a part of our continuing dialogue to find solutions. Awareness and safe computing practices by all participants are essential, and developing a culture of security where all participants work to minimize our many vulnerabilities is an imperative, not an alternative. Our efforts to solve the spam problem and secure our information systems and networks is not a destination. We are embarked upon a journey.

I thank you, Mr. Chairman.

[The prepared statement of Mr. Swindle follows:]

PREPARED STATEMENT OF HON. ORSON SWINDLE, COMMISSIONER,
FEDERAL TRADE COMMISSION

Thank you Mr. Chairman and members of the Committee for this timely discussion of SPAM and the threat it poses to the potential benefits of information technology.

Consumers must have trust, confidence and comfort with technology and its uses, particularly when it comes to their privacy and the security of personal and sensitive information.

SPAM undermines consumer trust and confidence. It represents a significant and rapidly growing threat to web-based services. The Commission's prepared testimony provides the Committee with an excellent overview of our efforts to combat SPAM.

What is SPAM? The FTC defines unwanted and unsolicited SPAM as "any commercial electronic mail message that is sent-typically in bulk-to consumers without the consumers prior request or consent."

There are at least four major concerns caused by SPAM.

First, the volume is increasing at astonishing rates, current estimates indicate at least 40 percent of all e-mail is SPAM.

Second, recent studies by the FTC indicate that SPAM has become the weapon of choice of those engaged in fraud and deception. Nearly 66 percent of the SPAM we examined appeared to contain falsity and deception. I would ask our False Claims in Spam report be included as part of the record.

Third, the sheer volume of SPAM—coupled with its capacity to transmit viruses, trojan horses, and other damaging code—threatens to do major damage to the Internet and our critical infrastructure and the Internet.

Fourth, there is no easy solution—no one silver bullet that will solve the problem. Solutions must be pursued from many directions.

These concerns represent enormous costs to businesses, the economy, consumers and society.

Two specific problems demand attention by policy makers and industry leaders. First, there is the complex combination of technology, market forces and public policy that will be evolving for years to come. The second problem is one that I characterize as heavily influenced by the emotions of consumers, small—businesses and home users by the millions who are literally fed up with SPAM.

I am concerned that SPAM is about to kill the “killer app” of the Internet—specifically—consumer use of e-mail and e-commerce. If consumers lose confidence in web-based services and turn away, tremendous harm will be done to the economic potential of information technology.

Solving these problems will require innovation, resources and time. However, dealing with the emotional reaction to SPAM by millions of users, demands immediate attention before it gets out of hand.

Internet service providers, software manufacturers, and those engaged in designing operating systems must empower consumers with better control over their incoming e-mail. Easing the SPAM burden on consumers would help to shore up trust and confidence. Surely, consumer empowerment is possible today. Why has industry not solved this problem?

Frankly, to date, *I am* not convinced that industry has made the commitment or really wants to empower consumers by giving them easy-to-use tools for personal control.

I read a book last summer, *Tuxedo Park*, by Jennet Conant—a fascinating account of Alfred Loomis, wealthy financier from the 1920s. He funded a private research laboratory at his Tuxedo Park estate, attracting the great scientists of his day. They were instrumental in the accelerated development of radar which enabled us to keep supply lines open to England early in WWII. War time crisis demanded that creative minds quickly find technical solutions to complex problems. Loomis and friends were up to the task.

It occurs to me that we have a crisis *today*—we must avoid major set backs to the potential of information technology. We need great minds to quickly find solutions to SPAM. Empowering consumers would be a good first step. Is industry motivated to do the right thing and do it now?

The FTC’s law enforcement efforts against SPAM are intensifying, but finding the guilty parties is resource intensive and a difficult technical challenge.

We give consumer education high priority at the Commission. Our information Security website and private sector partnerships continue to expand our reach.

Recently, we released findings from three studies to better understand the magnitude of the SPAM problem, how SPAM is proliferated, and how consumers and users are victimized.

Our recent three-day SPAM Forum aimed to better inform the dialogue and find the best possible solutions to the SPAM problem. The Forum was remarkable in its discussions and participation—over 400 participants and 80 panelists.

I would like to share some of the Forum’s revelations—as well as some personal observations—about the realities of SPAM.

First and most essential—the private sector must lead the way!

We likely will not find the perfect solution. The target will be constantly moving as technology evolves.

More laws are *not necessarily* the right answer.

I heard *little* universal enthusiasm from participants for currently proposed legislation.

Laws bestowing competitive advantage to larger firms over smaller competitors are questionable.

Unenforceable laws will have little real effect: Overreaching laws will have unintended adverse consequences.

Passing legislation to mandate best practices for “good actors” will not help us track down the “bad actors” engaged in fraud and deception.

We must work together. Consumers, users, and civil society organizations also must be a part of our continuing dialogue to find solutions.

Awareness and safe computing practices by all participants are essential.

Developing a culture of security where all participants work to minimize our many vulnerabilities is an imperative, not an alternative.

Our efforts to solve the SPAM problem and secure our information systems and networks is not a destination—we are embarked upon a journey!

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you.

Commissioner Thompson, welcome.

**STATEMENT OF HON. MOZELLE W. THOMPSON,
COMMISSIONER, FEDERAL TRADE COMMISSION**

Mr. THOMPSON. Thank you, Mr. Chairman. I thank you for this opportunity to appear before you today and talk about the issue of

spam, bulk unsolicited commercial e-mail. At the outset, I would like to praise this Committee and its Members for holding this hearing and the work that it has done over the years to focus attention on this important subject. Spam is a complex issue that resonates with consumers, businesses, and Governments alike. The FTC, along with Members of this Committee, have been interested in this issue for a long time.

In 2001, the Committee asked this Commission's views on the CAN-SPAM Act, S. 630, sponsored by Senators Burns and Wyden. At that time, we unanimously supported the bill, stating the Commission generally favors the underlying goal of the legislation, and as set forth in our written testimony submitted today, the FTC has already brought over 50 cases against deceptive and fraudulent spam. While these cases are important, they focus on only one aspect, fraud and deception, of what has grown to be a much larger problem. For this reason, 3 weeks ago, the Commission held a 3-day workshop to get a better insight on the problem of spam.

My observation is that it was a unique event. It was a unique week. It is not every day that an FTC workshop draws over 400 attendees for 3 days to pose questions to 87 panelists representing a wide perspective on one issue. At the same time, three of America's largest ISPs announced a voluntary business initiative and three new legislative proposals were introduced, and there have been more since then.

In addition, representatives from numerous countries, including Australia, Canada, Japan, and the European Union, also attended and participated in those discussions. We are just beginning to digest all of this information, so we have not reached conclusions about how this information may affect our views, but like Commissioner Swindle, I would like to share at least some of my observations.

One key lesson we learned from our spam workshop is the scope of the spam problem appears to have changed significantly. It is no longer simply a matter of consumer annoyance at receiving unwanted e-mail. We have some very significant problems. First, that through fraud and deception across international borders, there is an undermining of consumer confidence, as shown by this chart here, that how much of the spam has falsity in its face.

Second, that it threatens business, because the volume of e-mail places a choke-hold on E-commerce. It was the first time I had actually heard a large group of witnesses claim that spam constitutes a threat to the future of the Internet, and you can just see from this chart the growth from 8 percent to 45 percent this year, and projected to 2007, that it could constitute up to 70 percent of e-mail.

Finally, we heard a lot about areas that Commissioner Swindle has worked in, talking about security issues, including spam used to spread viruses, and the very disruption of service caused by volume that could impact the activities of consumers, businesses, and Governments on the Internet. What that tells me is that the problem of spam has become broader. It has evolved, and the scope of possible solutions may also have to expand. Clearly, strong law enforcement is an important part of this.

To address fraud and deception, we also have to work with other countries' law enforcers for cross-border actions, and I know the Committee is aware that the FTC has submitted some legislative proposals this year to enable us to have better tools to work cooperatively with other governments to root out fraud and deception, but there also has to be a business answer, with business initiatives and best practices that distinguishes good actors from bad, and we also want to ensure that there continues to be incentives to develop technological tools that provide consumers with means to address and manage their e-mail. Finally, there has to be strong consumer and business education to enable consumers to make better choices, and to protect themselves.

The interesting challenge for all of this is, all of it has to take place within a backdrop, or an umbrella that accommodates a desire for a timely solution, one that has ongoing flexibility, because, as was alluded to earlier, there are very clever people out there, and we have to have a mechanism to be as clever as they are, and finally, First Amendment concerns, because the Supreme Court, we know, is now considering what are the boundaries of commercial speech.

Now, I would like to conclude by saying that, to recognize the importance of what this Committee does and how we respond to spam, that as you all are aware, I spend also a lot of time internationally as Chair of the OECD Consumer Policy Committee, where we are talking about this issue and how to address it internationally. We are also talking about how to address this bilaterally.

I can tell you that, although other countries have looked at legislation, some have passed it, they have tried various enforcement tools, around the world people are looking to the United States for leadership on how we address this problem, how we can provide consumers with a good experience, how we can make this tool useful to businesses and consumers alike and still provide a free flow of information. It is an interesting challenge for us, but I am sure it is one the Committee is well-equipped to meet.

Thank you.

[The prepared statement of Mr. Thompson follows:]

PREPARED STATEMENT OF THE FEDERAL TRADE COMMISSION

Mr. Chairman, the Federal Trade Commission appreciates this opportunity to provide information to the Committee on the FTC's efforts to address the problems that result from bulk unsolicited commercial e-mail. This statement discusses the Commission's law enforcement efforts against spam, describes our efforts to educate consumers and businesses about the problem of spam, and focuses particularly on the Commission's recent Spam Forum and several studies on the subject that the Commission's staff has undertaken in recent months.¹

As the Federal Government's principal consumer protection agency, the FTC's mission is to promote the efficient functioning of the marketplace by acting against unfair or deceptive acts or practices and increasing consumer choice by promoting vigorous competition. To fulfill this mission, the Commission enforces the Federal Trade Commission Act, which prohibits unfair methods of competition and unfair

¹The views expressed in this statement represent the views of the Commission. Commissioners' oral statements and responses to any questions you may have represent their own views, and not necessarily the views of the Commission or any other Commissioner.

or deceptive acts or practices in or affecting commerce.² Commerce on the Internet, including unsolicited commercial e-mail, falls within the scope of this statutory mandate.

Unsolicited commercial e-mail (“UCE” or “spam”) is any commercial electronic mail message that is sent—typically in bulk—to consumers without the consumers’ prior request or consent. The extreme speed, anonymity and negligible cost of sending spam differentiate it from other forms of unsolicited marketing, such as direct mail or telemarketing. Those marketing techniques, unlike spam, impose costs on marketers that limit their use.

There are two basic problems with spam. First, deception and fraud appear to characterize the vast majority of spam. Indeed, spam appears to be the vehicle of choice for many fraudulent and deceptive marketers. Second, a serious Internet infrastructure problem flows from the sheer volume of spam that is now being sent. Spam, even if not deceptive, may lead to significant disruptions and inefficiencies in Internet services, and may constitute a significant problem for consumers and businesses using the Internet. In addition, spam can spread viruses that wreck havoc for computer users. These problems together pose a threat to consumers’ confidence in the Internet as a medium for electronic commerce.

Virtually all of the panelists at the Commission’s recent Spam Forum, described in more detail below, opined that the volume of unsolicited e-mail is increasing exponentially and that we are at a “tipping point,” requiring some action to avert deep erosion of public confidence in e-mail that could hinder, or even destroy, it as a tool for communication and online commerce. In other words, as some have expressed it, spam is “killing the killer ap.” The consensus of all participants in the workshop was that a solution to the spam problem is critically important, but cannot be found overnight. There is no quick or simple “silver bullet.” Rather, solutions must be pursued from many directions—technological, legal, and consumer action. The Forum helped to suggest paths to follow toward solutions to the spam problems. These solutions will depend on cooperative efforts between government and the private sector. In fact, the Forum is only the most recent example of the FTC’s role as convener, facilitator, and catalyst to encourage that activity. But the Commission also plays another important role—that of law enforcer.

The Commission has pursued a vigorous law enforcement program against deceptive spam, and to date has brought 53 cases in which spam was an integral element of the alleged overall deceptive or unfair practice.³ Most of those cases focused on the deceptive content of the spam message, alleging that the various defendants violated Section 5 of the FTC Act through misrepresentations in the body of the message.⁴ More recently, the Commission has expanded the scope of its allegations to encompass not just the content of the spam but also the *manner* in which the spam is sent. Thus, *FTC v. G. M. Funding*,⁵ and *F.T.C. v. Brain Westby*⁶ allege (1) that e-mail “spoofing” is an unfair practice,⁷ and (2) that failure to honor a “remove me” representation is a deceptive practice. In these cases, the defendants’ e-mail removal mechanisms did not work and consumers’ e-mailed attempts to remove themselves from defendants’ distribution lists were returned as undeliverable.

Westby is also the first FTC case to allege that a misleading subject line is deceptive because it tricks consumers into opening messages they otherwise would not open. In other cases, the Commission has alleged that the defendants falsely represented that subscribing to defendants’ service could stop spam from other sources⁸ or that purchasers of a spamming business opportunity could make substantial profits.⁹ Thus, through our law enforcement actions the Commission has attacked and will continue to attack deception and unfairness in every aspect of spam.

²The FTC has limited or no jurisdiction over specified types of entities and activities. These include banks, savings associations, and Federal credit unions; regulated common carriers; air carriers; non-retail sales of livestock and meat products under the Packers and Stockyards Act; certain activities of nonprofit corporations; and the business of insurance. *See, e.g.*, 15 U.S.C. §§ 44, 45, 46 (FTC Act); 15 U.S.C. § 21 (Clayton Act); 7 U.S.C. § 227 (Packers and Stockyards Act); 15 U.S.C. §§ 1011 *et seq.* (McCarran-Ferguson Act).

³A summary listing of these cases is attached as Appendix A.

⁴*E.g.*, *FTC v. 30 Minute Mortgage, Inc.*, No. 03-60021 (S.D. Fla. filed Jan. 9, 2003).

⁵No. SACV 02-1026 DOC (C.D. Cal. filed Nov. 2002).

⁶No. 032-3030 (N.D. Ill. filed Apr. 15, 2003).

⁷“Spoofing” involves forging the “from” or “reply to” lines in an e-mail to make it appear that the e-mail was sent from an innocent third-party. The third party then receives bounced-back undeliverable messages and angry “do not spam me” complaints.

⁸*FTC v. NetSource One*, No. 022-3077 (W.D. Ky. filed Nov. 2, 2002).

⁹*FTC v. Cyber Data*, No. CV 02-2120 LKK (E.D. Cal. filed Oct. 2002); *FTC v. Internet Specialists*, No. 302 CV 01722 RNC (D.Conn. filed Oct. 2002).

Experience in these cases shows that the primary law enforcement challenges are to identify and locate the targeted spammer. Of course, finding the wrongdoers is an important aspect of all law enforcement actions, but in spam cases it is a particularly daunting task. Spammers can easily hide their identity, forge the electronic path of their e-mail messages, or send their messages from anywhere in the world to anyone in the world. Tracking down a targeted spammer typically requires an unusually large commitment of staff time and resources, and rarely can it be known in advance whether the target's operation is large enough or injurious enough to consumers to justify the resource commitment.

To complement its law enforcement efforts, the Commission endeavors to educate consumers and businesses on ways they can reduce the amount of unwanted spam they receive, and about particular types of scams commonly disseminated through spam, such as illegal chain letters and "Nigerian" scams.¹⁰ These materials are available on the FTC's spam website, www.ftc.gov/spam.

Another aspect of the Commission's approach to spam is to investigate and research the problems it poses to understand them better. Through this research, the Commission can refine and better focus its law enforcement and consumer and business education efforts.

Studying the Spam Problem

The Commission has engaged in several research projects to explore how spam affects consumers and online commerce. These projects include a "Remove Me" surf, a "spam Harvest," and a study of False Claims in Spam.

The "Remove Me" Surf

Last year the Commission announced the results of the "Remove Me" surf, in which the FTC and law enforcement partners tested whether spammers were honoring the "remove me" or "unsubscribe" options in spam.¹¹ From e-mail that participating agencies had forwarded to the FTC's spam database, the Commission's staff selected more than 200 messages that purported to allow recipients to remove their names from a spam list. The agencies set up dummy e-mail accounts to test the pledges. We found that 63 percent of the removal links and addresses in our sample did not function. If a return address does not work to receive return messages, it is unlikely that it could be used to collect valid e-mail addresses for use in future spamming. This finding tends to disprove the common belief that responding to spam guarantees that you will receive more of it.

The "Spam Harvest"

In its "Spam Harvest," the Commission's staff conducted an examination of what online activities place consumers at risk for receiving spam. The examination discovered that one hundred percent of the e-mail addresses posted in chat rooms received spam; one received spam only eight minutes after the address was posted. Eighty-six percent of the e-mail addresses posted at newsgroups and Web pages received spam, as did 50 percent of addresses at free personal Web page services, 27 percent from message board postings, and 9 percent of e-mail service directories. The "Spam Harvest" also found that the type of spam received was not related to the sites where the e-mail addresses were posted. For example, e-mail addresses posted to children's newsgroups received a large amount of adult-content and work-at-home spam.

As part of this project, the staff developed consumer education material, including a publication, "E-mail Address Harvesting: How Spammers Reap What You Sow," that provides tips, based on the lessons learned from the Spam Harvest, to consumers who want to minimize their risk of receiving spam. The tips advise, among other things, that consumers can minimize the chances of their addresses being harvested by using at least two e-mail addresses—one for use on websites, newsgroups and other public venues on the web, and another e-mail address solely for personal

¹⁰ Claiming to be well-placed Nigerians, con artists offer to transfer millions of dollars into the prospective victim's bank account in exchange for a small fee. Those who respond to the initial offer may receive official-looking documents. Typically, the victim is then asked to provide blank letterhead and his or her bank account numbers, as well as some money to cover transaction and transfer costs and attorney's fees.

¹¹ The "Remove-Me" surf was conducted as part of International Netforce, an enforcement sweep in which the FTC was joined by the Alaska Attorney General, the Alaska State Troopers, Government Services of the Province of Alberta, the British Columbia Securities Commission, the British Columbia Solicitor General, the Canadian Competition Bureau, the Idaho Attorney General, the Montana Department of Administration, the Oregon Department of Justice, the Washington Attorney General, the Washington State Department of Financial Institutions, and the Wyoming Attorney General.

communication. Another suggested strategy to reduce spam is “masking” (disguising) e-mail addresses posted in public.¹²

The “False Claims in Spam” Study

An additional FTC staff study examined false claims in spam. The staff examined 1,000 spam messages selected randomly from three sources: our spam database of consumer-forwarded messages, the spam received at the addresses used in the Spam Harvest, and spam that reached FTC employee computers. The staff analyzed the messages based upon the types of products or services offered, the indicia of deception in the content of the messages, and the indicia of deception in the “from” and “subject” lines of the messages.

The Types of Products or Services Offered—The staff found that 20 percent of the spam contained offers for investment or business opportunities, which include such things as work-at-home offers, franchise opportunities, or offers for securities. Another 18 percent of the spam offered adult-oriented products or services. Of those adult messages, about one-fifth included images of nudity that appeared automatically in the body of the message. Further, 17 percent of the spam messages involved finance, including credit cards, mortgages, refinancing, and insurance. All together, the investment/business opportunity, adult, and finance offers comprised 55 percent of our sample.

Indicia of Falsity in the Content of Spam Messages—The staff also determined how many spam messages appeared misleading. Using expertise gleaned from past law enforcement actions and recent research efforts, the staff identified specific representations likely to be false. The staff found that 40 percent of all the combined categories of spam messages contained indicia of falsity in the body of the message. An astonishing 90 percent of the investment/business opportunity category of spam contained indicia of false claims.

Evidence of Falsity in the “From” and “Subject” Lines—The staff also looked at evidence of deception in the “from” and “subject” lines of the spam. One third of the messages contained indicia of falsity in the “from” line. Messages falling into this category included “from” lines connoting a business or personal relationship, such as using a first name only, or stating “Your Account@XYZ.COM.” Another common instance of misleading “from” lines occurs when spammers make the sender’s name the same as the recipient’s address, so it appears that one has sent the message to oneself.

In addition, the staff found that 22 percent of the spam messages contained indicia of falsity in the subject line, such as using “Re:” to indicate familiarity or a subject line that was unrelated to the content of the message, such as “Hi” or “Order Confirmation.” Over one third of adult-content spam contained false information in the subject line. Further, *only two percent* of the analyzed spam contained the label “ADV.” in the “subject” line, even though such a label is required by the laws of several states.

Conclusions of the False Claims in Spam Study—Adding up the various forms of deception, the staff found that 66 percent of the spam appeared to contain at least one form of deception.¹³ This Spam Study confirms the Commission’s earlier belief that fraud operators, who are often among the first to exploit any technological innovation, have seized on the Internet’s capacity to reach millions of consumers quickly and at a low cost through spam. Not only are fraud operators able to reach millions of individuals with one message, but they also can misuse technology to conceal their identity. The Commission believes the proliferation of fraudulent or deceptive spam on the Internet poses a threat to consumer confidence in online commerce and, therefore, views the problem of deception as a significant issue in the debate over spam.

The FTC Spam Forum

Building upon our research, education, and law enforcement efforts, the FTC held a three-day public forum from April 30 to May 2, 2003 on spam e-mail. This was a wide-ranging public examination of spam from all viewpoints. The Commission convened this event for two principal reasons. First, spam is frequently discussed, but facts about how it works, its origins, what incentives drive it, and so on, are not widely known. The Commission anticipated that the Forum would generate an

¹²Masking involves putting a word or phrase in one’s e-mail address so that it will trick a harvesting computer program, but not a person. For example, if one’s e-mail address is “johndoe@mysp.com,” one could mask it as “johndoe@spamaway.myisp.com.” Some newsgroup services or message boards won’t allow masking of e-mail addresses and some harvesting programs may be able to pick out common masks.

¹³The remaining spam messages were not necessarily truthful, but they did not contain any obvious indicia of falsity.

exchange of useful information about spam to help inform the public policy debate. This could help the Commission determine what more it might do to more effectively fulfill our consumer protection mission in this area. Second, the Commission sought to act as a potential catalyst for solutions to the spam problem. Through the Forum, the Commission brought to the table representatives from as many sides of the issue as possible to explore and encourage progress toward possible solutions to the detrimental effects of spam.

The Commission believes that the Forum advanced both goals. As described below, the panelists contributed valuable information from a variety of differing viewpoints to the public record. In addition, the Forum spurred a number of participants into cooperation and action. Most notably, on the eve of the Forum, industry leaders Microsoft, America Online, and Yahoo! announced a collaborative effort to stop spam. Moreover, several potential technological solutions to spam were announced either at or in anticipation of the Forum. The Commission intends to foster this dialogue, and, when possible, to encourage other similar positive steps on the part of industry.

The strong interest in addressing spam is shared by: consumers, Internet Service Providers (“ISPs”), law enforcement authorities, marketing services, bulk e-mail marketers, anti-spammers, and retailers and manufacturers. These interest groups were represented at the Forum by 87 different panelists collectively possessing a tremendous range of expertise, and coming from all over the globe to participate in this discussion. Distinguished representatives from the European Commission, Canada, Australia, Korea, and Japan offered their views on how spam affects their countries and how they are trying to tackle the problem. On the domestic front, panelists included prominent representatives from all sectors affected by spam, such as the president of the consumer group, the SpamCon Foundation, the president of the Direct Marketing Association, vice presidents of America Online and Microsoft, and the Washington State Attorney General. Distinguished members of Congress—Senators Burns, Wyden, and Schumer, and Representative Lofgren—also addressed Forum attendees.

The Spam Forum was organized into twelve panel discussions that were conducted over the course of three days. In addition to the 87 panelists, approximately 400 people were present each day in the audience at the FTC Conference Center, with many more individuals participating via a video link or by teleconference. Questions for the panelists were accepted from the audience and via a special e-mail address from those attending through video link or teleconferencing.

Day One of the Forum focused on the mechanics of spam. Panelists discussed in detail how spammers find e-mail addresses and how deception in the sending of spam affects consumers and online commerce. Discussions then focused upon security weaknesses that enable or facilitate spam, such as open relays¹⁴ and open proxies.¹⁵ Day Two explored the economic costs of spam. Panelists participated in an in-depth discussion of economic incentives inherent in spam and the costs of spam to marketers, ISPs, and consumers, and its effects on emerging technologies. Specifically, panelists discussed spam blacklists, e-mail marketers, and wireless spam (unsolicited text messages received via cell phone). Day Three focused on potential solutions to spam. Panelists discussed three potential avenues to a solution: legislation, litigation, and technology. Specific topics covered included: state, federal, and international legislation; civil and criminal law enforcement and private litigation against spammers; and various technological approaches.

Panelists at the Forum brought forward an enormous amount of information about spam and how it affects consumers and businesses. Several primary themes emerged from the various discussions. First, the volume of spam is increasing sharply. Many panelists reported that the rate of increase is accelerating. For example, one ISP reported that in 2002 alone it experienced a 150 percent increase in spam traffic. Second, spam imposes real costs. The panelists offered concrete information about the costs of spam to businesses and to ISPs. Specifically, ISPs reported that costs to address spam have increased dramatically over the past two

¹⁴ Open relays allow spammers to route their e-mail through servers of other organizations, thereby disguising the origin of the e-mail. Spammers identify and use other organizations’ open relays to avoid detection by the filter systems that ISPs use to protect their customers from unwanted spam. Routing spam through open relays also makes it difficult for law enforcement agencies to track down senders of fraudulent or deceptive spam.

¹⁵ A proxy server runs software that allows it to be the one machine in a network that directly interacts with the Internet. This provides the network with greater security. But if a proxy is not configured properly (*i.e.*, if it is an “open proxy”), it also may allow unauthorized users to pass through the site and connect to other hosts on the Internet. For example, a spammer can use an open proxy to connect to a mail server. If the server has an open mail relay, the spammer can send a large amount of spam and then disconnect—all anonymously.

years. ISPs bear the cost of servers and bandwidth necessary to channel the flood of spam, even that part of the flood that is being filtered out before reaching recipients' mail boxes. America Online reported that it recently blocked an astonishing 2.37 billion pieces of spam in a single day. Third, spam is an international problem. According to our international panelists, most of the spam received in their countries is in English and advertises American products or companies. Most panelists agreed that any solution to stopping spam will have to involve an international effort.

Our law enforcement experience has taught that the path from a fraudulent spammer to a consumer's in-box typically crosses at least one international border and frequently several. Thus, fraudulent spam exemplifies the growing problem of cross-border fraud. To enhance our effectiveness in the fight against fraudulent spam and other kinds of fraudulent schemes that cross international borders, the Commission will be asking this Committee, as part of our forthcoming reauthorization testimony, for additional legislative authority in a number of areas, including measures that would: allow the agency to share such information on targeted schemes with our overseas counterparts; provide investigative assistance to them in appropriate cases; improve our ability to obtain information from U.S. criminal agencies and Federal financial regulators, who are often investigating the same types of fraudulent conduct that we are; and improve the agency's ability to obtain consumer redress in cross-border cases by clarifying the Commission's authority to take action in such cases, and by expanding the agency's ability to use foreign counsel to pursue assets offshore. Legislation expanding the Commission's authority in these ways is essential to improve the agency's ability to fight fraudulent spam in particular, as well as other manifestations of the more general problem of cross-border fraud.

Approaches to Solving the Spam Problem

The broad themes that emerged from the Forum panel discussions depict the spam problem as increasing volume, increasing costs, and increasing international effects. This confirms that finding solutions to the problems posed by spam will not be quick or easy; moreover, the consensus of panelists was that no single approach will likely cure the problem. Some panelists at the Forum stated that a large scale technological change in the e-mail protocol system is not likely to occur. Nevertheless, others indicated that there are incremental technical changes that can be grafted onto the existing e-mail protocol to ease the burden of unwanted e-mail on ISPs and consumers. In addition, consumer representatives stressed that any solution should include consumer empowerment—to allow e-mail recipients to decide what messages they want to receive in their inbox, and to give recipients the technical tools to effectuate those decisions. Some panelists, but by no means all, advocated additional Federal legislation and law enforcement efforts as a means to provide needed accountability and deterrence.

All Spam Forum participants agreed that solving the problem of bulk unsolicited commercial e-mail will likely necessitate an integrated effort involving a variety of technological, legal, and consumer action, rather than one single solution. Through the Forum and the follow-up efforts it suggested, the Commission hopes to act as a catalyst for technologists, industry, law enforcement, and policy officials to work together to find a solution.

Conclusion

E-mail provides enormous benefits to consumers and businesses as a communication tool. The increasing volume of spam to ISPs, to businesses, and to consumers, coupled with the use of spam as a means to perpetrate fraud and deception put these benefits at serious risk. The Commission looks forward to continuing its research, education, and law enforcement efforts to protect consumers and businesses from the current onslaught of unwanted messages.

The Commission appreciates this opportunity to describe its efforts to address the problem of spam, and the outcome of its recent Spam Forum.

The CHAIRMAN. I thank you both. I have gotten letters, as I mentioned, I would include for the record from the Center for Democracy and Technology, Mr. Jerry Berman. He says, based on our research and further discussion, CDT believes that the spam problem merits targeted Federal legislation to help alleviate the burden spam causes to consumers, businesses, and ISPs, and I also had a letter from Mr. Gates which I think Mr. Leonsis is going to talk

about more, where he makes several recommendations. I would like for both of you, if you would, to comment on these recommendations, perhaps in writing to us, because there is a series of them, as to your views as to whether they should be included in the legislation or not.

I would hope, and I know that Senator Burns and Senator Wyden would hope that we could get this issue to the floor sometime before the summer recess, because it is clearly an issue that needs to be addressed one way or the other, so I would hope that you would get us that.

I guess my first question is, suppose that we enacted the best law that took care of every problem, every loophole—

We have 5 minutes left on the vote, Conrad. Do you want to go and vote and then come back?

Senator BURNS. We are voting again?

[Laughter.]

The CHAIRMAN. I think so. Maybe you want to go and then come back so we can keep the hearing going.

And what do you do about somebody located, and you have an international agreement with the major countries in the world, somebody located in the Grand Caymans, as is the case with Internet gambling sites today. What is the answer?

Mr. SWINDLE. Senator, I will start off. Obviously, and it has been said by, I think, everyone who has testified to this point, that no single solution, no single thing is going to be the solution. Passing legislation is not going to solve this problem.

Someone said earlier that having legislation penalties would help us hunt down the perpetrators, and that got right to the point here. The penalties are not going to help us hunt down the perpetrators. In fact, the biggest problem we have is finding those who are sending the spam out. It is a technical problem that from my observation, listening to the forum we had last week, most of the people in technology were saying we do not yet know how to do this. We have got a lot of work to do.

Laws can certainly classify a certain group of people who do certain things as criminals if we want to go that far and say that if we catch them, we penalize them heavily, and that might be a good idea as Senator Nelson was proposing, but the problem still remains finding them, and until we solve that problem, we have got to seek other alternatives.

I speak of the emotion of the broad base of users, hundreds of millions, certainly in this country, and I have been told the numbers may reach 600 million by the end of this year worldwide. It seems to me that it would be practical, and I am not much on technology, but if you would give me the ability to put a screen in front of my computer so that nothing comes in there except what is on that screen—in other words, my address book—you would go a long way to solving my emotional problem with spam, my frustration with it, my wanting to just turn this thing off and walk away from it. That will be the biggest disaster we can imagine right now.

Some of this technical stuff is going to take years to evolve, the same way with the legislation, but give the consumer the power, empower the consumer to say no to what is coming into his mailbox, and as I mentioned in my comments, I am not sure that indus-

try is prepared, and not because they cannot do it, but I am not sure they are prepared to do it because they do not want to do it, because it cuts them off from a potential customer. Well, I think that is dead wrong. We have an issue before us that can do grave damage to this incredible tool that we have. I think we all need to quit speaking and lobbying in terms of special interest, our own interest, and think about a cause greater than ourselves. We have a bigger issue here.

The CHAIRMAN. Commissioner Thompson.

Mr. THOMPSON. I think you highlight a very important point that we have to do what we can to eliminate jurisdictions of convenience, in other words, places that might serve as safe harbors for those who would engage in spamming. It is something we have discussed internationally.

Countries have different ways of approaching that, and we are trying to talk to them about what has been effective, what has not been effective, what are ways that we can look at in the future. I believe that some legislative vehicle is helpful, but it is not the only solution, but it also means a cooperative effort, and not just waiting for an international treaty, although that can be a long-term goal.

There is a short-term goal of having ongoing discussions, including bilateral agreements and understandings about how you actually prosecute cases that have fraud and deception at their core, and that includes what legislation we need to streamline the process so that we can share information with entities that have the same goals as we do.

I think what is important is for us at the very least to come an understanding with countries about why this issue is a problem and is a threat to the Internet, and a threat to consumer confidence. I think we are reaching those goals, and to talk about what are the potential avenues for solution. I think we are at that point, and it is a very important point.

The CHAIRMAN. Commissioner Swindle, would a do-not-spam list be an effective way of cutting down on some of this problem?

Mr. SWINDLE. In a word, I do not believe so. We are just now coming to grips with how we are going to implement a do-not-call list. In the business of telemarketing, there is a relatively finite or small number of telemarketers. There are 5,000 or 10,000. I am not sure how many there are, but when you talk about the Internet, we are talking millions. We are talking in telemarketing a very regulated industry that literally does have borders, state control of telecommunications and so forth. In the Internet, it is totally borderless.

I tried to imagine what the database for a telemarketing sales rule or do-not-call rule will be, and it will be large, because it is probably one of the more popular things that have come down the pike since I have been there. How we manage that, how we make it reactive, that it does what it is supposed to do, is a very complex problem, and we are going to get there, but we are not there yet. We have no experience, not ruling it out.

The CHAIRMAN. Do you agree?

Mr. THOMPSON. I agree. I also think there are challenges in terms of resources, because the scale and the size of what is going

to be contained in any database and the security that is going to be necessary will be very resource-intensive. I think it can be part of a solution, but in and of itself it may not be a solution.

The CHAIRMAN. Senator Nelson, I have got to go vote.

Senator NELSON. Mr. Chairman, do you want me to keep the testimony going or wait until you return?

The CHAIRMAN. Knowing you, I am sure that is not a problem. [Laughter.]

Senator NELSON. That is an appropriate reconfirmation of the relationship that I have with the Chairman. He knows I am not going to do anything crazy.

[Laughter.]

Mr. THOMPSON. Once again, you are in charge.

Mr. SWINDLE. If I might finish the point, and Senator—or Commissioner Thompson—congratulations.

[Laughter.]

Mr. SWINDLE. I gave you a promotion there. We are really going to take control here.

I was speaking of the database for telemarketing for the do-not-call list on the telephone. That is going to be an enormously big, complex thing, but we can get a grip on it. We have been doing this a long time. The Internet is something else. First off, you know the debate we get in on telephones of portability of numbers. We cannot figure out exactly how to do that.

How many times do people change their telephone numbers? Not very often. How many times do they change their e-mail addresses? It goes on. How many people are there out there with e-mail addresses, and they have multiple e-mail addresses. You are talking about an incredibly large database that will be difficult to secure, and if I am a spammer, I just look at that as a target-rich environment. I do not think it is a solution.

Mr. THOMPSON. One of the challenges we have is trying to cater static responses to moving targets, and in this area the target is moving very quickly. As we heard earlier, people who are engaged in spamming have every economic incentive to be clever and invest their time and money in morphing themselves into different entities, cloaking themselves, using the technology in order to send out their spam because it is so cheap for them to do so. For just a minimal positive response, your return on investment is quick and rapid. It is hard for us in an open network to change that, but I think we are talking about what other things that we can do to get at the bad actors, and one challenge that we still have to face is what do we do about volume, because even if we get after the bad actors, you still have this chart with rapid increase.

The slope may come down a little, but because of the economics, you are still going to have many people trying to use this in marketing, and it could have some disruptions in service and other things that make the consumer experience not very good. I do not know what the right answer is, but it is a challenge that we have to consider.

Senator NELSON. You all have mentioned that the FTC is seeking the additional legislative authority to improve the agency's ability to obtain information from U.S. law enforcement agencies. Now, can you discuss for the Committee how the FTC coordinates inves-

tigations with other agencies, criminal agencies, and can you expand on your request for the additional legislative authority in this area?

Mr. THOMPSON. I can talk briefly about it, that I think we have a good relationship with agencies within the United States, and I want to clarify the question a little. I think what we are asking for are ways to make it easier for us to share information with sister agencies that may lie outside of the United States.

One of the trends that we are seeing, especially in the E-commerce areas, is that we represent the richest and most robust marketplace in the E-commerce base in the world. That means others who would seek to defraud people want to come here and victimize our citizens. Right now, the way our legislation works, there are very complex rules dealing with confidentiality of investigations and the information we gather as part of a prosecution that makes it harder for us to share information with, for example, a law enforcer in France, or a law enforcer in Canada who may be interested in prosecuting those who are living there that victimize our citizens, so in some ways, what we would like to see is some legislative streamlining that would make it easier for us to prosecute in a way that recognizes the global nature of the problem.

Senator NELSON. Would you perhaps—while I was voting, both of you had already commented on the legislative approach to this problem in trying to put a criminal penalty as a means of stopping it, recognizing that we have got to work with the international arena as well. Would you further comment how, what you would like to see in law that would give you the tools as the regulator to attack this problem?

Mr. SWINDLE. Senator, I mentioned, made reference to your comments about rather punitive measures we could take against those who do cause damage, and I am moving more and more toward the belief that we are getting into criminal acts. When you consider how we are so totally integrated now with information systems and networks, how we are so dependent upon them, I mean, you know, today you can be at your home with a very inexpensive computer that is more powerful than the computers you had in the space shuttle you went up in. That computer can be captured if it is not adequately protected and then it can be used as a weapon to go out and do damage to financial systems, to air control systems, to the Defense Department, it is unlimited, because you are in these networks.

Those who would do this intentionally to disrupt information systems, to disrupt power grids, to disrupt air control, to shut down through the devices and code that goes out, and they overwhelm ISPs, overwhelm financial networks, this is grave, grave damage. This is far beyond going out and stealing 150 bucks from a grocery store, which is a crime. I think we are approaching the point where we do need to establish these people who do this as criminals, but we get back to the same problem, how do we find them, and that is a technology problem that we have not yet solved as far as I am familiar with.

But I do think, again to repeat the point that I think I made while you were out, as I said in my comment, we have got two problems here. One is this very complex technical, legal, public pol-

icy legislative arena, the other is this emotion, of all the wonderful people in this country and around the world who want to use this. They are excited about it.

I love to shop on Amazon and eBay and things of this nature, but the more we are harmed by spam, and spam is one of the biggest carriers of viruses that damage our computers, we lose confidence in it and we are going to back away from that. That is going to be a severe hit for the economic potential and entertainment potential and fun potential of information technology.

I contend that industry had better focus on that right now and get something done. They need to give consumers and users and students and home users and small businesses the capacity to put a wall in front of their computer and say, I do not want it in here if it is not on my wall, in other words, your address book, and you know, the argument is, well, you are going to miss a message from an old friend. My problem. I can deal with that much better than having this open relay. So, I think criminal designation is probably going to be necessary, and I do think we need—to sort of paraphrase what you said, I think we need a couple of good hangings here.

Mr. THOMPSON. I think a challenge, though, I think it is important perhaps to have some criminal penalties for the most egregious behavior, but let us talk a little about the fact that that may only represent the one tale of the people who are involved in spam, because one of the challenges you have when you introduce the element of criminalization, the standard of proof may be different. The idea of intent is different. Right now, for example, based on the FTC act for fraud and deception, we do not have to prove intent. Once you introduce that element, that makes it harder to go after what may be the bulk, which you may be able to get to based on civil prosecution and penalties.

Also, one other factor that I think is important to consider is that, how do you wind up prioritizing within the criminal enforcement community this kind of behavior, because it is not only just providing some sort of criminal remedy, but it is also talking to criminal prosecutors and making sure that they understand how important this is compared to any number of different criminal statutes they have to enforce, so I think the challenge is to view criminal penalties, maybe one aspect of a solution, but there have to be many more tools in addition to that.

Senator NELSON. Thank you for your statements.

After the April 30 spam workshop, the Commission has received a tremendous amount of testimony from consumers marketers, ISPs, filtering technology firms and many others. The work that the Commission has already done in combination with the workshop materials would aid this Committee in its work on crafting spam legislation that works. Can you report to this Committee in 45 days an outline of a legislative approach that deals with the issues raised during the workshop, a consumer education plan, any jurisdictional needs that should be addressed in reauthorization, and the cost to implement such recommendations?

Mr. SWINDLE. Senator, we would never refuse your request. We will make every effort. That is one of the reasons we held the workshop, because we believe that we needed to get everybody who is

involved in this in the same room at the same time and have it out, and actually a couple of them did try to have it out, but I think the whole purpose of that is to try to better inform all of us, the regulators, and the legislators as to what we can do with this, and in the process co-opt the industry in all of its respects, and even some of the people who like to engage in this stuff in here and talk about the harm that is being done. That is our goal, to try to prepare a well-informed body of knowledge, and I will certainly take back your request, and we will get to work on this and give you a response to that question. I would be a little remiss if I answered it before I found out what we have got.

Senator NELSON. Thank you very much. Thanks to both of you.

Senator WYDEN. Senator Burns.

Senator BURNS. Thanks for coming down today, and thanks for the invite you offered us during your three day workshop down there, and I am sorry I did not get to stay for it, and I have already got it written down here that maybe the video that—I think you videoed every session. I will tell you what, I would not mind having a set of those videos, and I know you have got hours and hours of them, but, you know, we could thumb through those things, and that would probably be a good way to do it, is just to get the videos of those sessions, those testimonies and those discussions. I think that was a very good workshop, and I thank you for allowing us to come down and participate in that.

And Commissioner Swindle, you are exactly right, the best solution to this whole thing is people who participate and use best business ethics, and we know those are the answers, but we also know that the industry is going to have to step forward. It is my belief that they will not until there is a national legislation that forces them to at least consider some things that can be flexible and be very light on their feet to deal with this thing as far as the legitimate marketers, because I am a market-oriented guy.

I think this thing, you know, when you walk from here to downtown, you walk by a lot of businesses and you see a lot of advertising, and you see a lot of things that are wanting to do business with you, and this industry should not be any different. However, I think the industry is going to have to step forward and set up a standard of best practices, and have those legitimate marketers—we welcome them—who want to do business in this realm of doing that.

Now, you have already responded to the no-spam list. We would be remiss if we did not consider that, but I am not real sure that that is not a detail maybe that the FTC could—on their own, because you have done a wonderful job down there. You have taken this issue and you have elevated it to a position of national awareness. You have done a terrific job down there, and we do not want to do anything through legislation that would curtail that particular activity with the FTC, but I just want—you mentioned, Mr. Swindle, in your testimony, the Commission mentioned the testimony that a solution to spam must include consumer empowerment, and of course, we use that term a lot. Do you think opting out constitutes consumer empowerment?

Mr. SWINDLE. That is certainly a form of it, Senator. Unfortunately, a lot of the spam does not honor the opt-out selection, so

you have still got the spam coming in, and the point I made is, I was reading the article this morning about Microsoft's initiative that was in the Post this morning, and my friend and sometimes adversary Marc Rotenberg, who I believe is going to be testifying on a later panel, made the statement, or is reported to have made the statement that Microsoft's proposal does not address the core need of consumers, which is to be free of commercial e-mail unless they specifically request it. That is different from opt out.

I have suggested that, to accommodate or try to resolve this emotional turning away from electronic commerce and e-mail that we are experiencing because of spam, that the ISPs and software manufacturers and the hardware manufacturers, whoever does this stuff can provide to the consumer the capacity to easily, recognizably simply say—this is oversimplification, but I do not want to receive any e-mail from anybody other than the ones I send to and the ones that are in my address book.

Think of all the e-mail that would not come in any more, just do not even have it come in, and that is what I mean about quick fixes for emotional problems, but I think there is a basic need. Opt out certainly recognizes this, but it is not honored. There is a basic need for consumers to be allowed, at their own choice, to be free of—Senator McCain used “unwanted.” That may be the best way to put it, unwanted e-mail, and if you put them in control of that, we will have a lot happier users out there and we will have less a problem on this emotional bent, and we can really get to work on this legislative and technology bent.

Senator BURNS. We could call them weeds. That is kind of an invasive and unwanted—

Mr. SWINDLE. Nutgrass down in South Georgia.

Mr. THOMPSON. I think that is a nice way of characterizing it.

Senator BURNS. We have to eliminate the weeds, and if we can find a herbicide to spray them and it kills the weed and lets the grass grow, that is what we are looking for in this situation.

Senator NELSON. Some of them are snakes.

Mr. SWINDLE. I would like to use an illustration, Senator, if I may, and it will take just another minute. I just bought my wife a brand new, nice computer. It is a great computer, Dell, a great company, has got Microsoft XP on it, a fine piece of software. All of a sudden, I started getting pop-up spam messages that says, Messenger, centered, dead center, large, right in my screen, and I do not know how to copy it. There is a way to copy it, but I am not technically savvy enough to figure it out. I said, where is this stuff coming from? It comes from a built-in Microsoft messenger, Instant Messaging, I guess, sort of like AOL, a wonderful device, if you want it.

The problem is, Microsoft put that in that computer, defaulted to the on position, did not tell me it was there, did not tell me how to easily get it off of there, and they use it, or somebody's using their system, maybe an affiliate, to send me spam that I do not want. The industry needs to solve this problem. They can solve it technically. They just need to want to solve it, and as to your initial proposal, maybe they need a fire lighted under them. I think they do.

I think the FTC has done a grand job of elevating the subject of privacy to the public. Everybody is aware that they ought to be concerned about their privacy. We have achieved a very—I would never say excellent, because we are still working on it. It is a journey, not a destination, but we have more companies doing better things on privacy than ever before, and we have not passed a law to get there, but public pressure, if you inform the public, they then demand. Industry will respond because that is how they stay in business.

Senator BURNS. I believe that, and I thank you for your openness and your frankness about this, because I think we have been talking about this issue for 4 or 5 years. It is time to quit beating around the bushes and tell it like it is and then go ahead and respond to that, and I thank both Commissioners for coming this morning.

Mr. Chairman, thank you.

The CHAIRMAN. Senator Wyden.

Senator WYDEN. Thank you, Mr. Chairman. First, I always welcome the views of the Federal Trade Commission, but I will tell you, I am a little troubled about sitting around and waiting another 45 days, or whatever. It is time to get going, folks. It is time to protect consumers. This problem has grown so dramatically, just in the last few months, that I just fear if we embark on yet another prolonged kind of study session, we are not going to get after this, and it is time to start moving, and frankly, Senator Burns and I in the last 4 years have been looking at just about every idea under the sun. We are going to continue to look at others, but I want to get some things clear on the record.

First, on the enforcement provisions, 2 years ago, Commissioner Swindle, Eileen Harrington came to the Committee and said that the enforcement mechanism in the Burns-Wyden bill would work. In fact, her comments are, the enforcement scheme laid out in the bill likely would work well.

Now, it has got four tiers. The four tiers are the criminal penalties, the Federal Trade Commission civil penalties, the authority of the state Attorneys General, and the ability of an ISP, an Internet service provider to bring suit. I guess the first question I would like to know from both of you on the record, do you disagree this morning—so we can actually get a sense of what two Commissioners think this morning, do either of you disagree with what Eileen Harrington said when she said the enforcement mechanism in the Burns-Wyden bill would work well?

Commissioner Swindle.

Mr. SWINDLE. Senator, we essentially do that already. Under section 5 of the Federal Trade Commission Act we deal with deception and unfairness, a false header, that is an address, the from line of somebody that is not the real person, that is deception. Deception in the subject line is deception. Deception in the subject matter is deception. We have the ability, with the existing laws, to do those things. Certainly the criminal and civil aspects of it are positive things. We do that already.

We work very well with the Department of Justice in trying to find solutions to these problems and certainly go after the bad guys. We certainly encourage the continued ability of states to en-

force the Federal Trade Commission Act, and working with the AGs, and we do a marvelous job with that.

Senator WYDEN. But Commissioner, obviously, empowering the state Attorneys General is something the Congress has to do. The ISP provision is something the Congress has to do. I just want to know, so we do not go out and reinvent the wheel every 45 days or 60 days, whether you agree with what Eileen Harrington said, and I happen to think you have done useful work. It is not a referendum on whether you all have done useful work. Eileen Harrington said our enforcement mechanism would work. Do you agree with that?

Mr. SWINDLE. I have not disagreed, but the point I want to make, Senator, is, we can have this structure, which you know is wonderful. The problem still remains finding those who are doing the evil. That is a technology challenge. It is a staffing challenge. We go after these cases, and one of the big dilemmas we have is trying to figure out how many resources can we devote to this when we very likely will not find who did it, and the effect of what was happening, does it warrant the spending of these resources. It is a very difficult thing.

Enforcement is many things. It is having the structures you described, certainly, but also you have to have the capacity to go do something with those tools. You have to have the capacity to find the person who has done wrong and bring them in and stand them up in front of those four standards and get them.

Senator WYDEN. Commissioner Thompson, Eileen Harrington, do you think she was right when she said, what we are trying to do on enforcement would work well?

Mr. THOMPSON. I think she was right, what she said when she said it. What I think is based upon what I have heard and the information that we have gotten that the problem may have morphed a little. Now, I do not want to make any mistake about it. You will hear from me today instances where I would like to come back and tell you whether certain parts of the various bills we see will address part of the problem, but I do not want to make any mistake about it. I think that we need legislation, and we need it this year.

The issue is whether the form of legislative vehicles we have seen so far address parts of the problem and not other parts of the problem, and we would like to be a resource to you to give you the best information of whether some of those parts might be more effective or might be necessary elements in addressing the problem.

Let me give you an example. I was actually moved by the information that was given to us by a small ISP provider, when I say small, less than 20,000 subscribers who said that last year, they spent \$200,000 to deal with spam, and they were able to spread that cost passing it through to their subscribers, but they saw a real choke point coming up ahead, because they were so small, that they would not be able to pass that cost on, and that is because of volume. I am not sure we have a way to address that, but I would like to give you the best information that I have, and I am willing to come back to you in 45 days or sooner, if necessary, to give you what that best judgment is.

Senator WYDEN. Mr. Chairman, if I could just get one other question in very briefly, what we tried to do in the Federal Trade Com-

mission portion of it is to give you all the flexibility to make distinctions between the big-time offenders and the small-time violators. Again, because we had gotten favorable testimony from the Federal Trade Commission, we felt we were headed in the right direction. Do you all still feel that that is a sensible distinction to be making, either of you?

Mr. SWINDLE. Senator, I think we need to continue this dialogue. I have been using this expression for a long time. There are no simple answers to this. I have not seen one piece of legislation that I think will be adequate.

I do not know that we need additional authority. As I said, we have the capacity to go after deception and fraud right now. We have got to realize that this is going to be an evolving process. It is going to take technology advances, it is going to take industry stepping up to the plate and doing what they ought to do because it is the right thing to do, and it is going to take us working and advising and consulting with you, Senator Burns, Senator McCain, and other Members of the Congress, trying to find the best possible solution. We want to find the best possible solution, I mentioned.

We are not going to find the perfect solution. We can forget that. We just are not going to find it, but the best possible solution will be the one that is effective and the one that does not do more harm than good and start to make impediments, and again, industry could solve much of this problem if they would get it done so that you would not be having to try to get it done through legislation, which invariably, because of the speed of this industry, the legislation will always be behind.

Senator WYDEN. My time has expired. My only point is that when you have the real scofflaws, when you have the real bad actors, those are not people who are paying attention to what industry self-regulatory initiatives are all about, and that is why we have got to move, and we have got to move quickly, and I think we ought to have your input, but Mr. Chairman, I hope that this effort to have 45 more days and more discussion will not turn into something that is so prolonged that we cannot get action on it. We have had a lot of years of studying it, and I think we ought to get moving, and I thank you for the time.

The CHAIRMAN. Senator Cantwell.

**STATEMENT OF HON. MARIA CANTWELL,
U.S. SENATOR FROM WASHINGTON**

Senator CANTWELL. Thank you, Mr. Chairman. I know this Committee and my colleagues here today have spent a great deal of time working on this issue, as the FTC has, on trying to enforce and crack down on the individuals, and I am anxious to hear from our second panel as well, because I think we are going to hear some interesting comments from them, because I think the industry is being very much impacted by this as well.

There are people who very much count on having a relationship with online consumers, and that relationship is being damaged by the perpetrators of spam, so I think everybody is interested in moving forward. Why not focus more narrowly on one particular aspect of this issue, which is harvesting.

I know my colleagues here have language in their legislation, but why not, as a first step, something that we can all have consensus on, and we know that there are perpetrators of spam, either autogenerated by computers, or people who are actually harvesting names that are available online from various websites. Why not crack down on that right away, and focus on the anti-harvesters as a key component?

Mr. SWINDLE. Senator, I personally think the clandestine capturing of e-mail addresses and then turning around and using them is an abominable act. It is commonplace, we all know that, and perhaps we need to look at it in terms of saying you cannot do this, but again, we get back to how do we enforce it, how do we find those who do it, because from a technology standpoint, it is fairly well concealable, but again, it is just one small element of this whole problem that we need to keep working and need to be getting industry to step up and tell us, number 1, how to solve the problem with technology, and number 2, we are not going to do this any more.

I have a good friendship with a member of industry that was telling me when he took over the company, and it is a fairly big company, he said that he found out that one of the practices of the company was, when they got e-mail addresses they sold them, and he asked, why are you doing that, did you ask for permission. They said, no. He said, we are stopping that right now. That is the kind of leadership we need.

Senator CANTWELL. We have had a lot of discussion, I am sure, in the last couple of years about what those relationships are and what businesses have the right, in various types of marketing, what relationships they can extend to some of their partners, but in this notion of anti-harvesting legislation, being specific, that you cannot autogenerate or cannot take names that you have gotten from other places online and e-mail them, and then going back to those, and I know it is not obvious who all of these entities are, but with a little investigation you can find them. If that organization cannot prove that they have a prior business relationship with that name, then they would be guilty of having harvested it. It is a more simple framework of saying that there are people—you know, we have had all this debate about opt in and opt out, and we can continue to have it, or what is the right framework, and how do you make the penalties, but I think 90 percent of the people would agree on the anti-harvesting aspect.

Mr. THOMPSON. I think that would be helpful.

Mr. SWINDLE. I think it is a legitimate approach. I would ask for consideration to how you define existing relationship, because some of the definitions of it I have seen, you could drive a Mack truck through them. You almost have an existing relationship just because you exist, and that needs to be carefully thought of, because, again, I made a statement in my opening remarks that the laws of legislation that will tend to favor larger firms over smaller firms is not a good idea in my mind, that I think some of the larger firms will have the capacity to drive trucks through large holes.

Mr. THOMPSON. I think it would be helpful. I think it is an element, but I think it is only one element. I know that this Committee has been particularly concerned about how to deal with pro-

pecting what consumers' interests are. I think it is important, though, that we also manage their expectations. I think that this is one element, but I think there are other parts of the problem that need to be addressed, too, and I think that a well-crafted legislation should have various pieces, because there is not one single answer to this problem.

Senator CANTWELL. Well, I think that that is—I agree with that, but I think focusing on the most egregious issues is important for us to do, too. If we are not going to move forward on the whole framework, let us make progress on the most egregious side of the equation.

And Mr. Swindle, I just wanted to clarify when you were talking about that example, you were talking about—with Microsoft, you were talking about seeing a pop-up message, right? You were not talking about somehow someone e-mailed you an additional message?

Mr. SWINDLE. I am going to use the term that is alien to Microsoft, I guess, Instant Message, which I guess belongs to AOL, but right in the middle of the screen a message.

Senator CANTWELL. I know what you are referring to. So are you saying that you lump that in with—I am not saying it might not be a rude behavior, and one that the consumer—

Mr. SWINDLE. It is spam.

Senator CANTWELL. How are you defining it as spam?

Mr. SWINDLE. It was a commercial notice placed on my screen without me being able to control it, not knowing it was there. I found out how to control it and cut it off, and I have not gotten any more, but it would have been nice if Microsoft told me, hey, Orson, thank you for buying the new computer and getting our software. By the way, our instant messenger service is on, and you are going to be receiving messages from us, and if you do not want it on, just do this and turn it off. They did not give me the courtesy of doing that. The message basically said, if you do not want to receive things like this, go to a website and you can get instant message blocker, or something like that. It was advertisement, pure, unadulterated advertising.

Senator CANTWELL. Well, and I certainly think that there are issues about what should be, once you have installed someone's software, what capabilities they should have in continuing to communicate to you, and that should be clear to consumers and you should give them options.

Mr. SWINDLE. Give me the power to turn it off, to say no—

Senator CANTWELL. Right. Exactly.

Mr. SWINDLE.—that is all I ask, and they should have done that and they did not do it, and I find it interesting, they are now promoting how they are going to stop spam, and by their own practices, they are sending me spam.

Senator CANTWELL. Well, I do not know that Microsoft is, but—

Mr. SWINDLE. An associate.

Senator CANTWELL.—I think that it is a related issue, the software functionality, and giving consumers obviously the ability to turn off and turn on, and to be asked permission is a very key point, but I would try to keep that as a related, but separate issue

to this notion of that then comes into your e-mail queue from a variety of people that are generating.

Mr. SWINDLE. I was looking at my e-mail and blanking over my inbox—

Senator CANTWELL. Your screen.

Mr. SWINDLE.—was this spam message. It cannot be called anything other than that.

The CHAIRMAN. Thank you, Senator. It is time—

Senator CANTWELL. Thank you. Thank you, Mr. Chairman.

The CHAIRMAN. The Senator from Washington's time has expired. Thank you.

Thank you very much, Commissioners. I appreciate your time and your input, and I will look forward to your comments on the Microsoft recommendations. The sooner you can get those to us, the better. Thank you.

Our next panel is Mr. Ted Leonsis, the Vice Chairman of America Online; Mr. Enrique Salem, President and CEO, Brightmail; Mr. J. Trevor Hughes, Executive Director, Network Advertising Initiative; Mr. Marc Rotenberg, Executive Director, Electronic Privacy Information Center; and Mr. Ronald Scelson, who is of Scelson Online Marketing. I welcome you. I appreciate your patience, and I apologize for the delay, which has been caused by votes on the floor. Mr. Leonsis, welcome. It is a pleasure. Please proceed.

**STATEMENT OF TED LEONSIS, VICE CHAIRMAN,
AMERICA ONLINE, INC. AND PRESIDENT, AOL CORE SERVICE**

Mr. LEONSIS. Thank you, Mr. Chairman. Chairman McCain, Members of the Committee. On behalf of America Online and our 35 million worldwide members, I would like to thank you for the opportunity to testify before the Committee on the issue of unsolicited commercial e-mail. My name is Ted Leonsis, and I am Vice Chairman of America Online and President of the AOL Core Service, and as one of the early pioneers in this industry, I am here today because I believe this issue is the most important matter that is facing us today, and that is not a personal opinion. That comes directly from the hearts and minds of our members.

I would also like to thank the fellow panelists for being here today, especially FTC Commissioners Orson Swindle and Mozelle Thompson for hosting a very timely workshop on spam earlier this month, and you will enjoy the tapes. It was at that forum where we made an announcement that to me was a shocking reflection of how bad things had truly gotten when it comes to the online medium that we helped to create, and the rising tide of spam.

On April 30, we announced that our company was blocking up to 2.4 billion spam e-mails in one day from being delivered to our members. That amount is double the number of spam e-mails we had blocked in one day from just 8 weeks earlier, on March 5, and over four times the amount of spam we blocked since early December.

On a yearly basis, and this is mind-boggling, that means we are now blocking almost 24,000 spam e-mails from going to each one of our members' e-mail inboxes.

And to give you some more context, if a standard business-size envelope represented each spam e-mail we were blocking, and

every day, every single day you laid those envelopes end to end, they would stretch around the earth four times and then on to the moon, but this is more than just sheer raw numbers. There is raw anger that spam generates from our members that has forced us and me personally to declare that the worst spammers are public enemy number 1, and we now know that canning the spam remains the priority, number 1 issue for online consumers today, and our members tell us, they go out of their way to tell us how much they hate spam every day on our service.

We put a report spam button on our AOL software that came out in the fall and today more than 9 million receipts will come from our members. They are forwarding spam to help us block more and more of it right at our servers. Those are more than 9 million individual pleas from our members for action on spam, and as far as I am concerned, we are hearing them loud and clear, but even though our members are reporting more spam to us than ever before, and even though we are blocking more spam from getting to our members than ever before, it is clearly not enough to stop the rot of the e-mail tool that has become so central to our people's daily online lives, and that is why we are all here today. We really need your help.

We are not just at a crisis period, but we are at a point now where the very tool that is the core communication point in the online world is under attack. In short, we are witnessing a serious threat to consumer confidence in the e-mail function, and if that happens, it will lead to an erosion of faith in the online medium in general, and that would be a crime. That is why we applaud everyone here for stepping forward. You would have had and will continue to have a very critical and timely role to play in the effort to eradicate this scourge of spam.

This is an issue that begs for attention but more importantly begs for action. We recognize better than anyone that there is no silver bullet that is going to kill spam on the Internet. It is everywhere, and no one owns the spam problem and no one will have the solution. We are in this together, Government, our competitors, our consumers, the entire industry. Every constituent that is online this matters to, and we are responding in AOL forcibly and comprehensively to the spam attack and believe we are rising to the occasion to defend our members in five key areas, and these are all pillars of our plan to battle against spam.

First, we are and will continue to invest in providing the very best software tools to empower members to fight back against spam and spammers, such as the report spam button in customizable mail controls on our 8.0 software. 100 days after that announcement, we released a new version of our software called 8.0 Plus, and made it very easy for our members to move into a mode where they would only receive e-mail from people that they knew, so we have listened to the FTC and that capability is already built in.

Second, we are constantly updating and strengthening the anti-spam filters that we own and operate at our server level, and we use our daily member feedback to do so. They are providing us with the lists, and we are listening and responding technically.

Third, we are working with State and Federal-level policymakers to ensure that the public laws stay abreast of and involved with the ever-changing, even more complex nature of spam.

Fourth, we are playing offense legally. We have filed civil lawsuits against over 100 individuals and corporations who spam our members, and we are raring to go to do it with more.

And fifth, we are working across the industry with key stakeholders such as Earthlink, Yahoo, and Microsoft, no small feat for AOL to do, in an effort to share resources, collaborate on technical solutions and set industry guidelines to beat these spammers, but even with all that, right now it is not enough, and so we are constantly seeking to advocate newer, tougher weapons against what I like to call the leadership targets in this war on spam, and that is where I believe you and Congress can step in with strong anti-spam legislation.

We need bigger mallets in this online version of Whack-a-Mole that we are playing to go after the worst spam offenders, namely the outlaws and the kingpins of the spam world, and I am talking about those spammers who systematically and perseveredly send spam using fraudulent and invasive methods, those who mislead, lie, and falsify with disdain and disregard for any law or measure of decency. They need to get what they deserve, criminal penalties, felony counts, and jail time.

I pointed to the recently unveiled Virginia anti-spam law, which is now the toughest in our nation, and the criminal penalties it contains, as well as the asset forfeiture provision as to a good starting point for Federal action.

At the same time, we cannot allow these spam evildoers to represent in any way appropriate, legitimate, and practical marketing via e-mail. That is why, in addition to the remedy I just mentioned for outlaw spammers, we would all like to see a Federal bill established of rules of the road on the Internet for marketers who legitimately communicate online with consumers.

If there is ever an idea whose time has come, it is stronger, meaningful anti-spam legislation with this two-pronged approach. Give law enforcement the tools to seek criminal and felony penalties against the very worst offenders on spam, and let the good practitioners of e-mail marketing be guided by a set of standards that we will all abide by.

I know this is a tall order, but we will continue to play our part and invest and do our best to innovate and constantly give our members better anti-spam tools, seek more and more technological solutions, make our anti-spam filters even better so we can block more spam, and also work across the industry in a collaborative and cooperative way without regard to competitive boundaries. I am calling for us to work together in a multifaceted way in a more comprehensive approach, but we really need all of you by our side every step of the way. Do not let the spammers get away with it, and we have to act now.

We are so pleased that Senators Burns and Wyden have taken such a strong and active interest in this issue, and we look forward to continuing to work with them and other Members in crafting legislation that will really help. I thank the Chairman and Members of the Committee.

[The prepared statement of Mr. Leonsis follows:]

PREPARED STATEMENT OF TED LEONSIS, VICE CHAIRMAN, AMERICA ONLINE, INC.
AND PRESIDENT, AOL CORE SERVICE

Chairman McCain, Senator Hollings, and members of the Committee, on behalf of America Online, Inc., I would like to thank you for the opportunity to testify before the Committee on the issue of junk e-mail—or “spam.” My name is Ted Leonsis, and I am Vice Chairman of America Online, Inc. and President of the AOL Core Service.

I would like to tell you a little bit about the nature of the spam problem and its effect on ISPs and Internet users, as well as some of the things that AOL is doing—along with our other industry colleagues—to help address this issue. But first, I would like to commend you for holding this hearing and taking a forward-looking approach to the spam problem at such a critical time. We believe that there is a strong and important role for government to play on this issue, and we are anxious to work with you to find a solution to this crisis.

Spam is one of the biggest problems facing Internet users and Internet service providers (ISPs) today. Junk e-mail clogs the arteries that carry communications across the Internet—misappropriating the network and resources of ISPs, and negatively affecting the online experience of Internet users. And because junk e-mailers do not bear most of the costs of sending their millions of messages, consumers and ISPs must shoulder the majority of the expense and burden of handling spam. Moreover, much of the mail contains objectionable or misleading advertisements. Consumers are being bombarded with offensive, deceptive, annoying e-mail; and legitimate commercial e-mail that consumers might want to read is being lost in a sea of junk. Clearly, spam is a significant business and consumer issue that needs to be addressed.

While spam has caused problems for ISPs and consumers for years, it has grown exponentially in recent months. Spam now accounts for 60–80 percent of all mail coming in from the Internet to AOL members, and AOL estimates that the overall volume of spam is doubling at least every four to six months. Spam is costing U.S. businesses in excess of \$10 billion annually, clogging the Internet and overwhelming e-mail service providers (see Ferris Research at www.ferris.com). For everyone in the online world, spam is a burden that has reached crisis proportions—and it’s only getting worse.

Fighting spam has become a serious quality of life issue for everyday consumers. At AOL, we’re listening to our members and have declared spammers to be “Public Enemy #1.” AOL has taken a number of important steps over the past few months to fight back against spam, basing our actions on the complaints and concerns of our members.

First, we have deployed strong technologies across our network to block and filter spam. Our anti-spam filters are now blocking up to 2.4 billion pieces of unwanted mail per day, which means we are stopping almost 70 spam e-mails per account per day from landing in the e-mail inboxes of our members. And we’ve fine-tuned technology that stops spam before it happens by preventing spammers from gathering—or “harvesting”—e-mail addresses from AOL areas.

Second, we’re enlisting our members in this fight by giving them new tools that make it easier than ever to block spam and report spammers. Our popular “Report Spam” button has resulted in a dramatic increase in the amount of spam being reported directly to AOL by its members—we now receive upwards of 9 million reports of unwanted e-mail per day. AOL’s Mail Controls are easy to use and allow our Members to block e-mail from specific mail address or entire domains, or to create a “permit list” of addresses from whom they will accept mail. We’re also providing our members with important consumer safety tips that can help them reduce spam and improve the security of their online experience—particularly in the broadband environment, where it is critical that consumers know how to protect themselves in the world of “always-on” high-speed connections.

Later this year we will introduce new spam identification tools that will be personalized for each member, so members can decide for themselves what is unwanted mail. And we will strengthen our already powerful Mail Controls, offering more ways to stop spam before it reaches the inbox. In addition, AOL will—in keeping with our longstanding commitment to providing strong Parental Controls—take special steps to help provide kids on AOL with a safe, spam-free experience.

In addition to the technology tools we use and provide to our members, we’re also joining with other ISPs in waging war against spammers in court. Just recently, AOL filed lawsuits against over a dozen companies and individuals responsible for

sending 1 billion spam e-mails to our members. We've taken more than 100 individuals and companies to court over the past few years, resulting in millions of dollars in monetary penalties against spammers. We're supportive of the actions that Earthlink and other ISPs have taken to fight spam on the legal front, and we look forward to finding new ways that industry can work together to bring spammers to justice.

We're also building alliances with others in our industry to think creatively and constructively about how to craft and implement real solutions to the spam problem. Just last month we joined with Microsoft and Yahoo! to announce a commitment to work together and with other industry stakeholders to combat spam. The group will initiate an open dialogue to drive the development of open technical standards and industry guidelines that will help fight spam, as well as discussing ways to cooperate with law enforcement efforts against large-scale spammers.

And finally, we're working with policymakers to support efforts to reduce unwanted e-mail. For example, we worked with Virginia legislators, the Attorney General, and the Governor to get a tough new law enacted in Virginia earlier this month that would provide criminal penalties for spammers who send junk e-mail by fraudulent means. We were also honored to participate in the spam workshop sponsored by the FTC several weeks ago, which served as a lively forum for debate and discussion about the complexities of the spam problem and how it can be addressed.

Yet despite these efforts, spam remains a problem for service providers and their customers, particularly because many spammers use fraudulent transmission tactics—such as forging e-mail addresses and Internet domain names—to circumvent filters that are designed to allow ISPs to manage their mail load and empower consumers to exercise choice. In fact, we believe that these “outlaw spammers” (those who engage in fraud) are the primary cause of the overall spam problem.

The “outlaw” spam problem includes: 1) e-mail that is sent using falsified means of technical transmission; 2) e-mail sent using hacked e-mail accounts; and 3) e-mail sent by spammers who intentionally abuse legitimate e-mail service providers by registering for multiple e-mail accounts or domain names using a false identity for the sole purpose of transmitting spam. “Outlaw” spam has increased alarmingly in the past year, and we believe that this dramatic growth underlies the astonishing increase in overall spam volume. These spammers are hijacking the computer resources and bandwidth of private consumers and businesses large and small, threatening to overwhelm the entire online medium.

With the spam problem reaching crisis proportions, we believe that government can play a strong role in helping fight spam—both through increased enforcement efforts and through the enactment of new laws to target spam. AOL believes that Federal legislation can serve two purposes in helping to fight spam. First, it can help set baseline rules of the road for legitimate marketers who use the e-mail medium to reach consumers. Such rules, combined with industry standards and new spam-fighting technologies developed by relevant stakeholders, will help to ensure that marketers use e-mail responsibly and will also provide legitimate businesses with some clarity regarding the legal obligations governing their marketing operations.

Second, we believe that government action is critical to deterring “outlaw” spammers. Strong and effective laws—including tough criminal penalties—must be put in place to pursue and prosecute spammers who use fraudulent transmission tactics. The newly amended Virginia Computer Crimes Act is an example of a law that gives ISPs and law enforcement powerful tools for fighting “outlaw” spam. The Act calls for enhanced criminal penalties if, for instance, spammers employ minors to send spam or derive significant revenue from sending large-scale spam. This statute provides another way for law enforcement and service providers to take direct aim at “outlaw” spammers, using the law to put them out of business.

We hope that Congress will follow Virginia's lead by enacting legislation that will target “outlaw spam” by imposing stiff penalties on spammers who engage in techniques of fraud and falsification. Such legislation is needed not only to stop existing abuses, but also to safeguard new e-mail technologies that outlaw spammers may try to circumvent. We are pleased that many Members of Congress—including Members of this Committee—have taken an interest in the spam problem and are working to advance legislative solutions.

In the meantime, AOL is committed to maintaining a leadership role in the fight against spam. The goodwill and trust of our members depends on our continued focus on developing solutions to this problem. AOL will continue to pursue strong enforcement actions and innovate our spam fighting tools—putting our members in even greater control. But ultimately, we believe the spam battle must be fought on many fronts simultaneously in order to be successful. From technology to education,

from legislation to enforcement, industry and government can work together to reduce spam significantly and give consumers control over their e-mail inboxes.

We applaud the Committee for examining this issue at such a critical time, and we look forward to working with you and other lawmakers to stop spammers in their tracks.

Thank you for the opportunity to testify; I am happy to answer any questions you may have on this topic.

The CHAIRMAN. Thank you. Mr. Salem, welcome.

**STATEMENT OF ENRIQUE SALEM, PRESIDENT AND CEO,
BRIGHTMAIL INC.**

Mr. SALEM. Thank you, Mr. Chairman and Members of this distinguished Committee, for allowing me to address you on this topic of unsolicited commercial e-mail, often referred to as spam. I am Enrique Salem, Chief Executive Officer of Brightmail Incorporated. Today, our software process is approximately 10 percent of the world's Internet e-mail for our customers. E-mail has become a ubiquitous form of communication for businesses and personal use. Spam is flooding our inboxes and it is threatening the viability of e-mail as a communication tool. It undermines consumer confidence and threatens the future of e-mail and online commerce.

The growth curve of spam has been steep over the last 5 years. Brightmail has seen an increase of more than 900 percent in the number of unique spam attacks per month, dating from April 2001 to April 2003. Attacks can have anywhere from 10 to tens of millions of messages that span a few hours to many days. Over the same period, the amount of unsolicited commercial e-mail has increased from a few messages to approximately 46 percent of all Internet e-mail, and that is a conservative number.

The numbers are actually growing very, very rapidly, and we believe that by the end of this year, it will be more than 50 percent. The current volume of spam being sent has a significant cost to ISPs and businesses. Spam is currently the number 1 complaint for many ISPs, and is negatively impacting customer satisfaction while driving support costs and infrastructure costs.

On the business front, a recent report from Ferris Research estimates that spam costs U.S. businesses \$10 billion a year in lost productivity, bandwidth, and storage costs. Businesses face an additional liability by allowing offensive and fraudulent content to reach employees. Adult content has increased more than 170 percent in the last 12 months. Unlike traditional direct mail or telemarketing, e-mail marketing has a very low marginal cost. As a result, despite extremely low response rates, spammers can make a profit. The more e-mails a spammer can send, the greater his profit, while costs remain nearly constant.

The Internet does not know geographic boundaries. 90 percent of the spam hitting our probe network is untraceable, or uses some form of deception to hide its origin. In many cases, this is accomplished by sending the mail through unsecured open relays and open proxies that are spread out across the world. Of the 10 percent that is traceable, 60 percent claims to be from Europe, with 16 percent claiming to be from Asia.

Spammers will continue to use deceptive techniques to evade filters. We are starting to see an increasing amount of corporate identity theft, where spammers send mail using well-known brand

names in an attempt to evade filters and reach user inboxes. A consequence of this technique is that less dynamic spam filters can blacklist legitimate corporate domains in a misguided attempt to fight spam.

The sheer volume of spam is also having a direct impact on legitimate direct marketers. The messages are being lost in a sea of spam. Overzealous filters now block an increasing amount of legitimate mail. In many cases, it is inappropriately deleted or placed in a bulk mail folder, which reduces the response rates to legitimate marketing campaigns. It is important to note that spam is invading other forms of electronic communication, including Instant Messaging and wireless devices. One only needs to look at what has happened in the international wireless markets to see that spam has become a very serious problem on cell phones, such as in Japan and on the NTT DoCoMo Network. We should not exclude these other valuable communication tools from consideration, because the same problems affecting e-mail today will soon affect these other forms of communication.

I am here to tell you we will solve the spam problem. The solution will require strong legislation, cooperation between direct marketers, ISPs, and technology providers. It will require legislation, but there are limits to what laws alone can do. Strong laws can serve as a deterrent to spammers. We need Federal laws that prohibit deception in e-mail headers. There also needs to be a valid way to opt out, but we still need to define what it means to opt out. What are we opting out of? We need to prohibit the sale of tools to harvest e-mail addresses, as well as the sale of e-mail lists that have been inappropriately created.

Beyond spam filtering, technology will be required to identify legitimate e-mail. There will need to be a set of best practices and guidelines defined and managed by industry coalitions that are followed by legitimate direct e-mail marketers, allowing us to more effectively block spam and allowing legitimate mail to be successfully delivered, preserving e-mail as a viable communications tool.

Thank you for the opportunity to comment and participate in this important discussion.

[The prepared statement of Mr. Salem follows:]

PREPARED STATEMENT OF ENRIQUE SALEM, PRESIDENT AND CEO, BRIGHTMAIL INC.

Spam Problem Overview

E-mail has become a ubiquitous form of communication for both business and personal use. With e-mail has come spam. Today, spam is spreading in such staggering amounts—flooding both corporate and personal inboxes—that it now threatens the viability of e-mail as a primary communication tool. Unsolicited commercial e-mail (UCE), commonly known as spam, has reached epidemic proportions. Analyst firm IDC currently estimates that 7.3 billion pieces of spam are sent each day with 3.9 billion of those sent in North America.

The growth curve has been steep. Over the last 5 years, we have seen the amount of unsolicited commercial e-mail increase from a few messages to approximately 46 percent of all Internet e-mail. Brightmail predicts that by December of 2003 spam will become more than 50 percent of all Internet e-mail. It has become a serious problem for Internet Service Providers (ISPs), businesses and individuals.

Unlike direct mail or telemarketing, e-mail marketing has very low marginal cost. As a result, despite extremely low response rates, spammers can make a profit fairly easily. The more e-mails a spammer can send, the greater his profit, while the cost remains nearly constant. Bulk e-mailers are sending between 80 and 100 million messages a day. This both explains the alarming growth rate of spam and

makes it more frightening—there is no financial disincentive for flooding the Internet with more and more spam.

Costs to ISPs and Businesses

A recent Gartner Group study on spam estimates that spam costs an ISP with 1,000,000 users \$7 million per year. Spam is currently the number one complaint for many ISPs and is negatively impacting customer satisfaction while driving up support and infrastructure costs. Businesses are also not immune from the costs. A 2003 report by Ferris Research estimates that spam costs U.S. businesses \$10 billion/year in lost productivity alone. Businesses must also add additional storage and bandwidth to handle the increase in e-mail traffic due solely to spam. Lastly, businesses face an additional liability—allowing offensive and fraudulent content that is often a part of spam to reach employees. Adult content has increased more than 170 percent in the last 12 months and scams have nearly doubled in the same time period. These are concerns that go beyond the IT department and into the human resources arena.

Costs to Direct Marketers

Another significant consequence of the sheer volume of spam being sent is that over zealous filtering attempts are now blocking an increasing amount of legitimate mail. In many cases it is improperly deleted or placed in a bulk mail folder reducing the response rates to legitimate marketing campaigns.

Spam is a large and growing problem

As seen in Chart 1 below, Brightmail has seen an increase of more than 900 percent in the number of unique spam attacks/month from April 2001 to April 2003. A spam attack is a unique grouping of messages based on their content—for example, Herbal Viagra. Spammers will inject random content into each message to attempt to confuse filters by making each message that they send appear to be different. Attacks can have anywhere from ten to tens of millions of messages and can last from a few hours to many days.

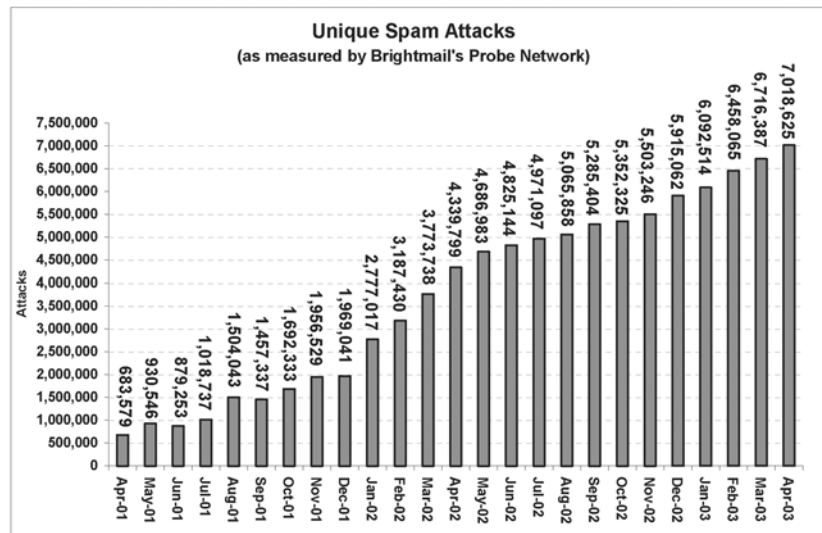
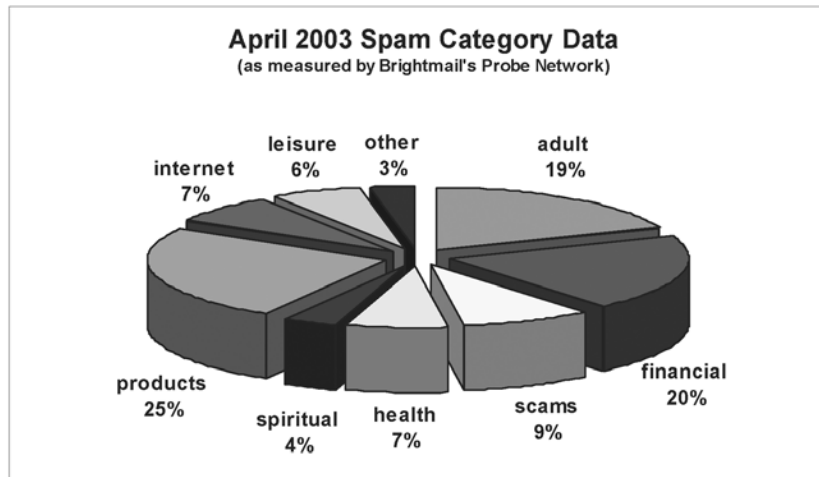
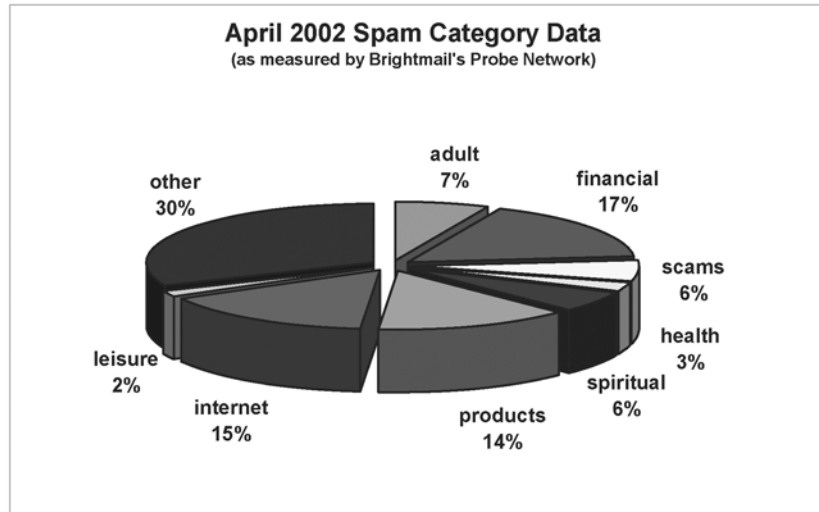


Chart 1

Spam is becoming increasingly offensive or fraudulent

As noted in Charts 2 and 3 below, from April 2002 to April 2003, Brightmail has seen “adult” spam increase by more than 170 percent and spam categorized as “scams” nearly double. These offensive e-mails are troublesome and costly for consumers as well as for businesses.



Charts 2 & 3

Spam is threatening the viability of e-mail

As seen in Chart 4 below, over the past two years, both spam and e-mail have grown. However, spam comprises a greater and greater percentage of the total amount of e-mail that is sent each year, which is threatening the viability of e-mail as a communications tool.

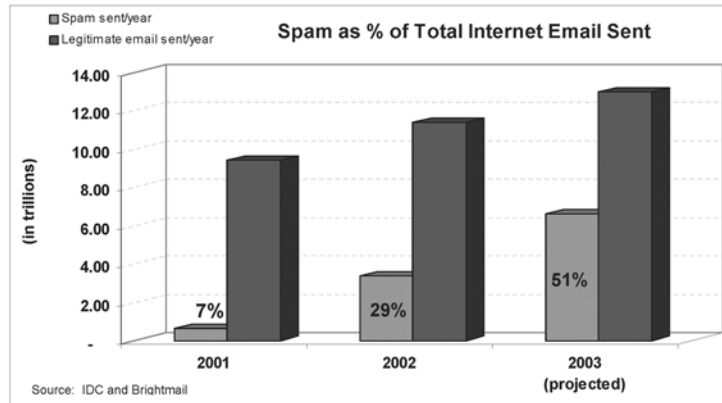


Chart 4

Spam is an International Problem

Much of the spam reaching U.S. inboxes is routed through other countries. The majority of spam is untraceable (90 percent), but of that spam that does claim to come from a certain region of the world, the majority comes from Europe—with the Russian Federation comprising 10 percent—and Asia—with China leading Asia. A key point to make is that even if a spam message claims to originate in China, it very well could have originated in North America or somewhere else. This point has implications as we consider the impact of various state and Federal spam legislation.

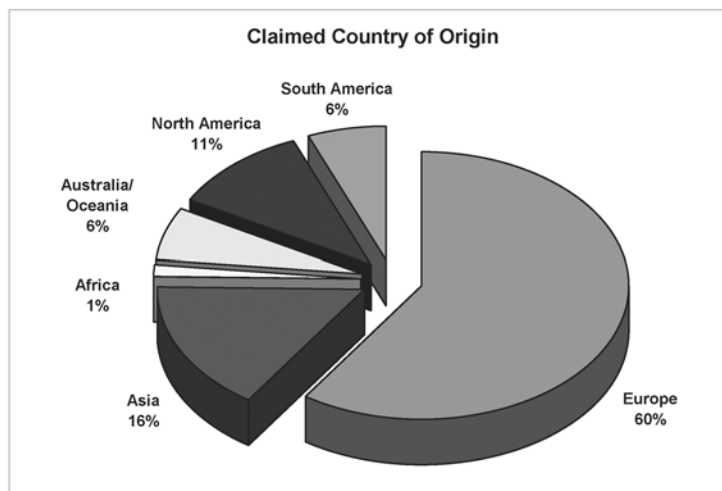


Chart 5

Tracking Spammers is difficult

Spammers often obfuscate their true location by enlisting open relays or proxy servers throughout the world. Trying to track down the true origin of a known spam message is often quite difficult, as demonstrated in Exhibit 1 below.

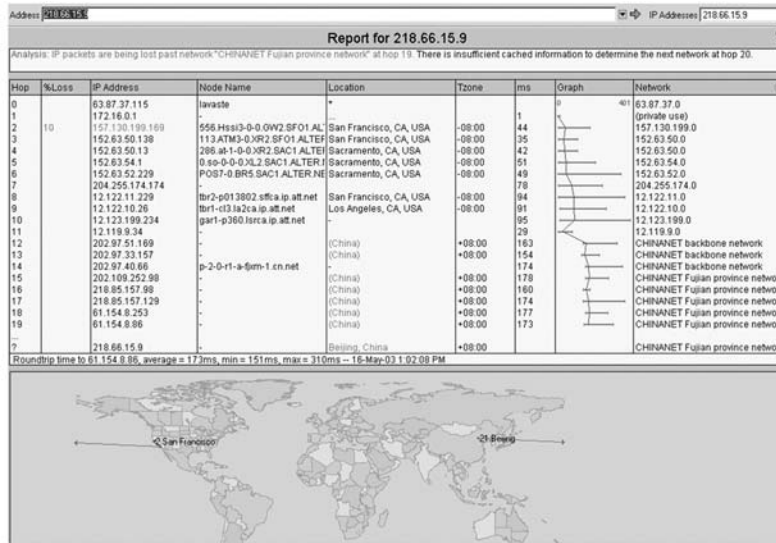


Exhibit 1

Use of Open Proxies

Spammers aggressively use technology to hide their tracks. A perfect example is the growing use of open proxies; open proxies are misconfigured servers that allow spammers to generate large volumes of e-mail that are not easily traceable to the actual sender. There are many thousands of open proxy servers available to spammers at any given time and a great deal of spam flows through these servers—both in the U.S. and overseas.

Changing Techniques to Reach Inboxes

Spammers have moved beyond simple text-based e-mail to entice end-users to click through. One such technique is using HTML-based e-mail. An example of a recent HTML-based spam message appears to the recipient as follows:

Exhibit 2



When in reality, the HTML code behind this seemingly benign image is collecting valuable information for the spammer.

```

<BR><BR></FONT></DIV>
<DIV align=center>
<P><A
href="http://www.info@abc-
deals1.com/cellbooster/welcome11.html?affid=1000&amp;e=info@brightlight.com">
<IMG
height=340 src="http://210.22.144.195/cbgraphics.jpg" width=468 border=0
NOSEND="1"></A>
<P><A href="http://210.22.144.195/r/?e==info@brightlight.com"><IMG height=20
src="http://210.22.144.195/re.gif" width=209 border=0
NOSEND="1"></A><BR>"Why
aren't you in a more interesting business?"<BR>"Yes," said Arthur, "yes I did.
It was on display in the bottom of a locked filing cabinet stuck in a disused
lavatory with a sign on the door saying "Beware of The Leopard"."
</FONT></P></DIV></BODY></HTML>

```

Pulls info down from URL and provides feedback to spammers!

Random text inserted by spammer tools

Spam Can Lead to Digital Identity Theft

Spammers also employ well-known brand names in an attempt to get end-users to open e-mails. Not only does this perpetrate the spam problem, it also does considerable damage to the reputations of companies.

We see spam from global corporations that was actually sent out by a spam shop halfway around the globe. These innocent corporations face more than the wave of bounced messages and angry responses from the spammed. This type of corporate identity theft can severely damage a company's worldwide brand since spammers have global reach.

Additionally, some misguided attempts to fight spam result in building blacklists that often include the domain names of these victims of domain identity theft. These blacklists further the damage done by the open relays and falsified headers of spammers when subscribers to these blacklists can no longer receive e-mail from the legitimate enterprises. Domain names are an intrinsic part of a corporate brand. The theft of these names for mass mailing of unsolicited e-mail has hurt some companies already and the trend may grow in the months and years ahead.

Corporations have a responsibility to their employees and shareholders to take measured steps in securing their messaging systems. In fact, as liability cases do make their way into the courts, the extent to which corporations can demonstrate that they made "best efforts to protect against spam" will have a large bearing on the outcomes.

In the header information in Exhibit 3 below, a spammer has used two well-known company names to trick the recipient into thinking that the e-mail is from a trusted source, when in fact it is just an attempt to obfuscate the true identity of the sender.

```

From: "Chase S. Stewart" <cs_stewart@fedex.com>
To: xyz123@hotmail.com
Subject: Whatever works better
Date: Wed, 26 Mar 2003 13:05:01 +0000
MIME-Version: 1.0
Received: from 3com.com ([218.62.7.234]) by mc4-f42.law16.hotmail.com with
Microsoft SMTPSVC(5.0.2195.5600); Wed, 23 Apr 2003 02:09:59 -0700
X-Message-Info: JGYoYF78jEHjx36O18+Q1OJDRSDidP
Message-ID: <HJHOBKICNELIIEBKOCFFLPADPAB.cs_stewart@fedex.com>
In-Reply-To: <d21101c2f1b6$db026239$9d8010e0@4e5d6bz>
X-MIMEOLE: Produced By Microsoft MimeOLE V6.00.2800.1106
X-Mailer: Microsoft Outlook IMO, Build 9.0.2416 (9.0.2910.0)
Return-Path: cs_stewart@fedex.com
X-OriginalArrivalTime: 23 Apr 2003 09:10:03.0620 (UTC)
FILETIME=[20200240:01C30978]

```

Exhibit 3

Spam: Moving Beyond E-mail

Wireless Spam

There is a huge impending need for anti-spam protection in the mobile/wireless environment. Wireless e-mail produces a unique set of threats from spam, including volume issues when wireless users receive large amounts of spam. Viruses and worms can harm or temporarily paralyze PDA devices or the applications that run on them. Cell phones are particularly vulnerable to dictionary attacks done by spammers using phone numbers, with the advent of text messaging and SMS.

There is currently more of a need for anti-spam protection for wireless devices in foreign markets than in the U.S. The highest risk to wireless spam and viruses exists in Asia and Europe, but the need in the U.S. for protection is growing. We can see the future for U.S. wireless in overseas experiences as they have adopted wireless technology more rapidly. One way that spam is affecting wireless communications overseas is by causing carriers to pay back their own customers for each spam message received. Since carriers like NTT DoCoMo in Japan charge for incoming messages, customers were at first paying their carrier for the pleasure of receiving and having to delete spam from their own devices. Now DoCoMo refunds customers for spam messages received, which is detrimental to DoCoMo's bottom line.

Additional costs of wireless spam are passed on to end-users. With wireless messaging pricing models, wireless users must pay for each message and, often, each line of content within that message. With unwanted messages flooding wireless devices, end-users will no longer find technologies like SMS a viable mode of commu-

nication. With the continued adoption of wireless communications in the U.S. will come a dramatically increased need for wireless anti-spam and anti-virus technology, to protect the end user and the provider's bottom-line. As wireless adoption continues, spammers will increasingly target wireless users with spam, making for an expensive and very inconvenient dilemma. As spam invades PDAs, cell phones and the like, wireless carriers will have to block spam or face customer churn and costly refunds for unwanted wireless spam.

Instant Messaging (IM) Spam

Spam is also infiltrating the desktops of business and home users via another popular communication tool—Instant Messaging (IM). As more businesses use IM to communicate with business colleagues who are offsite or traveling, spam via this route has some of the same negative impacts that it does via e-mail—productivity issues and potential liability issues for offensive content that is delivered via IM.

Exhibits 4 and 5 below are examples of recent IM spam that were received by business users. Exhibit 4 offers a common pitch to lose weight while Exhibit 5 contains more offensive content. Spam via IM is of particular concern to parents whose children use IM to communicate with friends.

Exhibit 4

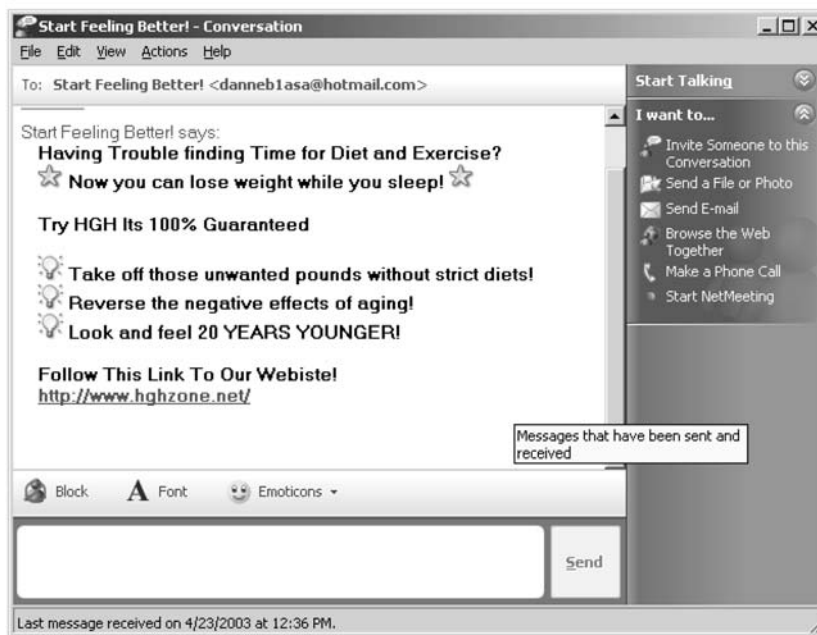
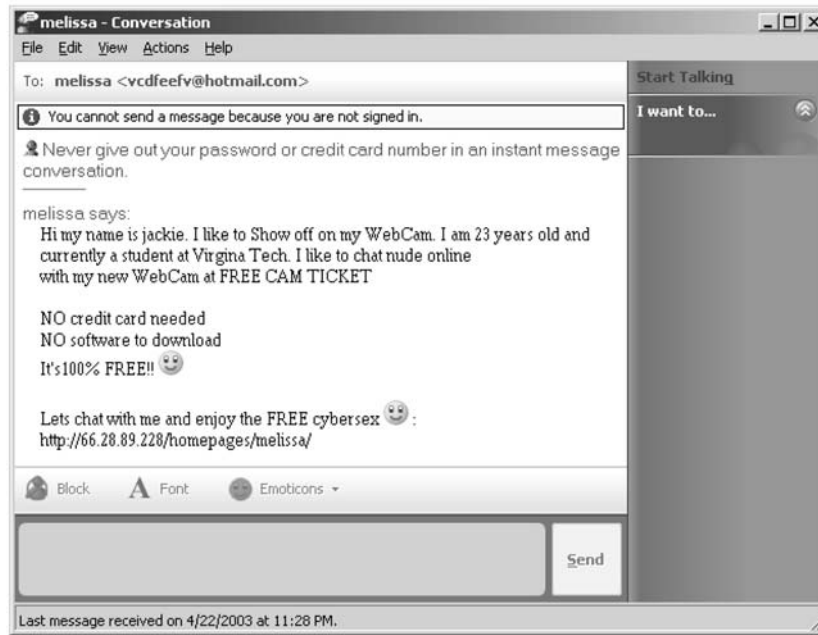


Exhibit 5**Impact of Current Spam Legislation***State Legislation*

As of April 2003, twenty-nine (29) states have spam control laws. In July 1997 Nevada became the first state to enact spam control legislation (law amended in 2001 and 2003). Nevada law states that it is illegal to send unsolicited commercial e-mail unless it is labeled “ADV” or “ADVERTISEMENT” at the beginning of the subject line, and includes the sender’s name, street address, and e-mail address, along with opt-out instructions.

Similar spam control legislation was passed in California in September 1998. California law currently states that unsolicited commercial e-mail messages must include opt-out instructions and contact information, and opt-out requests must be honored and that certain messages must contain a label (“ADV:” or “ADV:ADLT”) at the beginning of the subject line. Only a small percentage of the messages Brightmail processes each month uses these labels, partly because less sophisticated spam filters were identifying messages with these marks and partly because spammers do not abide by these U.S. state laws since they are not sending spam from these states.

Indiana and New Mexico and Virginia are the states to most recently pass spam related legislation, doing so in April 2003. Virginia’s recently updated law has received a great deal of attention due to the stiff penalties for sending spam from within the state of Virginia, including giving the authorities power to seize assets earned from sending bulk unsolicited e-mail pitches while imposing up to 5 years in prison for violators.

Have these state laws had an impact on the volume of spam? Not really—spam has continued to increase dramatically over the past few years, from being an annoyance to a serious threat to the viability of e-mail. Part of the problem has to do with enforcement of the laws—there have been limited number of cases that leverage current state law given that the burden of proof is often on the recipient and can be a heavy burden at best. An example of this heavy burden is the eTracks case that is currently being litigated by a San Francisco-based law firm, Morrison and Foerster LLP. States have limited budgets and those dollars are being allocated to enforcing laws that more directly impacts the safety and well being of its residents.

Foreign Spam Legislation

We've seen spam legislation enacted in other countries, such as Japan where businesses delayed implementing technological solutions in hopes that Federal legislation would eliminate the spam problem. The law, enacted in October 2002, which required unsolicited text messages to be tagged, has had little impact on reducing the volume of spam sent via text messaging in Japan.

The European Union (EU) has also passed legislation that its member states must comply with by October 2003, which requires that there must be a prior opt-in relationship between a sender and recipient in order for unsolicited e-mail or text messaging to be sent. Some member states are already in compliance, but the amount of spam that European e-mail users receive continues to climb. ISPs and European businesses are being forced to examine technological solutions to the spam problem, given that legislation is having little impact on the spam problem.

Federal Spam Legislation

There is hope that Federal laws will have the muscle required to combat the growing spam problem. The only current Federal restrictions on e-mail spam are the general criminal and civil fraud prohibitions. The FTC currently works with law enforcement to combat fraudulent e-mail scams, but at the moment 56 percent of spam does not fit the legal definition for fraud, according to a recent study by the FTC, and is therefore beyond current law. Given federal, state, and local law enforcement's focus on preventing terrorism and their limited resources, they simply cannot keep up with spam.

However, there are a number of proposals currently in front of Congress.

These include the Can Spam Act (revised in April 2003) that would require unsolicited commercial e-mail messages to be labeled, require unsolicited commercial e-mail messages to include opt-out instructions and the sender's physical address, and prohibit the use of deceptive subject lines and false headers in such messages. Additionally, this bill would pre-empt any state laws that prohibit unsolicited commercial e-mail outright, but would not affect the majority of state spam laws.

Another Federal initiative, the Computer Owners' Bill of Rights (S. 563) would require the Federal Trade Commission to establish a "do-not-e-mail" registry of addresses of persons and entities who do not wish to receive unsolicited commercial e-mail messages. Additionally, the FTC would be empowered to impose civil penalties upon those who send unsolicited commercial e-mail to addresses listed on the registry.

A third proposed law, the Reduce Spam Act, requires that unsolicited bulk commercial e-mail messages would be required to include a valid reply address and opt-out instructions, and a label ("ADV:" or "ADV:ADLT", or other recognized standard identification). These requirements would apply to messages sent in the same or similar form to 1,000 or more e-mail addresses within a two-day period. In addition, false or misleading headers and deceptive subject lines would be prohibited in all unsolicited commercial e-mail messages, whether or not sent in bulk.

Additionally, New York Senator Charles Schumer is planning to propose legislation that would incorporate many elements of other proposed legislation but also adds funding for enforcement of the "do not mail" registry component of his proposed legislation.

From our point of view labeling has not helped to solve the problem, as it is a component of current state legislation.

Benefits and Consequences of Legislation

As with other public hazards, legislation can play an important role in the fight against spam. However, the extent of the problems often extends beyond state and country borders, preventing legislation alone from solving the problem. Consider the parallels in the offline world. While there are many "laws of the road" for drivers, still the public wants the auto industry to build as many safety features into cars as they possibly can. Similarly, while "Breaking and Entering" is a felony crime, homeowners use locks, bars and alarm systems to protect themselves from robbery.

While legislation plays an important role in highlighting the seriousness of spamming, it is currently very difficult to enforce. Spamming is a global problem, with e-mail being routed around the globe and with wanton disregard for local regulations. Governments cannot impose regional laws on assailants outside their boundaries. Even when legal authorities can catch a spammer within their jurisdiction, the burden of proof can be daunting to prosecuting attorneys.

Legislation may help to deter some spammers and provides a framework for prosecution and operations of both Direct Marketers and anti-spam companies. But, enforcement is key and will prove expensive and difficult. We need to alert this com-

mittee that is it critical to set the expectations of the public at the right level as far as the real impact of legislation on the volume of spam received.

We believe the solution will involve a coordinated effort by Internet Service Providers, Direct Marketers, technology providers and law enforcement agencies. We will need to establish guidelines that outline e-mail best practices. These guidelines will need to be followed by direct marketers. It will become important to be able to identify legitimate direct marketers and there will need to be improvements in how direct marketers manage their lists.

APPENDIX

Brightmail Corporate Overview

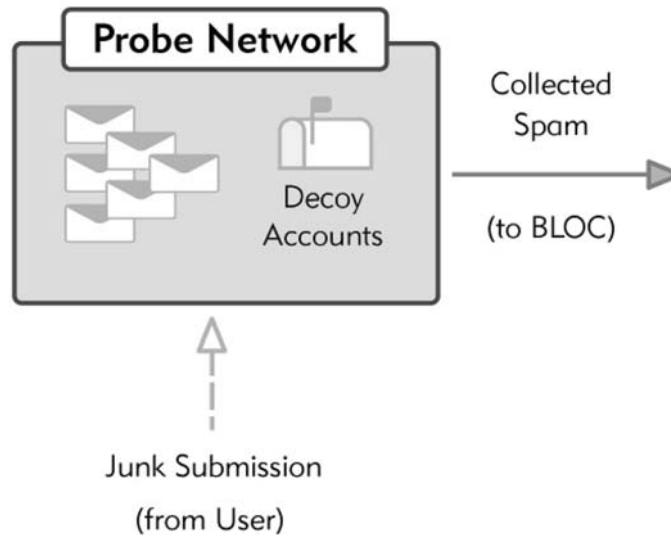
Brightmail, the worldwide leader in anti-spam technology, provides anti-spam software that makes messaging secure and manageable. Founded in 1998, Brightmail protects the networks of enterprises, service providers, and mobile network operators by filtering spam, viruses and undesired messages at the Internet gateway. Brightmail currently serves many of the largest service providers, including AT&T WorldNet, EarthLink, MSN, and Verizon Online as well as leading enterprises that include eBay, Booz Allen Hamilton, Deutsche Bank, and Cypress Semiconductors.

In April 2003, across its customer base, Brightmail software filtered over 60 billion messages and protected over 250 million mailboxes.

Brightmail anti-spam architecture includes a patent protected “spam alert network” called the Brightmail Probe Network, a collection of more than a million decoy e-mail accounts. It is designed to attract unsolicited e-mail and has a statistical reach of more than 250 million e-mail accounts that provide Brightmail with a unique insight into the changing face of spam throughout the world.

Brightmail is backed by world-class investors and partners and is headquartered in San Francisco, CA.

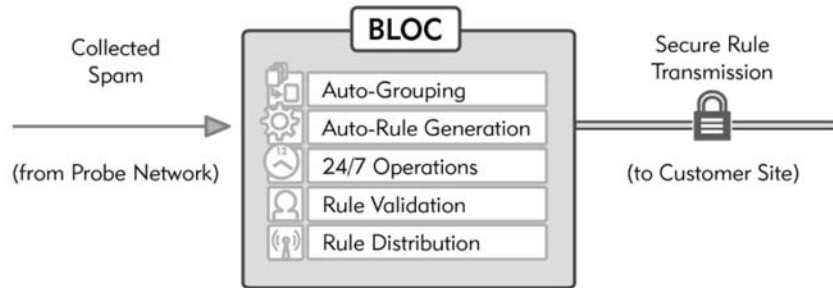
Brightmail Architecture



Probe Network™

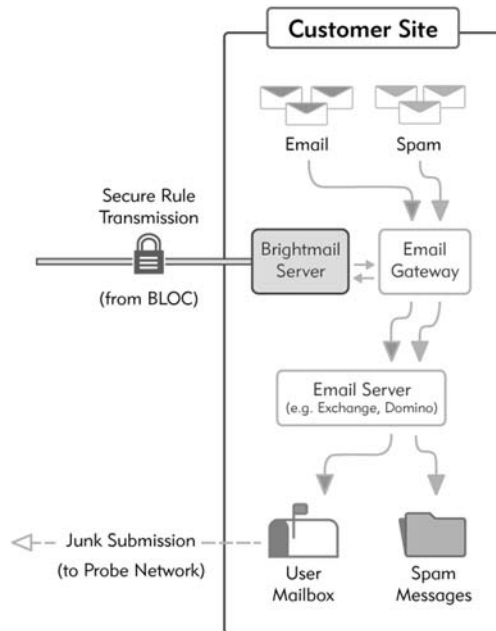
The Probe Network has a statistical reach of more than 250 million e-mail accounts. It consists of millions of decoy e-mail addresses that receive more than 300 million spam messages per month. The data from the Probe Network is used for the real-time creation of anti-spam rules that are propagated to Brightmail customers every few minutes—24 hours per day. This patent protected technology is used to provide Brightmail customers with spam protection from the highly dynamic, ever changing, phenomena that spam has become.

U.S. Patent 6,052,709 (Apparatus and method for controlling delivery of unsolicited electronic e-mail)



BLOC (Brightmail Logistics and Operations Center)

- Operates 24 hours/day—365 days/year
- Employs state-of-the-art tools to identify new spam attacks
- Messages are automatically grouped into spam attacks and then rules automatically written against them
- QA technicians verify the rules before they are made available
- New anti-spam rule updates every few minutes
- Rules are transmitted via a secure conduit (HTTPS)



- Brightmail software is installed at the customer site
- Brightmail's extensive anti-spam rule set contains filters that automatically block identified spam attacks
- Uses sophisticated grouping algorithms and pattern matching to identify and eliminate spam as it enters the e-mail gateway
- Updated in real-time
- Protection against spam is always current

The CHAIRMAN. Thank you, sir. Mr. Hughes.

**STATEMENT OF J. TREVOR HUGHES, EXECUTIVE DIRECTOR,
NETWORK ADVERTISING INITIATIVE**

Mr. HUGHES. Mr. Chairman and Members of the Committee, I want to thank you for inviting me to testify. My name is Trevor Hughes, and I am the Executive Director of the Network Advertising Initiative.

The NAI is a cooperative group of companies, and we are dedicated to resolving public policy concerns related to emerging technologies. In the past, the group has tackled issues such as self-regulatory solutions for online ad targeting and the use of web beacons online. We have now turned our focus to the growing problem of spam and to that end, a coalition has been formed within the NAI which is made up of 35 leading companies which are e-mail service providers. All of these companies are struggling with the onslaught of spam, as well as the emerging problem related to the deliverability of legitimate and wanted e-mail.

Let me tell you a little bit about e-mail service providers. E-mail service providers enable their customers to deliver volume quantities of e-mail messages. These messages originate from the full spectrum of the U.S. economy. Large and small businesses, educational institutions, nonprofits, governmental agencies, publications and affinity groups all use the services of e-mail service providers to communicate with their customers, members, and constituents.

While ESPs do serve the marketing needs of the marketplace, it is by no means the only customer group served. My members provide and deliver transactional messages such as account statements, airline confirmations, and purchase confirmations. They deliver e-mail publications and newsletters. They deliver affinity messages. The NAI and the e-mail Service Provider Coalition believes that much can be done to solve the problem of spam. At the most fundamental level, we believe that we need to create accountability within the e-mail delivery system. Spammers spend their days concocting new methods to obscure and falsify their identity in order to sneak past existing filters and avoid accountability.

In many ways, our existing tools are merely reacting to the spam that is received today and not preparing for or combatting the spam that will arrive tomorrow. For this reason, we believe that the solution to spam exists in three components, a legislative component, a technological component, and a social component. I will address the technological component briefly, and then focus on the part of the solution for which we look to you, Federal legislation.

Part of the problem in treating the spam epidemic is that spammers enjoy the impunity of anonymity. Spammers hide behind open relays, they spoof identities, and they deceive recipients with misleading from and subject lines. Make no mistake, the business of spamming is one of fraud and deception.

The NAI recently proposed a technological blueprint to respond to this problem. Essentially the blueprint, called Project LUMOS, is designed to force senders of volume e-mail to incorporate authenticated identity into every message sent. The use of authenticated identity, along with a rating of sending practices over time, pre-

vents spammers from hiding behind the technology of e-mail, and forces all senders to be accountable for their sending practices. We have engaged with many of the major ISPs and other groups on this effort, and we are greatly encouraged by the traction our effort has gained since it was launched 1 month ago.

The ESP coalition strongly believes that strong, preemptive Federal legislation will be a critical component, but again not the only component in the successful resolution of the spam problem. In the United States today we have 28, and it could be 29 by now, states that have enacted some form of spam legislation. Unfortunately, the standards and definitions applied by these statutes are not consistent. As a result, we have a crazy quilt of different standards that has created an unnecessarily complex compliance system.

To make matters worse, enforcement within the global medium of e-mail is exceedingly difficult when limited by state boundaries. We need preemptive Federal legislation to harmonize these standards and provide powerful tools to enforcement officials.

We believe that the current spam bill before the Senate, the CAN-SPAM Act, strikes the appropriate balance with regard to preemption. The CAN-SPAM Act would allow for a national standard to be set for the delivery of unsolicited commercial e-mail. Given the incentives provided within the bill, most legitimate businesses will move to a fully consent-based model for e-mail delivery. This is particularly true where the standards set by the bill will be uniform across the entire country. To combat spammers, the bill provides strong enforcement tools for the FTC, the state Attorneys General, and to ISPs. We strongly support enforcement by all of these groups.

One issue that has been raised in discussions regarding spam legislation and may be raised again is a private cause of action. Such a solution, while tempting, would do nothing to stop spam. Spammers spend their days looking for ways to technologically obscure their identity. Pursuing spammers requires enormous technological, financial, and investigative resources. Individuals do not have such resources, but Governments and ISPs do.

We have a very real example of what a private cause of action means when included in a spam statute. In the state of Utah, a spam statute was passed last year that allows for a private cause of action in class action lawsuits. A single plaintiffs firm in Utah has now filed hundreds and by some accounts thousands of class action lawsuits under the statute, but the firm is not pursuing spammers.

Given the cost and complexity of finding actual spammers, this firm has targeted leading companies and brands using law firm employees as plaintiffs and seeking out "gotcha" moments as the basis of their complaints. Perhaps most telling is the fact that there are no data to suggest that the amount of spam in Utah has been reduced by even one message.

Another issue that has been raised in relation to spam is that of opt in versus opt out. Over the past few years, our industry has lost critical time debating this issue while spam has been allowed to proliferate. Let me make this perfectly clear. This debate, regardless of what standard is eventually adopted, will not result in the reduction of spam. A spammer's stock in trade is in deception.

They do not care about whether they have permission from the recipient. They pay no heed to all of the existing state laws regarding spam. The most restrictive opt-in statute will do nothing to dissuade spammers from sending their messages.

Again, the NAI is very supportive of the CAN-SPAM Act. We will continue to work with staff over a few technical details of the bill, but look forward to seeing a Federal law enacted this year. On behalf of the NAI E-mail Service Provider Coalition, I want to pledge that we will continue to work to fight spam and preserve e-mail with you and the members of your staff.

Thank you, and I look forward to your questions.
[The prepared statement of Mr. Hughes follows:]

PREPARED STATEMENT OF J. TREVOR HUGHES, EXECUTIVE DIRECTOR,
NETWORK ADVERTISING INITIATIVE

Executive Summary

The NAI is a cooperative group of companies dedicated to resolving public policy concerns related to privacy and emerging technologies. In the past, the NAI has successfully launched self-regulatory solutions to online ad targeting, and the use of web beacons. The NAI has now turned its focus to the growing problem of spam and the related concern of deliverability of wanted e-mails. As part of this effort, a coalition has been formed within the NAI to represent the interests of e-mail service providers (ESPs). The E-mail Service Provider Coalition ("ESP Coalition") is made up of 35 leading companies—all of which are struggling with the onslaught of spam, as well as the emerging problems related to the deliverability of legitimate and wanted e-mail.

E-mail service providers enable their customers to deliver volume quantities of e-mail messages. These messages originate from the full spectrum of the U.S. economy—large and small businesses, educational institutions, non-profits, governmental agencies, publications, and affinity groups all use the services of ESPs to communicate with their customers, members, and constituents. While ESPs serve the marketing needs of the business community, it is by no means the only customer group served. E-mail service providers also deliver transactional messages (such as account statements, airline confirmations, and purchase confirmations); e-mail publications; affinity messages; and relational messages. Within the ESP Coalition, we estimate that our members provide volume e-mail services to over 250,000 customers.

The ESP Coalition sees spam as a threat to the long-term viability of the ESP industry. Indeed, spam presents a dire threat to all uses of e-mail—marketing, transactional, affinity and relational—as the continued growth of spam will lead to the widespread abandonment of e-mail as a communications tool. Put simply, the spam problem will critically damage the ESP industry if it is not curtailed. Consumers and businesses will not use e-mail if the system becomes so choked with misleading and deceptive messages that those messages that are actually wanted are lost in the fray.

The ESP Coalition strongly supports legislation to respond to the growing menace of spam. We believe that strong preemptive Federal legislation will be a critical component (but not the only component) in the successful resolution of the spam problem.

In the United States today, we have 28 states that have enacted some form of spam legislation. Many more are considering spam legislation in their current legislative sessions. Unfortunately, the standards and definitions applied by these statutes (and proposed in pending bills) are not consistent. As a result, we have a crazy quilt of differing standards and definitions that has created an unnecessarily complex compliance system. To make matters worse, enforcement within the global medium of e-mail is exceedingly difficult when limited by state boundaries. We need preemptive Federal legislation to harmonize these standards and provide powerful tools to enforcement officials.

Federal legislation must carefully balance the legitimate use of e-mail against the need to respond to spam. E-mail represents one of the most powerful drivers of efficiency and productivity in today's economy. Our response to spam must take into account and protect the widespread utility of e-mail. Overly restrictive or poorly

crafted solutions may end up “throwing the baby out with the bathwater” and damaging the very tool we hope to protect.

The NAI is very supportive of the current spam bill proposed in the Senate (the CAN-SPAM Act). While we continue to work on some minor technical details within the bill—such as the length of time available for processing unsubscribe requests and definitional issues—we are encouraged by the fundamental structure and approach taken by Senators Burns and Wyden. We feel that this bill endeavors to balance the continued use of e-mail as a legitimate communications tool with strong standards and enforcement tools to prevent spam.

Testimony

Mr. Chairman and Members of the Committee, I want to thank you for inviting me to testify. My name is Trevor Hughes, and I am the Executive Director of the Network Advertising Initiative (NAI). The NAI is a cooperative group of companies dedicated to resolving public policy concerns related to privacy and emerging technologies. In the past, the NAI has created self-regulatory programs for online ad targeting, and the use of web beacons. The group has now turned its focus to the growing problem of spam and the related concern of deliverability of wanted e-mails. As part of this effort, a coalition has been formed within the NAI to represent the interests of e-mail service providers (ESPs). The E-mail Service Provider Coalition (“ESP Coalition”) is made up of 35 leading companies—all of which are struggling with the onslaught of spam, as well as the emerging problem related to the deliverability of legitimate and wanted e-mail.

Let me begin my testimony by explaining the unique role that e-mail service providers play in the search for solutions to the spam problem.

E-mail service providers enable their customers to deliver volume quantities of e-mail messages. These messages originate from the full spectrum of the U.S. economy—large and small businesses, educational institutions, non-profits, governmental agencies, publications, and affinity groups all use the services of ESPs to communicate with their customers, members, and constituents. While ESPs serve the marketing needs of the business community, it is by no means the only customer group served. E-mail service providers also deliver transactional messages (such as account statements, airline confirmations, and purchase confirmations); e-mail publications; affinity messages; and relational messages.

The ESP industry is robust and growing. Within the ESP Coalition, we estimate that our 35 members provide volume e-mail services to over 250,000 customers. These customers represent the full breadth of the U.S. marketplace—from the largest multi-national corporations to smallest local businesses; from local schools to national non-profit groups and political campaigns; from major publications with millions of subscribers to small affinity-based newsletters. Even my local soccer association uses an e-mail service provider to deliver schedules and standings to the players in the league.

Jupiter Research estimates that the e-mail marketing industry (which, again, is only a portion of the total spectrum of ESP customers) will grow in size to *2.1 billion dollars in 2003* (up from 1.4 billion dollars in 2002). By 2007, Jupiter estimates that the size of the e-mail marketing industry will reach 8.2 billion dollars. All of these numbers are for the U.S. market alone. Expanding the scope of this research to include all customers served by ESPs and foreign markets would increase these numbers significantly.

But the size and importance of e-mail in the marketplace should not be measured by dollars alone. E-mail is indeed the “killer app”. Over the past ten years, e-mail has been a strong driver of productivity and efficiency in the marketplace. It has also been an important social tool. E-mail has shortened distances in the world—allowing communication to occur with unprecedented speed and detail. E-mail has created affinity within groups that previously were too widely separated geographically to effectively recognize their common interests and positions.

As an example of the importance of e-mail, a recent study by the META Group showed that, given a choice between e-mail or telephones, 74 percent of business people would give up their phones before e-mail. In other words, 74 percent of people now find e-mail to be more critical than the telephone in their daily work.

The Threat of Spam and the Solution(s) to Spam

The ESP Coalition sees spam as a threat to the long-term viability of the e-mail service provider industry. Indeed, spam presents a dire threat to all uses of e-mail—marketing, transactional, affinity and relational—as the continued growth of spam will lead to the widespread abandonment of e-mail as a communications tool. Put simply, the spam problem will critically damage the ESP industry if it is not curtailed. Consumers and businesses will not use e-mail if the system becomes so

choked with misleading and deceptive messages that those messages that are actually wanted are lost in the fray.

I will not belabor the statistics on the growth of spam or the costs associated with handling spam. Surely all of the panelist can agree that we are presented with an enormous problem. Without an expedient solution, spam may end up killing the “killer app” of e-mail.

The media and marketplace have been replete with spam solutions for many years. Important vendors, such as Brightmail, have done a tremendous job at stemming the tide of spam. But the problem still exists and continues to grow. Increasingly, we are presented with the question: can anything be done?

The NAI believes that much can be done to solve the problem of spam. At the most fundamental level, we believe that we need to create accountability within the e-mail delivery system. Spammers spend their days concocting new methods to obscure and falsify their identity in order to sneak past existing filters and avoid accountability. In many ways, our existing tools are merely reacting to the spam received today—and not preparing for or combating the spam that will arrive tomorrow. Stated differently, our efforts to cure spam are responding to the symptoms (the actual spam received) and not the cause (the lack of accountability on the part of spammers).

So how do we create accountability within the e-mail system?

We believe that the solution to spam exists in three components: legislative, technological, and social. Let me address the technological and social components quickly and then focus on the part of the solution for which we look to you: Federal legislation.

The Technological Component

Part of the problem in treating the spam epidemic is that spammers enjoy the impunity of anonymity. Spammers hide behind open relays, they spoof identity, and they deceive recipients with misleading “from” and “subject” lines. Make no mistake; the business of spamming is one of fraud and deception.

The recent efforts of the FTC in relation to open relays and deception in spam should be commended. It is critical that we have strong deterrents to dissuade spammers from their trade. But the fundamental architecture of the Internet and e-mail protocols still allows for the deception to occur.

The NAI recently proposed an architectural “blueprint” to respond to this problem. I will submit a description of the effort along with this testimony. Essentially, the NAI’s blueprint, called “Project Lumos”, is designed to force senders of volume e-mail to incorporate authenticated identification into every message sent. The use of authenticated identity, along with a rating of sending practices over time, prevents spammers from hiding behind the technology of e-mail and forces all senders to be accountable for their sending practices. We have engaged with many of the major ISPs and other groups on this effort and are greatly encouraged by the traction our effort has gained since our launch just one month ago.

Other technological solutions also hold promise. The NAI is actively working with other constituencies in the marketplace to bring about such solutions. I hope that we will have much more to share with you before the end of this year.

The Social Component

One part of the spam problem that has not been actively discussed is the need for consumer education around the appropriate use of e-mail addresses.

The Center for Democracy and Technology (www.cdt.org) recently released a study on the consumer actions that result in exposure of e-mail addresses and, subsequently, spam. The results were compelling: the CDT report found that appropriate management of an e-mail address by the holder of that address can drastically reduce the amount of spam received. Further, the study found that there are a few actions that can create enormous amounts of spam. Specifically, the CDT reported that posting an e-mail address on a public website and posting an e-mail address in a public newsgroup or chatroom both resulted in huge amounts of spam. This is due to the use of “spiders” or “bots”—programs that scour the web for e-mail addresses and harvest them into a spammer’s database.

Clearly, one component in the total solution to spam is the education of consumers on issues such as those raised by the CDT report. If consumers understand those practices that result in spam, they will be much better able to control the amount of spam in their in-boxes.

The Legislative Component

The ESP Coalition strongly supports Federal legislation to respond to the growing menace of spam. We believe that strong preemptive Federal legislation will be a

critical component (but not the only component) in the successful resolution of the spam problem.

In the United States today, we have 28 states that have enacted some form of spam legislation. Many more are considering spam legislation in their current legislative sessions. Unfortunately, the standards and definitions applied by these statutes (and proposed in pending bills) are not consistent. As a result, we have a crazy quilt of differing standards that has created an unnecessarily complex compliance system. To make matters worse, enforcement within the global medium of e-mail is exceedingly difficult when limited by state boundaries. We need preemptive Federal legislation to harmonize these standards and provide powerful tools to enforcement officials.

We believe that the current spam bill before the Senate, the CAN-SPAM Act, sponsored by Senators Burns and Wyden, strikes the appropriate balance with regard to preemption. The CAN-SPAM Act would allow for a national standard to be set for the delivery of unsolicited commercial e-mail. Given the incentives provided within the bill, most legitimate businesses will move to a fully consent-based model for e-mail delivery. This is particularly true where the standard set by the bill will be uniform across the entire country. To combat spammers, the bill provides strong enforcement tools to the FTC, state attorneys general, and ISPs. We strongly support enforcement by all of these groups.

As a coalition made up of legitimate businesses in the e-mail industry, the NAI also strongly supports the inclusion of an affirmative defense for good faith compliance efforts within the CAN SPAM Act. Such tools help to ensure that litigation is properly targeted towards true spammers, and offers important protections for businesses working diligently to maintain approved best practices.

One issue that has been raised in discussions regarding spam legislation, and may be raised again, is that of a private cause of action. Such a solution, while tempting, would do nothing to stop spam and would definitely create a morass of litigation against legitimate companies. Spammers spend their days looking for ways to technologically obscure their identities. Pursuing spammers requires enormous technological, financial and investigative resources. Individuals do not have such resources, but governments and ISPs do. In fact, if a private cause of action existed, ISPs would be drawn away from their enforcement efforts by a flood of discovery requests generated through consumer litigation.

We have a very real example of what a private cause of action means when included in a spam statute. In the state of Utah, a spam statute was passed last year that allows for a private cause of action and class action suits. A single plaintiffs' firm in Utah has now filed hundreds (and by some accounts, over a thousand) class action lawsuits under this statute. But the firm is not pursuing spammers. Given the cost and complexity of finding actual spammers, this firm has targeted leading companies and brands—using law firm employees as plaintiffs and seeking out “gotcha” moments as the basis of their complaints. Perhaps most telling is the fact that there are no data to suggest that the amount of spam in Utah has been reduced by even one message.

Another issue that has been raised in relation to spam legislation is that of “opt-in” versus “opt-out”. Over the past few years, our industry has lost critical time debating this issue, while spam has been allowed to proliferate.

Let me make one thing perfectly clear: the debate over “opt-in” or “opt-out”, regardless of what standard is eventually adopted, will not result in the reduction of spam. A spammer's stock and trade is in deception. They do not care about whether they have permission from the recipient of the message. They pay no heed to all of the existing state laws regarding spam. The most restrictive “opt-in” spam statute will do nothing to dissuade spammers from sending their messages.

A recent FTC study conveys this point succinctly. By reviewing a large body of spam received within the agency, the FTC estimated that fully two thirds of spam is fraudulent, misleading or deceptive. This means that the majority of spam is already violating an existing law in the United States.

As currently written, the CAN-SPAM Act will provide important incentives for legitimate businesses to raise their e-mail standards. The NAI firmly believes that e-mail must be sent with the consent of the recipient, or within a pre-existing business relationship. Furthermore, we believe that e-mail should be sent with *informed* consent—meaning that recipients have clear and conspicuous notice as to the results of providing their e-mail address. This is a meaningful and workable standard.

Again, the NAI is very supportive of the CAN-SPAM Act. We will continue to work with staff on a few technical issues details of the bill (such as the need for longer processing periods for unsubscribe requests), but look forward to seeing a Federal law enacted this year.

The Threat of Filtering and Blacklists

Before I conclude today, I want to raise one growing problem in the fight against spam. While spam clearly represents a serious threat to the continued viability of e-mail, the problems created by some of the current tools used to combat spam are equally threatening. Internet Service Providers (ISPs) are aggressively building filtering technologies to limit the amount of spam entering their systems. Conceptually, this is a positive development. However, the spam filters currently in place are creating a new problem: *wanted e-mail is not being received*.

According to a report by Assurance Systems, in the 4th quarter of 2002, an average of 15 percent of permission based e-mail was not received by subscribers to the major ISPs. Some ISPs had non-delivery rates that were startling:

NetZero	27%
Yahoo	22%
AOL	18%
Compuserve	14%
AT&T	12%

The same report for the 3rd quarter of 2002 showed an average of 12 percent non-delivery rate for the major ISPs—meaning that the filtering of permission based e-mail increased 25 percent from the third to fourth quarters of 2002. Some of the e-mail campaigns within the Assurance Systems report had non-delivery rates as high as 38 percent.

Non-delivery of wanted messages due to filtering (called “false positives” within the industry) represents an enormous threat to the ongoing viability of e-mail as an effective communications tool. *The market will stop using e-mail for important communications if e-mail delivery is unreliable*. It is critical that false positives be eliminated if e-mail is to survive as an efficient and productive means for communication.

One of the main drivers in the false positive problem is the emergence and use of blacklists. These are lists of alleged spammers that ISPs—and any network administrator—can use to filter incoming e-mail. The blacklist operators build registries of IP addresses that they believe are associated with spam and make the lists available publicly. Currently, there are an estimated 300 blacklists in operation.

Again, the concept of a blacklist may seem to make sense at first glance. Unfortunately, the reality of blacklists in today’s marketplace is far different.

Many blacklists operate without standards and operate behind a veil of anonymity. For example, one of the leading blacklists, SPEWS (www.spews.org), offers no contact information: no phone numbers, no names, no addresses, and no e-mail address for the organization. The website has purportedly been registered in Irkutsk, Russia. SPEWS has no defined standards for posting to its blacklist—evidence has shown that a single complaint can result in the blocking of an entire range, or “neighborhood”, of IP addresses. Further, for those innocent senders that become listed on SPEWS, the only way to resolve the problem is to post their request for removal to a public spam forum available through Google (<http://groups.google.com/groups?hl=en&lr=&ie=UTF-8&oe=UTF-8&group=news.admin.net-abuse.email>).

All of these efforts are designed to combat spam. But in their zeal to eliminate the problem, they have created a potentially disastrous “ricochet” effect: false positives. Going forward, our solution to spam must carefully balance the need for strong action against spammers with a determination to preserve the deliverability of legitimate e-mail.

Conclusion

The NAI believes that the problem of spam will be best resolved through three powerful forces: legislation (and enforcement); technology; and consumer education. Our group is actively working with ISPs and solutions providers to craft architectural solutions to spam that will drive accountability into the dark recesses of the Internet. We strongly feel that technology must be used to force spammers to identify themselves and be held accountable for their practices. We also believe that consumers must understand the need for careful management of their e-mail addresses. We could drastically reduce the amount of spam received by average consumers through educational efforts on what not to do with an e-mail address.

But the technological and educational solutions are not enough. We need a strong Federal statute to raise the standards for e-mail practices across the entire country. Legitimate businesses will respond to such a statute by raising their practices to meet or exceed the standard set by law. Enforcement officials at both the state and Federal level and ISPs will have powerful tools to seek out and bring to justice those individuals responsible for spam. And we can do it while maintaining the balance necessary to preserve the legitimate use of e-mail.

Mr. Chairman, on behalf of the NAI E-mail Service Provider Coalition, I want to pledge that we will continue to work to fight spam and preserve e-mail with you and members of your staff. Spam is a complex problem and our efforts to craft solutions must be thoughtful, robust and effective.

Thank you and I look forward to any questions you may have.

The CHAIRMAN. Thank you. Mr. Rotenberg.

**STATEMENT OF MARC ROTENBERG, EXECUTIVE DIRECTOR,
ELECTRONIC PRIVACY INFORMATION CENTER AND ADJUNCT
PROFESSOR, GEORGETOWN UNIVERSITY LAW CENTER**

Mr. ROTENBERG. Thank you, Mr. Chairman and Members of the Committee. My name is Marc Rotenberg. I am Executive Director of the Electronic Privacy Information Center. We are a nonprofit, nonpartisan research organization here in Washington. We work in close association with the consumer and civil liberties organizations both in the United States and around the world.

I think it is fair to say that there are few issues of greater concern to Internet users today than the growing problem of spam, but I think it is also fair to say that it is one of the most complex policy issues facing the Internet. Even though there is broad agreement about the tremendous cost and inconvenience that spam is placing on the use of the Internet, there is still important questions about the appropriate role of law and technology, the relationship between the Federal Governments and the states, and even the question of how best to ensure consumer protection with a problem that clearly has international dimensions, but all of these factors do not diminish the scope of the problem.

As Chairman Muris stated at the public workshop last month, approximately 40 percent of e-mail messages today could be considered spam, and it is to be anticipated that in the next year the majority of e-mail traffic on the Internet will be spam.

As Mr. Salem commented as well, it is also the case that spam will be migrating to new communication environments, including both Internet messaging and cell phone advertising, so the need to draw an effective line here with respect to the Internet has consequences as well for development of new industry and new consumer services.

There are many factors that contribute to the problem of spam. As you all know, it is relatively easy and inexpensive to send a message to many, many people online. It is also obviously difficult to determine the origin of the messages, particularly for the most aggressive spammers. There are difficult jurisdictional problems, particularly with respect to international spam, and there are even some definitional problems associated with spam, as well as the fact that technical solutions which are being pursued aggressively by the ISPs are nonetheless imperfect.

As one of the witnesses commented earlier, spam filters have the effect of both underblocking, which is to say, allowing messages to go through that the user does not desire, as well as overblocking, which means to exclude messages that the end user would like to receive. In almost any filter system, the end user has to download the e-mail and incur the cost and connection time to receive the messages before the filters are activated.

I wanted to focus briefly on what I think are the key policy issues in trying to find a solution to the spam problem, and I am going to draw both on the experience of list development on the Internet as well as previous efforts with legislation to protect privacy when similar problems have arisen, and I would like to point out first of all that I think if any case is clearly made for an opt-in provision, it is for online marketing. In fact, the traditions on the Internet indicate this, because as people who have been on the Internet for a while and understand the operations of lists, the best lists operate on an opt-in basis.

People are provided the opportunity to sign up for the list. If their e-mail address changes, there are easy ways for them to change the e-mail address, and if they wish to be removed from the list, they can do so by quickly going to a web page or sending an unsubscribe message. These are the practices that are being followed by the best marketing firms online, as well as the companies that understand that permission-based marketing, marketing based on opt in, works particularly well in the online environment. Now, there is a good argument about whether or not it would work in the offline environment, but for the online environment, I think opt in is the right way to go.

I would also like to suggest that on the question of enforcement means, the private right of action that is found in the Telephone Consumer Protection Act that gives individual consumers the opportunity to go to small claims court and seek a maximum, a maximum of \$500, has proven to be an effective way of dealing with the problem of junk faxes and telemarketing, and I think a private right of action that provides limited damages is also a matter of fairness, because, of course, it is the end user who is being inconvenienced and burdened by the unsolicited marketing.

Finally, on this critical issue of preemption, I am very sympathetic to the concerns of the industry groups about trying to comply with 50 different state statutes, but the reality is that it is the state Attorneys General who have been on the front lines of dealing with the spam problem, and it has been the state legislatures that have developed many of the most effective and innovative responses in response to the growing problem of spam, and I would like to caution you about the danger of basically telling the state legislatures and the state Attorneys General that the problem to spam will be found in Washington, and that the limited opportunities to go after spammers if a Federal preemption law was passed will essentially be eliminated.

That having been said, I would like to thank you, Mr. Chairman and Members of the Committee, and particular Senator Burns and Senator Wyden, who I know have been doing a great deal of work on this issue for a number of years, for your efforts. Many people online will be very grateful to you if an effective, sensible solution can be found to the problem of spam.

[The prepared statement of Mr. Rotenberg follows:]

PREPARED STATEMENT OF MARC ROTENBERG, EXECUTIVE DIRECTOR, ELECTRONIC PRIVACY INFORMATION CENTER AND ADJUNCT PROFESSOR, GEORGETOWN UNIVERSITY LAW CENTER

Summary of Recommendations

- Continue to support strong enforcement action by the FTC
- Promote international cooperation, particularly with consumer protection agencies
- Recognize that many of the current spammers are likely subject to prosecution under current unfair and deceptive trade practices laws
- Enact a Federal baseline that establishes an opt-in standard, gives consumers legal rights to go after spammers, and does not preempt state law
- Anticipate that similar problems may arise with cellular phone advertising in the near future

Statement

Mr. Chairman, members of the Committee. Thank you for the opportunity to testify today about the problem of Unsolicited Commercial E-mail, or "spam." My name is Marc Rotenberg. I am the Executive Director of the Electronic Privacy Information Center. EPIC is a non-profit, non-partisan research organization. We work in close association with a wide range of consumer and civil liberties organizations, both in the United States and around the world.

There are few issues of greater concern today to users of the Internet than spam. Spam is also one of the most complex policy issues for the Internet. Even though there is broad agreement about the urgency of the problem, there are still questions about the appropriate role of law and technology, the relationship between the Federal Government and states, and even the question of how best to tackle a consumer problem that clearly has a significant international dimension.

Scope of the Spam Problem

As Chairman Muris noted at the recent FTC public workshop, the spam problem is increasing rapidly. In 2001 the FTC began to routinely collect spam. During that year, the FTC received an average of 10,000 messages per day. In 2002, that figure went up to 47,000 a day. The number has gone to 130,000 e-mails a day this year. As a measure of how fast a new e-mail address can attract spam, Chairman Muris reported that the FTC had seeded an e-mail address in a chat room. That e-mail address began receiving spam in eight minutes.

It has been estimated that 40 percent of e-mail in the United States is spam, creating an annual cost of over \$10 billion. These costs are incurred through lost productivity and the additional equipment, software and labor needed to deal with the problem.

On spam, the interests of Internet users and the Internet industry are generally aligned. Only the Direct Marketing Association has expressed opposition to sensible opt-in legislation. However, as the recent FTC Workshop made clear, this position is simply not viable in the online world. Permission-based marketing, which relies on the affirmative consent of consumers, has always been a good business practice. Now it may be critical to stem the flood of undesired e-mail.

Factors Contributing to Spam

Several factors contribute to the spam problem. First, it is inexpensive and relatively simple to send spam to a very large number of Internet users. Unlike traditional junk mail, the marginal cost for each additional electronic message is essentially zero. Therefore, spammers are as likely to send to a million users as they are to a thousand.

Second, the origin of spam is often difficult to determine. Spammers will frequently send messages from domains they do not own and in ways that conceal the source of the message. The spammers also show little regard for any effective list management. There is no meaningful effort to obtain consent or allow users to opt-out of undesired marketing.

Third, spam raises difficult jurisdictional problems. Spammers may send messages from one state to another and even from one country to another. While there is general agreement across jurisdictions about the need to reduce spam, there are questions about how best to coordinate enforcement measures.

Fourth, there are definitional problems associated with spam. Commercial marketers who engage in bulk e-mail advertising may be reluctant to concede that their messages are spam even though the vast majority of recipients find the messages burdensome and undesirable. Some Internet users may consider bulk political mail

as “spam,” though for both practical reasons and the First Amendment, it is appropriate to distinguish between commercial and non-commercial bulk mail.

Fifth, technical solutions are imperfect. While ISPs have had some success identifying the source of spam, spammers rotate domains and even change the key terms in a message to avoid detection. Similarly, typical users find it difficult to adapt filters and other techniques to accurately remove spam. There is always the risk that a filter will delete messages that the user needs to receive. Other techniques, such as challenge and response, may be too cumbersome for most users.

Sixth, the long-time reluctance of the private sector to acknowledge the need for a legislative solution to the spam problem coupled with the Direct Marketing Association’s active opposition to Internet privacy has certainly contributed to the problem. While the industry’s desire to avoid regulation is understandable, here the failure to establish strong measures to limit spam are contributing to a tragedy of the commons that threatens to undermine the commercial potential of the Internet.

Difficultly Consumers Face with Spam

While ISPs clearly face a significant cost that can be measured in bandwidth, staff hours, hardware, and even litigation fees, consumers face the ongoing annoyance that spam simply makes the Internet less friendly and e-mail less useful. For the consumer facing a mailbox full of spam, even good software programs do not solve the problem of the time and cost of downloading e-mail before it can be analyzed and assessed. These burdens fall particularly on consumers in rural regions, consumers who are traveling outside the country, and others who are likely to pay high fees while connected to the Internet.

The most widely used spam filters, while they can be effective, invariably under block and over block incoming mail. As a result, users continue to receive undesired e-mail and are losing important e-mails that may include business proposals or simply notes from friends. Some spam filters group incoming messages as likely being spam, but the consumer must still sort through the messages.

In addition, many of the techniques proposed by some are simply impractical or nonsensical. For example, a challenge response method to determine whether e-mail is coming from an actual person would probably discourage even desired communication. Similarly, routinely changing mail addresses is an impractical solution as is trying to prevent one’s mail address from being posted on a website where it can be harvested by one of the programs is not a workable approach as anyone who has a publicly accessible staff directory knows.

A better approach for the consumer is one that empowers individuals to go after the spammers who misuse their personal e-mail address for unsolicited commercial e-mail and impose costs and burdens.

Technical Measures

It is clear that industry groups and technical groups are eager to find a solution to the spam problem. Many innovative approaches are currently being pursued even as some of the routine flaws that are exploited by spammers are fixed.

Congress should continue to encourage technical solutions, but the possibility of technical solutions should not be a reason to avoid legislation. ISPs clearly favor better legal tools as well as better technologies to go after spammers when they can be identified. Moreover, without legal sanctions there is no practical basis to put an end to egregious spamming.

There is one caution on the technology front that should be brought to the attention of the Committee. Several technological solutions, not surprisingly, focus on determining the actual identity of spammers, and would make identification through digital certificates and other means a requirement for sending e-mail to multiple recipients. While this approach may be appropriate for commercial speech, it would not be appropriate for political or religious speech. The Supreme Court has made clear in a series of cases that the right to speak anonymously is a central element of the First Amendment. Any attempt by the government to require identification for bulk e-mail that would include political speech would raise significant Constitutional concerns.

Legislative Proposals

S. 877, the CAN-SPAM Act, sponsored by Senator Burns and Senator Wyden, contains many important elements for a good anti-spam measure. All unsolicited marketing e-mail would be required to have a valid return e-mail address so recipients could ask to be removed from mass e-mail lists. Once notified, marketers would be prohibited from sending any further messages to a consumer who has asked them to stop.

The bill would enable Internet Service Providers (ISPs) to bring action to keep unlawful spam from their networks. The legislation contains enforcement provisions

allowing the Federal Trade Commission to impose civil fines on those who violate the law. State Attorneys General would be given the ability to sue on behalf of citizens who have been targeted by unscrupulous marketers.

This is a good starting point, but we urge the Committee to go further, particularly to protect consumer interests. As the Burns-Wyden measure currently stands, it is simply not a sufficient solution. It gives the FTC a great deal of authority and the ISPs many opportunities to bring complaints. However, for the state attorneys who are already on the front lines and for the users who are also saddled with the costs and burden of spam there is not enough in the bill currently to reform egregious online practices or assure that spammers will be pursued.

Three critical changes are necessary to strengthen the Burns-Wyden measure. First, the Committee should endorse a full opt-in regime for unsolicited commercial e-mail except in those cases where a prior business relationship exists. Opt-in is the logical basis for Internet mailings. In fact, most Internet lists today are based on opt-in. These lists typically also provide users with the opportunity to update their contact information and remove themselves from the list if they choose. There are many opportunities for companies to obtain consent and to build online marketing techniques, in parallel with the traditional Internet lists, which would be welcome by consumers. Where there is a genuine preexisting relationship, then it would be appropriate to communicate by e-mail. Simply visiting a website is not sufficient. There should be some actual exchange for consideration before a "preexisting business relationship is established."

Second, the bill should incorporate a private right of action that allows individuals to bring action in small claims court, similar to the approach established by the Telephone Consumer Protection Act (TCPA) for junk faxes and telemarketing. The opportunity to pursue a modest judgment in small claims court has provided a useful incentive in the effort to stem junk faxes and would be helpful for spam. In fact, many of the state measures take an approach similar to the TCPA in recognition that those who are the target of spam should have the legal right to seek redress against those who are responsible for the spam. Also, as the TCPA has shown, a national do not e-mail list may help with enforcement, though technical experts have expressed some concerns about the possible misuse of a national Do Not Spam list.

Third, the bill should not preempt state law. While it is clear that some revisions have been made to the CAN SPAM Act to take account of the important efforts of states to combat spam, the bill still unduly restricts state legislatures that have been on the front lines of the problem. Even with the FTC's important enforcement efforts, there is a real risk that a "one size fits all" approach will not be effective and will undermine the basic structure of federalism in the United States that allows the states to pursue different approaches to common problems.

As Washington Attorney General Christine Gregoire stated on behalf of the Attorney Generals for 44 states, a weak Federal statute that preempts stronger state laws will reduce the level of consumer protection and facilitate the continued growth of spam. This would clearly not be a desirable outcome.

House Proposals

Several proposals are also under consideration in the House. Those bills that establish opt-in, provided for a private right of action, and leave the states free to pursue innovative approaches will respond to the spam problem most effectively. There is also an interesting provision in one of the House measures that would penalize automated harvesting techniques that are deployed for the purpose of sending unsolicited commercial e-mail. This provision may help with the spam problem.

Additional Issues

Mr. Chairman, you asked us also to address related issues that may be of interest to the Committee. I'd like to note that the problems of Unsolicited Commercial E-mail are likely to arise in a new setting that will impact millions of consumers in the United States and that is cell phone based advertising. Although we are still in the early stages, it is apparent from the experience of other countries that consumers are beginning to express concern about advertising on their phones. If it is permission-based, there should be few problems. But if marketers begin to send bulk text messages or video messages to cell phone users, there will certainly be negative effects on the growth of cell phone based services. Already, providers in the United States are proposing to send e-mail to cell phones.

There is also significant work on the spam problem underway in many countries outside of the United States, and in particular in the European Union. It is interesting to note that virtually all of these approaches rely on an opt-in and some private right of action. The approach taken in the European Union Communications

Directive emphasizes permission-based marketing and the need to ensure that even after opt-in is established, consumers retain the right to opt-out of online marketing lists.

Similarly, an extensive report from the Australian government on the spam problem released just last month urges the adoption of legislation based on prior consent where there is no preexisting business relationship; requires commercial electronic messages to contain accurate details of the senders names and physical and electronic addresses; and further recommends appropriate codes of conduct for marketers and effective means of enforcement.

Finally, a joint resolution issued in 2001 by the Trans Atlantic Consumer Dialogue, an alliance of more than sixty consumer organizations in the United States and Europe, recognized that the use of unsolicited commercial electronic communication is a growing burden for people who use e-mail. The TACD said, "governments need to work together to develop common approaches to address consumer concerns about unsolicited commercial e-mail." The group acknowledged the important differences between commercial and non-commercial speech, and urged the adoption of a policy based on prior affirmative consent.

Conclusion

Mr. Chairman, spam is a complex problem. There is no simple legislative solution. A multi-tiered approach that includes aggressive enforcement, better technology for identifying and filtering spam, and cooperation at the state and international level will all be necessary. In addition, baseline Federal legislation that gives users the opportunity to go after spammers and ensures that marketing lists are built on explicit consent and not on deception is a critical part of the effort to stem the tide of undesired commercial e-mail. Given the rapid increase in the spam problem in just the last two years, I urge the Committee not to delay action on legislation.

References

Prepared Statement of the Federal Trade Commission before the Subcommittee on Commerce, State, the Judiciary and Related Agencies of the Committee on Appropriations, United States House of Representatives, April 9, 2003 (Chairman Timothy J. Muris).

Coalition Against Unsolicited Commercial E-mail
<http://www.cauce.org/>

Commission Nationale Informatique et Libertés, website on spam.
http://www.cnil.fr/frame.htm?http://www.cnil.fr/thematic/internet/spam/spam_sommaire.htm

CNIL's Report on Spam
http://www.cnil.fr/thematic/docs/internet/boite_a_spam.pdf

EPIC Spam Page
http://www.epic.org/privacy/junk_mail/spam/

FTC Spam Page
<http://www.ftc.gov/spam/>

Federal Trade Commission, "False Claims in Spam" (April 2003)
<http://www.ftc.gov/spam/>

CAN-SPAM Act, S. 877 (Senators Burns-Wyden)
<http://www.spamlaws.com/federal/108s877.htm>

Internet Society, "All About the Internet: Spamming"
<http://www.isoc.org/internet/issues/spamming/>

Junkbusters
<http://www.junkbusters.com/>

National Office of the Information Economy, "Final Report of the NOIE Review of the Spam Problem and How It Can Be Countered" (April 2003)

David E. Sorkin, Spam Laws
<http://www.spamlaws.org/>

Directive 2002/58/EC of the European Parliament and of the Council Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector ("Directive on Privacy and Electronic Communications")
<http://register.consilium.eu.int/pdf/en/02/st03/03636en2.pdf>

TransAtlantic Consumer Dialogue (TACD), "Resolution on Unsolicited Commercial E-mail" (2001)
<http://www.tacd.org/cgi-bin/db.cgi?page=view&config=admin/docs.cfg&id=98>

The CHAIRMAN. Thank you, Mr. Rotenberg. Mr. Scelson, welcome.

**STATEMENT OF RONALD SCELSON,
SCELSON ONLINE MARKETING**

Mr. SCELSON. First off I would like to thank Senator McCain for inviting me here for this. I know I am probably the most disliked person in this entire room. I send close to 100 million e-mails out every 12 hours.

The CHAIRMAN. You have shown a great deal of courage by coming here today, and we appreciate it.

Mr. SCELSON. There are a lot of things, listening to you speak—

The CHAIRMAN. Pull the microphone closer.

Mr. SCELSON. Listening to you all speak, I originally had a speech just like these gentlemen, but being here today, I have to get a little bit more of a feel about the things people do not like and what the Government's aspects of this are, and the e-mails I send out right now, the reason I have gone back to being a spammer—I originally started out, spam was not known as spam back then, but eventually started becoming one—

The CHAIRMAN. How long have you been in business?

Mr. SCELSON. Fifteen years. The reason e-mail has grown is, people still buy. My average complaint ratio is 1,000 people complain, close to 2,000 removes in a mailing, and a 1 to 2 percent response rate. If it is hated so bad then why do more people buy than they complain about it?

Most of what the Government is not aware of, and certain ISPs, including Hotmail's newest filters that are here with us, leave out in detail to you all is, right now, the state laws, for instance, that say you have to provide a valid remove and ADV and a subject, their key filter, which was just updated on Thursday, I had broken as of Friday and released free to the other bulk mailers, has in there that remove word, unsubscribe, opt in.

Well, now, you tell me follow the law, do not send spam, be a good guy. I would be a good guy and mail in the Hotmail and AOL, no offense, and their filters will filter this out. Now, if I do not use this, I am then accused of being a spammer. I agree with all of the people here, there is no reason to use proxies, there is no reason to use relays, and a remove is a good option to add in there for people to use.

As far as the way we gather our addresses, most addresses for bulk snail mail are purchased from banks and a lot of companies. Your proposal to make extracting and gathering e-mail addresses and buying them is a good idea if this is also going to be added to the snail mail industry. What is fair for one is fair for the other.

Personally, I do not get addresses this way, so it does not affect me. Most of the gentlemen that are here all offer a member's directory and I am a paid member of all of these clients. This member's directory is identical to a Yellow Pages providing e-mail name, phone number, and address. To automate software, which I have done for clients to extract phone numbers and phone books, is the exact same technology that extracts their members directory, which

I am a paid member of, and this is granted free from AOL to give me access to all these users.

AOL does have the highest filter system in the world, no matter what anybody thinks. I do this every day. I give them full credit for this. The biggest thing I find, most people also seem to forget when it comes to this, is the carriers right now are deciding and filtering whose mail gets what. Whether you are going to read and see our mail or not, this is censorship. I was brought up and fought for this, and still fight for this, because I believe in freedom. As an individual, what makes us free is the freedom of choice, and that is who should decide whether or not they are going to receive this mail or not. The Senator here does not like receiving e-mail. It should be his choice to decide whether he is going to receive it or not.

I have heard the facts that it has risen the price of AOL and other companies' business to their customers, to increase pricing, and the burden of mail basically getting into their system. Some of these price increases are brought on by their own filters. At one time, you could send 100 messages, 100 people one message at a time, using less resources and less bandwidth. Their new filters now make it mandatory that we send one person one message at a time, thus chewing up their bandwidth and increasing their cost.

On our end, I have one location alone that is \$2,200 a week in bandwidth, so I keep hearing, the more we send, the less cost we have. The same bandwidth which you chew up on your end we are chewing up on our end. I am more than willing to work with any legislation to solve this problem. I agree spam is not the way to go. When I set up my company to not send spam and send 100 percent legal mail, we went above and beyond that to include a toll-free phone number, a physical address, a website, full information on the bottom of our messages, so that we were 100 percent we are above and beyond all common laws.

The areas such as Qwest, which I have lawsuits against some of these carriers, AT&T, BellSouth, AOL I have had dial up accounts through that they have also terminated. If you mail 100 percent legal and they get a single complaint, they will turn around and kill your circuit, so A, we go out of business, or B, we then resort to forging the headers.

The biggest complaint here is, you cannot find us. Well, if you could, you are going to shut us down, so why should we let you find us?

The laws definitely need to be made. I keep hearing there is no one simple solution. If you look at my written testimony, which it will take Government backing, and I am sure AOL's people would like to look at this as well, it states in there a very simple way that costs no money on AOL's end, no money on our end, makes the tax dollars go back to the Government, because if I stay here in the U.S. I owe you tax money for all the money I am making, the customers, et cetera. You pass the laws, we go outside the U.S., operations get moved outside the U.S., and from what attorneys have told me, if the corporation, the incoming money and everything is outside the U.S., there is no tax dollars owed in the U.S.

And basically, if you look at this system, it is very simple, to the point it does not cost money, and if the system's broken, that is

where legislation again would have to enforce it. It solves the whole problem.

As of right now the last carrier I was on was Covista. I was on them for 2 weeks, sending approximately 180 million e-mails a day. That is one e-mail per user in my database a day. I never send more than that. They shut me down for a total of 1,200 complaints. Well, when you look at the volume of mail I am pumping out, to get 1,200 complaints mathematically is nothing.

I do honor my removes. Even to this day, I send spam because I have to cloak my circuits to protect them from being shut down, but I still run, still have an honor, have a valid remove. It is not known as opt out, it is not known as a remove because the filters would interfere, but words such as take me off your list is very understandable to a person receiving it, and very much honored.

One of the other big problems in e-mail is, the anti-spam organizations preach, do not use the removes, we are confirming your address is good, we will not remove you. I cannot say there are not dumb people in the world. They are in every form of business and any walk of life, every nationality, it does not matter, but most companies I know of have the advanced technology that when I send an e-mail to Hotmail server, I know right out of the gate whether that address is good or bad, and if it is bad, instead of, because we have to force affirm addresses due to your filters, if that address is bad, my mailer will not send it to it, just to keep from clogging up anybody else's server, so since I know whether the address is good or bad or not, whether you ask to be removed, all that tells me is yes, you want the mail or no, you do not. I already know you are good. AOL, on the other hand's, system accepts everything, but AOL is nice enough to provide the undeliverable to everybody, so I still know if you are good or not.

Agreed, there needs to be a solution, but just do not take the freedom away from the individual. This should be their right and not the carrier's to say, we are going to shut you down and we are going to block you.

Most anti-spam groups that are fighting against spam are not Government-backed, Government-owned or anything. The reason Covista shut me down is that Spam House went to Qwest, which is Covista's carrier, and threatened to blacklist their entire network because every anti-filtering trick they hit me with did not work, and I still stayed 100 percent legal, and because of their threat Qwest passed it on down the line. I had to sue Covista for this.

Now, between everybody here, it is not their fault. I do not feel I should have to sue them, but that is the way the Government works. The anti-spam groups that have no legal right are interfering and forcing these people to shut us down. The Pink Contracts, which is what got me really well-known, everyone thinks they are contracts to send spam. I can show these contracts to you. There is not a single word in that contract to send spam. The details of that contract define every state, what its law is, and that if I send mail staying within every one of these laws, they will not shut me down, which I should not have a contract to have to do this.

My price for the bandwidth is three times higher when used for this particular means of doing it, and they still will step in eventu-

ally, once they get threatened enough, and shut you down, and most people are not aware of all of this. Most bulk mailers are scared to admit it because of the recourses that will happen. I have been fighting for so long that if I do not say anything and no one else does, then either everyone is going to really turn to the underground and become a really bad thing, or we can find a solution and work together.

AOL has AOL's special offers. I am assuming you are familiar with this. It is their own personal spam company. They spam their own users with it, and I have received at my Hotmail account from AOL special offers advertisements to sign up for AOL, so the same people that are here complaining about mail send mail. Why? Because it is profitable to the client and to them.

I am told there are a lot of cost factors in reading this e-mail, and the time it takes up on your end, Senator, when you read this e-mail, for you to go through it and push delete, which if we could use ADD you would know which ones are junk to make it a lot easier.

When you read this mail and push delete, yes, it took some of your time, but if you are at home where you do not have the extra assistance of the people around you, you have to walk outside, go get the junk mail out of the box, read this junk mail—do you ever think of how many chemicals, pollution, trees and all are involved in this, and then you have to throw it away, so if you add the time it takes you to deal with snail mail versus e-mail, both of them cost you time and money. E-mail is less on that comparison.

And that is basically all I have to say, and thank you again for having me here today.

[The prepared statement of Mr. Scelson follows:]

SCELSON'S ONLINE MARKETING
Slidell, LA

To Whom It May Concern,

My name is Ronald Scelson and I am the owner/operator of a commercial e-mail company that sends bulk e-mail as a form of advertising for companies over the Internet. I feel my company is doing no different than any other advertising company who uses the postal service to send out unsolicited bulk-mail to your home. The only difference is we send this information via the Internet instead of the United States Postal Service.

It all began with sending e-mail into newsgroups. It went from there to the sending of e-mail, as we know it today. At that time mail was just sent, we didn't care how. It was just pumped out and there were no removes. "Removes" is an industry term meaning—a hyperlink that will be sent back to the sender asking to have his/her e-mail address removed from your mailing list. When e-mail advertising started getting known by people as "Spam," my company was one of the first companies to get removes and valid "From" addresses. Now, in response to the commercializing of e-mails, some groups were formed as "Blacklisting" companies. For example, SpamCop started interfering and getting us blacklisted. Note: These companies are *not* government-backed nor funded, they are typical "everyday people" playing the role of a bully. Intimidating Internet carriers to cut off service to my company and other companies paying top dollar for Internet Service. My belief is that this business is doing a legitimate form of advertising and when done correctly, makes the client, government, and the commercial mailers money.

In response to the bully tactics used by the Anti-Spam hate groups, my company decided to go *Opt-In*. In order to do this, Commercial Mailers had to sign a contract with the carriers now known as "Pink Contracts." They are said to be Spam contracts to allow the sending of Spam under today's terminology. What these contracts were really for was to force us to pay twice as much money as a normal business would for Internet Service. Allow commercial e-mail to be sent not "Spam" to people without shutting us down. Now what this really means is that all states have laws

pertaining to e-mail and if you break this law the e-mail that is sent will be considered to be "Spam." This contract allowed us to send e-mail as long as we abide by every state law. Meeting all of the requirements indicated by individual state law will not be considered Spam. This would also not be in violation of any *ISP's (Internet Service Provider)* policy.

Now, when we sent the mail this way *Anti-Spam (groups of people against Commercial e-mail that post your private info on their site. They also violate and interfere with current laws)* groups would go to the carrier and tell the carrier "Hey! We've blacklisted them every way we can they are getting around it somehow so either you shut them down or we will shut you down!" Well, then the carrier shuts us down and breaks the contract. We have tried this with several companies. The last time we tried this doing it 100 percent legal the outcome was my circuit was shut down, we were put out of business and a major lawsuit—which to this day has still not been resolved. So, I was forced to go back to being a "Spammer," where I could keep my Internet connection live and support my family. I believe that there should be guidelines and Spam should be illegal. But the only way this would work is when the carriers realize *that we live in the United States and not a communist country!* They provide services that aren't different than any electric company. They get paid not to read, censor, and destroy people's e-mail, but to provide a service!

Now the individual has lost his/her right to get any e-mail he/she wants. The Carriers have determined that they would screen all incoming mail and only allow e-mail that the carrier wants the end user to receive. But not limiting themselves to their own advertising, that still to *this* day does not get screened. If I *were* to go into your Post Office Box, without your written permission, open your mail, decide what I think you should have or should not have, I would go to jail for this. This is exactly what the carriers are doing, The government says they want you to identify yourself and put "*ADV*" (*advertising*) in the subject and not forge your headers. If I mail 100 percent legal you come across two problems:

1. The carrier, not the individual, filters ADV, then none of my mail will get in and I will go out of business,
2. If I identify myself and not forge anything, the 'SP will terminate my circuit for mailing legal and put me out of business.

This is called legal mail, but I won't last a week and my line will be turned off for no legal reasons, except for the bullying power the anti-spam groups have. I agree with having laws governing bulk e-mails. But carriers should be held accountable when they submit to these anti-spam groups. Terminating service to companies; such as my own, without any legal reason to do so is not the democracy that we all should be living. I think it should be done the right way as long as the carriers know they will be shut down for blocking a company or shutting down a company doing it legally. Filters are designed for ISPs to eliminate "Spam". Most of these people that design these are "scam-artists." Think about it, if the server accepts mail in any way. Then there is a way to send bulk mail. If laws are passed to eliminate bulk e-mail, then the ISPs will shut down the commercial mailers. Then all the mailers are going to do is start corporations offshore and send their mail from offshore, now your laws and filters do nothing. Then, there is no taxable money being exchanged and money will be sent out of the country. This is not a solution, this is a joke!

I designed a system 5 years ago because I believe in the freedom of the United States and the company that I stand behind. We should have the right to do our business in a legal way with out any interference from someone whom has no say so in the matter. The system that can stop Spam gives the freedom back to the people, It is very simple and very cheap, especially when you look at AOT. who spent 11 million dollars last year to stop Spam and it did not work. Most people are not aware when you hit the send e-mail button what all happens behind the scenes. Mail servers talk together just like people, if you send an e-mail to *fjdjhfdhsj@hotmail.com* it will give an answer, error 550 user not available this means the address is no good. If you send it to *ronniescelson@hotmail.com* and my mailbox is full it will give an error 520 users mailbox full. Now my system is really simple and would be used by the individual not the carrier to stop Spam. They all have buttons in web-based e-mails example (Send mail) all you have to do is put an option "No Bulk E-mail" and put a check in the box. What this will cause to happen is when I send an e-mail to you, I will see an error (example: 420) at that point, I know this user does not want e-mail.

This could only work if legislature enacts a law that would require Commercial mailers to look for this error when mailing. They would also be held criminally liable if they ignore and continue to send mail to these accounts. If you mail without forged headers, a valid from address, contact information and "Adv" in the subject

they cannot shut you down or block you. If they do, there should be a fine imposed on the ISP. There would be no need for removes. Users are complaining they didn't ask to receive the mail so why should they remove themselves from 2000 plus different e-mail companies; they are right this system eliminates that problem.

Reporters have interviewed me several times on this issue; and the articles have always focused on the money being made and never mention the cost that "we" as Commercial Mailers have to put out. The bandwidth at just one location cost \$2,100.00/wkly, which is approximately \$110,000.00 annually just for one carrier. AOL says they spend millions stopping Spam. This is a cost factor they brought on themselves and are passing on to the consumer. They are spending money doing something they should not be doing in the first place. I find this to be illegal, immoral, and unconstitutional. An example of this, is if I take a *gun* and shoot someone, the gun doesn't go to jail for murder, I do. I, as a human, squeezed the trigger. Well, AOL puts a filter in place that reads, censors, and destroys legal mail THIS is illegal. They get away with this because they say a human does not read these messages, but a human did press the enter key to read and destroy mail. What is the difference? Some people state that snail mail is okay because you pay the post office to send it. We are more like private carriers like UPS and FedEx. (*UPS and FedEx are registered trademarks to the individual companies. They are not in any way affiliated with my company.*) A customer pays a private carrier to send mail. This company then pays the costs for fuel, drivers, and the truck to deliver the mail. As a customer pays us to send mail, we in turn pay for the servers, networking, electricity, and technology to deliver the mail. The ISPs say that "Spam" is chewing up so much bandwidth they are right at the end of capacity; this is their own fault. Part of ISPs Anti-spam filters do not allow high "BCC" (*blind carbon copy*) I could set my BCC setting to 500 for every 500 people who get this e-mail I will use up a total of 33k in size (est. the ad is 33k). Since this filter is in place, I have to mail at 1 BCC, which means that if I send an ad to 500 people then it would be like 500 times 33k. Now I have consumed 1.6 megabytes of bandwidth for those 500 people. So, now you see why their cost went up.

They say "Spammers" break laws, well here are some examples:

If we use *ADV* it, we are blocked.

If we use *Remove or unsubscribe*, we are blocked.

If we use the same "From" address that is valid, we are blocked..

If we send too many e-mails from one IP, we are blocked.

So, we have two options:

- (1) Break the law and stay in business or do it legal and go out of business. (Meanwhile these carriers continue to violate the laws that are passed and for a touch of proof if you go to this website there is a list of common filters look for yourself. http://www_mirror.ac.uk/sites/spamassassin.taint.org/spamassassin.org/tests.html)
- (2) If the government wants to pass laws it needs to be fair to everyone involved. The Commercial Mailers and the Carriers. But not allow these Anti-Spam groups to get away with threatening peoples lives just to feel that they have the power to control a company's destiny. Every state should have the same law to eliminate any possibility of violating these laws. This is necessary, due to the fact, that it is unknown where the recipient of an e-mail resides and whether or not you have violated any laws.

I don't believe you should e-mail private servers. *AOL, Hobnail, Yahoo* etc. provide consumers a service offering e-mail addresses. The consumer should have the right to choose to receive and sort his or her own mail, not the carrier. Laws and Censoring (*filtering*) e-mail are not going to work, it will only drive the price *up* for the smaller companies. As with the larger companies, like Norton's System Works,. Which sold more copies than ever before with e-mail. Due to the reduction of the marketing and merchandising costs, the product was made available to the consumer at \$39.95 in contrast to the \$299.99 retail cost in stores.

I consider myself living the American dream. I went to school in New Orleans where it was plagued by drugs and weapons. This is not what school was meant to be. I managed to survive the experience and ended up in a low-income neighborhood, still filled with drugs and violence. Even with a GED, I could not give my children the life I believe they deserve. So I started my own company and taught myself how to accomplish these things. In doing so, I found a way to create a business, provide for my family and put my children through a better school environment than I had. This to me *IS* the American Dream; freedom to grow and become something you dream of being. For doing this I was criticized, shut down, put out of busi-

ness and threatened. I hope by me coming forward, this will show the untold side of the story that these anti-spam groups don't want you to hear.

Please allow yourself to be open-minded and compare this industry to bulk mail. The differences between the two are that when you receive mail at your home, You open it, read it if you want, then throw it in the trash. You then have to carry that trash to the curb, where it is then hauled away and used as landfill (like we don't have enough trash already). Not to mention the trees that are cut down for the paper used! Then there is the Electronic Mail (E-Mail). If you don't want it, just check off DELETE. No mess, no cleanup, no pollution. I think my way is better!

If there are any questions or comments, or if I could be of any service, please don't hesitate to contact me.

Respectfully submitted,

RONALD SCELSON.

The CHAIRMAN. Did you say that it took you less than 24 hours to break one of Mr. Salem's filters?

Mr. SCELSON. Yes, sir.

The CHAIRMAN. How do you feel about that, Mr. Salem?

Mr. SCELSON. Excuse me, on his part, to defend him, something most people forget is, if a server accepts mail, obviously there is a way in. Unless the server does not accept mail there will always be a way in.

Mr. SALEM. So I think that it is pretty clear that spammers have an economic incentive to try to avoid filters. One comment that I will make is that the way our solution works, we actually have set up a very elaborate system that basically only receives unsolicited bulk e-mail, so any mail messages that are being blocked are not based on words such as remove or unsubscribe, or anything else, so what that means is, if you hit our decoys, by definition, that decoy never requested the mail, so we are able to say, yes, it is definitively spam, and what our customers contract us to do is block that mail.

I will tell you that we will continue the fight, because that is what our customers want us to do, and over the next couple of years I am confident we will solve this problem.

The CHAIRMAN. Mr. Leonsis, are you a spammer?

Mr. LEONSIS. Well, I would like to hire you.

[Laughter.]

Mr. LEONSIS. We would probably have a better relationship if you were on our side of the fence. I took a couple of notes during your comments, and very articulate, very heartfelt, and we have not raised prices to our members because of spam. We are absorbing that cost. We are taking an advocacy position for our members.

With AOL, when you sign on, and since you are a paid member you would know that there is a terms of service, and our privacy policy, and we do not allow any member or any company or any partner that pays us to spam our members. We have preferences that allow you to opt out of AOL e-mails, AOL pop-ups, and we promote that.

In fact, we have been actively promoting that off of our front screen, and so you have been violating TOSS, and I am sure you have been opening multiple accounts.

In regards to how they are getting e-mail addresses from member directories, that is a shame. AOL has always considered itself a community, and we have been able to get people to locate other people. My mother, as an example, died of breast cancer, and when she was sick she would go to the member directory to try and lo-

cate other women who were recently diagnosed with breast cancer. She certainly was not going to the member directory so that she could get e-mails that were unwanted or unsolicited or pornographic, and that is why that part of the business across the industry has shrunken, because people are gaining knowledge of what the tricks are and are now looking at their identity as being something that they need to protect.

So while I believe that marketing is important, I also believe that e-mail is not a medium, that e-mail is more a utility. It is something basic and fundamental. There are places on ISPs and places on services that you can buy advertising and reach out to members, it does not trick people, and we need to kind of separate out kind of the myths from the facts of how commerce is done.

The CHAIRMAN. Mr. Scelson talks about Pink Contracts. What do you know about that, and do you believe it is prevalent today, and I will ask Mr. Hughes and Mr. Rotenberg the same question.

Mr. LEONSIS. We are taking a different approach right now. We do not look at black lists.

The CHAIRMAN. My question is, do you know about Pink Contracts and do you believe it is prevalent today?

Mr. LEONSIS. I am not aware of how prevalent or not it is. What we have really done is say that how we look at what spam is, it is not our opinion, it is our members' opinion. We every day baseline where the complaints are coming, and the ones that rise to the top and get escalated, that is what spam is, and we have really no opinions on it. We have a very, very large, active community. We let them report in, and the numbers do not lie. When our members say, this is spam, that is when it gets blocked.

The CHAIRMAN. Mr. Hughes, do you know of the Pink Contracts that Mr. Scelson refers to, and Mr. Salem knows about them. Maybe I should ask him next. Go ahead, about the Pink Contracts.

Mr. SALEM. There are definitely relationships between marketers and ISPs, and oftentimes we are asked to make sure certain mail is not blocked. That is absolutely the case. As far as the details of those agreements, I am not aware of those details.

The CHAIRMAN. Mr. Hughes.

Mr. HUGHES. Clearly, we have heard of Pink Contracts, and as we understand it, Pink Contracts are paid for delivery contracts. I am not aware of any of my members engaging in those practices, but let me say that we truly are in a Spy v. Spy situation. We have heard on the other end of our panel here today that AOL on the one hand is building more robust filters day by day by day, and spammers on the other side are working at ways to avoid those filters.

As a result, the legitimate players in the middle delivering transactional messages, the consent-based marketing messages, have to build relationships with ISPs in order to make sure that wanted mail is actually delivered, and in some situations this is actually critical mail to have delivered. For example, it could be an airline ticket confirmation. It is a transactional message that is delivered in volume.

So I can tell you quite definitively that a year ago, 18 months ago, none of my members really had resources that were dedicated to ISP relationships. In other words, delivery relationships. Today,

most of my members have at least one, and sometimes they have full staffs.

The CHAIRMAN. I was referring to the relationship of spammers and ISPs. I am talking about the illegitimate contracts, not the one where you get an airline ticket.

Mr. HUGHES. Sure. We have definitely heard of the practice. I have never heard of it within our organization. There definitely is a place, though—I want to make sure it is clear, there is a place for a dialogue between senders and ISPs.

The CHAIRMAN. I understand there is room for dialogue between all the mail recipients and senders, but if there are contracts that go, that actually not only condone but contractualize the practice of spamming, then we have got an issue here.

Mr. HUGHES. I would agree.

The CHAIRMAN. Mr. Rotenberg.

Mr. ROTENBERG. Mr. Chairman, I am not familiar with the practice, but I do want to say briefly that I would challenge Mr. Scelson's assertion that he gets 1 to 2 percent response rate on his mailings. I find that very hard to believe.

The CHAIRMAN. Well, we will let Mr. Scelson respond, then. Go ahead.

Mr. SCELSON. I can pull lead stats from one of my servers off my laptop to show you what it did before filters were kicked in, after filters were penetrated. The 1 percent is the most average. There are a few exceptions, and one good exception to this was Norton System Works was a reseller, was a client of mine. AOL is very familiar with that one. I know they got hit hard with it. I think they also have a lawsuit involved in that one, too, if I am not mistaken.

The CHAIRMAN. Mr. Scelson, one of the things that disturbs a lot of us about this, and maybe you could comment on this, does it disturb you that so much of this is pornography, and occasionally child pornography?

Mr. SCELSON. Yes, sir, totally. I personally do not send any adult material, have not sent adult material, and do not intend to, no matter how this boils out.

The CHAIRMAN. But it is up to—I understand about 20 percent of the spam.

Mr. SCELSON. Yes, sir, it is, and most of the bad names that all e-mail companies get is not Norton System Works being sold that is really making people upset, it is the adult industry. Personally, you and I, even though I will not mail it, Playboy advertises that in the real world today nobody frowns on it. Why? Because it is kept very low key. There is no nudity, there is no vulgarity, unless you are a paid member. The porn you see in your e-mail today, all of us have seen, and it is just dreadful. My daughter is 9 years old, and she uses the computer quite well, and she sees this, so I understand where you all are coming from this, and totally agree with you.

The CHAIRMAN. My time has expired.

Mr. LEONSIS, you want to make a comment?

Mr. LEONSIS. I think as an ISP, as I stated earlier, we have a very strict covenant with our members on privacy and security. It is called Terms of Service, and we never enter into contracts to allow spam on our service. It is why the most egregious spammers

we are taking to court, and you have to read TOSS. It prohibits unsolicited bulk e-mail, and that applies whether you are one of our partners or not. We have people that pay us a lot of money, and sometimes it gets escalated to me on why cannot we spam, and we say, that is not what our rules allow, and so again, this is a utility function. You cannot just look at it as media, and an efficient way to deliver ad messages.

The CHAIRMAN. Well, again, I was not challenging your organization, but if the so-called Pink Contracts are in existence, then it is something we have to deal with.

Mr. LEONSIS. There are none in our organization.

The CHAIRMAN. But there is ample testimony that they are in existence.

Mr. SCELSON. Senator McCain, again the contracts are not to send spam. The contracts are to send e-mail that obeys all the laws. There is no such thing as a spam contract. If you are going to violate a law, I have not seen a carrier yet sign a contract for this.

The CHAIRMAN. Now we get into definitions. Senator Wyden, do you want to go, or Senator Burns? Either way.

Senator BURNS. I have a couple of questions, and I will tell you what I am going to do, I am going to set up a private little appointment with a couple of you, because we need to explore some of this a little bit further.

We have heard you may get legislation that has unintended consequences, and that worries me a little bit, and Mr. Rotenberg, you are exactly right about some of these areas.

As you know, I am a free marketer. I like that, and I do not want to get into a situation where we do have unintended consequences. In other words, when you come up here and serve in the Senate you sort of file back here the little saying that says, do no harm in everything that you do. I am wondering if this legislation—now, this is the first time I have run into Pink Contracts. Now, you would have thought I would have picked that up along the way, but us country boys, we do not pick up everything.

This tells me that should you pass a law that you are actually falling into forcing people into the grips of maybe an enterprise that another middle man in business that somebody does not want to pay just to get your message to a legitimate message of what you have a return address that you really want to do business on the Internet, but you are putting another middle man in there, injecting one in there that is going to drive the costs for both the consumer and the person that is doing business. Is that a false way of looking at things? It was not explained very well, but you understand where I am coming from.

Mr. SALEM. If I could make a quick comment, I think there has to be a way to identify legitimate marketers, and that is something that is going to become very, very important so that we can deliver messages from airlines or car companies, and so there is going to have to be relationships between the direct marketers and the carriers to make sure that that can happen, because what has happened to date is because some of those relationships do not exist. They are all being treated the same in many cases.

Mr. LEONSIS. Nine million reports a day on spam, and I cannot remember the last e-mail I received from an AOL member saying, please send me spam, so I understand the concern about erring, or the pendulum swinging too far, but it is way over here right now, and the laws that we are in discussion about today are very good steps, and as an industry we are going to work with our State AGs, and we need your help to get that pendulum back into a balance.

Senator BURNS. If anybody wants to comment on this, because it is sort of an interesting idea.

Mr. ROTENBERG. I think it is a very important point you make, Senator. Consumer groups are not against the use of the Internet for advertising. In fact, one of the wonderful things about the Internet for the consumer is the ability to get great prices on stuff you want, to be notified about books and authors that you are interested in, to get travel deals, and a lot of people are signing up for those lists to get that information because it frankly gives them a good deal.

The problem, and I agree with Mr. Leonsis, the pendulum has swung so far in terms of the amount of marketing that the stuff you desire is just getting drowned out. You cannot even find it any more, because there is so much junk you are getting with the commercial marketing that you would like to receive, so I think legislation is appropriate. I want to be clear on that point. I think there is always a risk of unintended consequences. I think legislation will help. I do not think it will solve the problem, but I am sensitive to this issue of not closing some doors you might want to leave open, and the question of state enforcement, particularly if they are issues around illegal business contracts, suddenly becomes very important.

Senator BURNS. Anyone else? I want to hear a comment from all of you, really, basically.

Mr. HUGHES. Senator Burns, this is clearly complex problem, and unintended consequences exist today. I would like to give you two dystopian visions of the future we have about e-mail. One is, we allow spam to proliferate, and all of us stop using e-mail because our inboxes have become so choked with spam. The other is, we use blunt instruments to solve spam, and in the process of fixing the problem we kill the killer app. We kill e-mail. That emerges in something called false positives. False positives are wanted messages that are unreceived because of a filter or black list or some other tool to block them.

What we have seen in the marketplace today, there is a study that came out from a company called Assurance Systems, is that in the fourth quarter of 2002 there was an average 15 percent false positive rate across the top 10 ISPs. That means 15 percent of wanted messages, of legitimate messages were not being delivered the inboxes of recipients. That is one of the unintended consequences of the blunt instruments that we are using. We need a much more balanced system to make sure that we kill spam but save e-mail.

Senator BURNS. Yes, sir.

Mr. SCELSON. Senator, I do totally agree there needs to be legislation on it. Again, the solution that is in my written testimony that I gave you all, you all have not got to see this yet. I am sure

you will see it before the end of the day. It is a no cost factor. It is very simple. There is no loss of unwanted mail, and one of the biggest complaints I have heard from people I send mail to is, there are over 2,000 bulk mail companies, not 200, that I am well aware in full existence out of 2,000 bulk companies you did not ask to receive mail in the first place.

Why should you have to remove from each one? The Government gets involved with the remove. Why should the Government have to spend tax dollars on a global remove system? The system I propose costs no money and gives the power back to the people.

The other thing I am looking for from the Government is, if I mail 100 percent within your laws, that companies like Brightmail will not filter the removes that are mandatory on us, and that carriers like BellSouth and AT&T and MSN will not come in and shut my circuits down for sending legal mail, and right now that is basically what they are doing, so I cannot reveal who I am, but they are right, we need to.

Now, the same people that fight the spam have websites up that I used to reveal exactly who I was, and everything about the company website, the whole info. These people have my children's school on their website, my children's social security numbers, they have threats in there that if nothing else can stop me, maybe we should do something to their family. They are not bluntly saying go out and hurt them, but they are pushing strong accusations. I have never seen AOL or you all do anything like this, but a lot of these big anti-spam groups that were at the FCC hearing, it is on their website. You have the Internet, look for yourself. All I ask is, open your eyes to see it all.

Senator BURNS. I am going to go to Senator Wyden now, but I appreciate those comments, and sure, we will take a very serious look at this, because I am still—we think we are on the right track with our piece of legislation, but that is not to say that we are written in stone of a better idea or something that could be incorporated with what we are doing, and we will probably explore that as we move along.

Senator Wyden.

Senator WYDEN. Thank you, Mr. Chairman. All of you were excellent.

Mr. Scelson, a question for you to see if I can get it straight. You said that you were above-board and complying with all the laws and trying to act in a straightforward way, but I think I also heard you say, and I just want to clarify this, that you are, in fact, disguising the source of the e-mail because you believe otherwise you are going to get blocked by ISPs, is that right?

Mr. SCELSON. Senator, that is a two-part question. I have not sent 100 percent legal mail in the last 6 months, since my last carrier breached a contract for sending legal mail. Since that time, again, if I send right off of one IP their systems detect how many e-mails come from one IP, will block this. If I send right off of my real IP, the carrier will come in and yank the circuit from me, so I have no choice but to hide this. I do not want this. If I am told today, you mail legal we will not shut you down, my spam days are over with. There is no need for spam. There are legitimate ways to do this.

Senator WYDEN. I understand that, and that is really what is at issue, and to your credit you are being very honest. What I think has concerned Senator Burns and I now for 4 years is that the bottom line is, is that the recipient of the e-mail cannot really tell where it is coming from, number 1, and number 2, if the recipient, again empowering the consumer, wants to tell the ISP to do certain things to protect them, the recipient is not in a position to do it. That is why we are trying to come up with a legislative solution here.

And just a couple of other points. Is there any dispute among you five about the urgency of this effort, because I will tell you, it just seems to me that the volume of spam today really has the potential of poisoning the medium, and doing it in a real hurry.

If you look at how fast it is going, I have been at this for three or 4 years now, and I am going to be looking at Senator Nelson, who has an attractive idea, and Senator Schumer has an attractive idea, but you know, those ideas of sending it to the Federal Trade Commission for 45 days, giving the exponential growth, I want us to move now, and I would just like to make sure that all of you are clear for the record how urgent this is, and if it is not done quickly, you are really talking about the potential to poison this medium.

Mr. HUGHES. Senator, if I could, we needed legislation last year, we needed it yesterday, we need it as soon as possible, but more important than Federal preemptive legislation is, once we have that, we need strong enforcement. Legislation will be useless unless we create the deterrent effect that it is intended to create, so we are very supportive of legislation today.

Senator WYDEN. I will tell you that beyond the fact that the Federal Trade Commission 2 years ago said that the enforcement model on the Burns-Wyden bill worked well, I am absolutely convinced, having worked on these issues since the days when I was Director of the Gray Panthers, that you bring a modest number of enforcement actions—you are not going to have to bring hundreds, but you bring a modest number of enforcement actions that are tough, that send a real message out there, that there are going to be consequences, that there are going to be significant consequences, and I think you change the world out there in the cyber arena.

The only other point I wanted to make sure we were on the record, Mr. Rotenberg, you know I have enormous respect for you and what your organization does. We work with you on everything from the total information awareness program to CAPS, privacy issues and the like, but clearly what the states are doing is not working. We have got 30 states now that have enacted anti-spam statutes. If this was going to be solved at the state level, it would seem to me what the states would have put together collectively would have been more effective. Do any of you disagree with the proposition that Senator Burns and I have been advancing that this has got to be dealt with at the national level?

Mr. SALEM. Just a couple of comments, Senator Wyden. First, there is definitely an urgency on this problem right now. A lot of the state legislation has talked about labeling. Labeling has not proven to help us solve the problem, so I think that is something

that does need to be looked at as your bill continues forward. I think the other thing that I would say is that we are going to need to invent some technology, because in my testimony I said 90 percent of e-mail today is untraceable, so there is some form of deception that is making it hard to identify who is sending it, and that is why I am surprised it took 24 hours.

I think that is good, because we actually have data filters every five to 10 minutes to try to stay ahead of the spammers, because that is what is required to block and keep spam out of inboxes, so we absolutely support what you are doing. We would like to continue to help shape it so that it can be enforced, but there is going to have to be some technology invention so we can track who is the originator of that mail.

Senator WYDEN. It is a fair point, and that is one of the reasons we tried to give a wide berth as it relates to the enforcement tools. We have got four enforcement tools, we have got flexibility for the Federal Trade Commission, because we know that the spammers are not technological simpletons. They are people who are constantly going to be on the cutting edge, and you can act on Tuesday and they will be devising something on Thursday.

The last point that I wanted to ask about was the question in the *New York Times* report yesterday that indicated that in the last 2 years 200,000 computers worldwide had been hijacked without the owners' knowledge, and are currently being used to forward spam.

Now, in our legislation, we say that you cannot use an originating e-mail address the access to which was obtained by means of false or fraudulent pretenses or representations. We think that that might have been a useful tool had it been enacted to try to prevent the hijacking, but I am going to turn this over to Senator Nelson to wrap up.

We would just like you to look at that language, because it may need some tweaking, but my sense is that had that part of the Burns-Wyden bill been on the books, that could have been used to derail that very serious hijacking situation, and we would like you to work with us, and I am not saying this is the last word.

Mr. ROTENBERG.

Mr. ROTENBERG. I wanted to say we very much supported the efforts to pass Federal legislation. We think it is necessary. We think your bill is a good model. We completely agree that there has to be a strong national approach. I think the FTC has done good work and the workshop was good, and I think the enforcement intentions are there.

As I said, I think the real concern is simply, if you close the door on the states, which is not to say that they solved the problem, but if you largely prevent them from pursuing the problem, then I think that raises some problems, but beyond that, I think there is a lot of support in the consumer community, and it was the consumer groups actually a couple of years ago, to their credit, that said we have got to get a handle on the spam problem, because otherwise the Internet is going to be largely useless in terms of consumer use, and the groups that we have worked with have said, make this a priority, so I think if it can be done right, it will be a great accomplishment.

Senator WYDEN. You are absolutely right. We would not be anywhere near where we are without the consumer groups, and you are absolutely right on that point. The reason that Senator Burns and I give that activist role to the state Attorneys General to bring actions is that we think, again, that they bring a modest number of those actions, and that is a significant deterrent.

And my final message to you five, because you have been excellent, keep the heat on us and do not let the Congress dawdle on this. At every possible stage for the last three or 4 years Senator Burns and I have been up against this argument. Well, now is not really the time. We need to study this. We need to send it to the Committee on Acoustics and Ventilation and let them look at it for another 6 months, and we cannot afford it. Ted Leonsis has made the point that this has grown so dramatically that we cannot afford to let that happen.

There are a lot of good ideas in the Congress. We should look at them. You should tell us how to make them fit into an integrated system, but my message is, do not let the Congress dawdle now, do not let the Congress delay, so that we can get this passed.

Mr. Chairman, are you going to chair? I know Senator Nelson had some questions.

Senator BURNS. I do not have any more, and it is almost lunchtime, and I have never missed a meal and by God I do not plan to.

Senator NELSON. Well, you can just turn the Committee over to me.

[Laughter.]

Senator BURNS. We already did that a while ago and it did not work, Senator.

[Laughter.]

Senator NELSON. We got a lot of business done while you were gone.

Senator BURNS. You proceed on, please, Senator. We signed on for the term.

Senator NELSON. Mr. Chairman, one of the characterizations that I would modify in some of your characterizations, your concern naturally about impeding the normal intercourse of commerce, and that is a legitimate concern also expressed by Mr. Scelson, but the difference, I think, that I would look at it, you gave the example of walking down the street and seeing advertisements, and that is in a public domain.

I think when you get into personal mail coming into a personal box sitting in your personal home, then it is a little bit different, and that is what I think rises this to the level of concern where I think we are going to have to have some criminal laws applicable. I would love to have your response to that.

Mr. SCELSON. Senator, based upon what you said is basically the reason I am fighting. That choice is the individual's right. No offense to any of these individual companies. They should not decide if they are going to censor, read or destroy your legal mail. As an individual, that should be that person's right to decide. If the carriers did not shut you down for doing it the right way, ADV is a way that as soon as you open your e-mail you know you can get rid of it. My IPs would never change. If the individual wanted to

block me, I have no problems with this. It is the companies that are going in and destroying your mail.

If I go to your office and decide to go snoop through your mail and decide what you are going to get, I am not going to make it out the front door without going to jail, but at the same time, these filters are taking from your rights. They say a computer is doing this. There is nothing wrong with it. A human does not see this. Well, as an example, if you shoot someone with a gun, the gun shot him, not me. But I am a human, I squeeze that trigger, I am responsible.

When they filter and censor people's mail, a human is sitting in that entity. A human is responsible for destroying your private mail. It is the same scenario. What you are saying is absolutely correct.

Senator NELSON. Well, the temporary Chairman characterized the problem at one point as weeds, weeds growing up, you use some Round-Up on them, get rid of the weeds, and I interjected with a big smile on my face. I said, it is not weeds, it is snakes in the weeds, and when the pornography starts coming at me, I think that is poisonous snakes, and that is where we have got to figure out some way to draw the line.

Let me just ask one final question. Twenty-nine states have grappled with this, the most recent of which is Virginia, which has the strongest law, and so since Mr. Leonsis is from Virginia, what do you like about the new Virginia law, and are there parts of that that could serve for us to incorporate in this Federal legislation?

Mr. LEONSIS. Well, the Virginia law really worked in tandem with what we can do commercially, and where we like the law, it really does give teeth especially to the Attorney General, and I think in all cases at the state level it is the Attorney General who has to go in and do the biting, and I think what is really important is that there be a rules of the road on a national level, and the states, looking at their individual laws we will have to deal with, it would be much better if we had a unified view from the top down, but we always need to be able to empower the AGs to go execute the law state by state.

Senator BURNS. If the Senator would yield, what drove us in this direction, Senator Nelson, was the fact that some of us that has been here for a day or two know and understand and see the ramifications of trying to pass legislation that one size fits all for 50 states, and it does not work. We tried to write policy in agriculture, I mean, a host of things that it just does not work, so that is the reason we did not want to take a giant step that erodes the state's ability to deal with the situation. That is the reason we went down the road we went down.

Senator NELSON. Well, I would just give in response, from the basis of my experience when I was in the state legislature in the 1970s, I passed the first computer crimes law in the Nation, giving prosecutors the tools to go after the more sophisticated type of criminal that was using a computer instead of a crowbar.

When I came to Congress, I passed the Federal computer crimes law. Now, it was a law that had Federal application, but it supplemented what the states were starting to do, and we have got to kind of find this balance. I can understand Mr. Scelson. He would

be going nuts if he had to deal with 50 different state standards, and so somehow you have got to have perhaps if there is a stronger standard in a state, that that takes precedence over the Federal law, but that there would be a uniformity with the Federal law to which they could then comply.

Mr. SCELSON. Excuse me, Senator, what I am about to tell you has never been challenged before, and very few people are aware of this. There is a website called *w3c.com*. It is all the guidelines that were presented by the Federal Government when the Internet was released to the people. In those guidelines it states, "states do not have the right to pass laws pertaining to the Internet." It has not stopped anyone. It has not been changed on that site, so if that is true, then Federal law is the only way to go with this, but as of so far, no one has ever fought or challenged this to my knowledge.

Senator BURNS. Well, thank you, and Senator Nelson, we thank you for your participation. We are going to leave this record open for a couple of weeks if there is something else, and there are other Senators that will probably want to make inquiries, so if there are, you can respond both to the Senators and the Committee, and we thank you for your testimony today, and this Committee is adjourned.

[Whereupon, at 12:30 p.m., the hearing was adjourned.]

