S. HRG. 108–1024

# REVIEW OF THE CAN-SPAM ACT AND NEW ANTI-SPAM INITIATIVES

## HEARING

BEFORE THE

## COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION UNITED STATES SENATE

ONE HUNDRED EIGHTH CONGRESS

SECOND SESSION

MAY 20, 2004

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

U.S. GOVERNMENT PUBLISHING OFFICE

21–618 PDF WASHINGTON : 2016

For sale by the Superintendent of Documents, U.S. Government Publishing 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

SECOND SESSION

JOHN MCCAIN, Arizona, *Chairman*

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



WITNESSES

# REVIEW OF THE CAN–SPAM ACT AND NEW ANTI-SPAM INITIATIVES

**THURSDAY, MAY 20, 2004**

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

The Committee met, pursuant to notice, at 10:20 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. I'd like to thank the witnesses for their patience. The Republicans had a meeting with the President this morning. I'm sure he'll schedule one with my Democratic colleagues soon. And so I appreciate your patience, and we'll now proceed with the hearing.

Today, the Committee will examine the effectiveness of the CAN–SPAM Act of 2003 aimed at curtailing the proliferation of spam in America. Since our review of this issue last May, the volume of spam received by American consumers has risen unabatedly. Spam now accounts for anywhere from 64 percent to 83 percent of all e-mail traffic on the Internet. Just a year ago, spam constituted only 45 percent of e-mail traffic. Additionally, a Pew survey on "Internet & American Life" released this past March found that 77 percent of e-mail users are receiving the same amount or more spam since the law was passed. As a result, 30 percent of those surveyed have reduced their use of e-mail, up from 25 percent last year who did the same. The rising tide of spam is driving nearly a third of consumers away from using e-mail, a result that could well impact Internet usage and, consequently, the future financial health of our telecommunications online retail and information technology industries.

I am reminded of Commissioner Swindle's apparently prophetic testimony before us last year when he said, "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."

Fraud and the decline of e-commerce are not our only concerns with spam, because spam is used as a delivery mechanism for pornography, viruses, and applications enabling identity threat and the hijacking of consumers' computers for malicious purposes. Every percentage increase in the volume of spam in turn increases

the risks and prevalence of cybercrime as well as cybersecurity threats to our Nation's critical infrastructure. I thank the FBI for appearing today to discuss its efforts to combat these dangers.

I voted with other Senators to unanimously pass the CAN–SPAM Act by a vote of 97 to zero last fall. I reminded my colleagues, at the time, of my repeated statements that legislation alone would not solve the problem of spam. But the fact there is no silver bullet to spam does not mean we should stand idly by and do nothing.

We should, at the very least, enforce the Act by the most effective means possible. If spammers continue to win a technological game of hide-and-seek with ISPs, the FTC, and the FBI, then the law will have little effect at stopping spam. I do not believe, however, that authorizing broad private rights of action will improve enforcement efforts. If industry and government authorities spending vast resources in this effort can only muster enough evidence to bring a grand total of eight spam cases over the past 5 months, then private rights of action will produce little more than expenses for legitimate businesses to fend off opportunistic trial lawyers. Spammers will remain at large.

If the FTC can't find the spammers, it should do the next best thing, go after the businesses that knowingly hire spammers to promote their goods and services. The Act gives the FTC the tools to do so in Section 6. The FTC should use them. The businesses promoted by spammers take credit cards. They are established businesses, and they are liable under the Act for using falsified e-mail to promote their sites, even if what they sell there is not fraudulent or otherwise illegal. At a minimum, the FTC could put thousands of businesses, many of them online pornography retailers, on notice that using anonymous spam is an illegal means of driving consumer traffic to their websites. Using its authority to get out this message, the FTC could help dry up the market for the use of deceptive spam as a marketing tool, and, thereby, reduce the amount sent to consumers.

In the long run, though, I continue to believe that dynamic market-based efforts have a far better chance at defeating the ever-changing global technological maneuvers of spammers than anything we can write into our static laws.

[The prepared statement of Senator McCain follows:]

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

Today, the Committee will examine the effectiveness of the CAN–SPAM Act of 2003 at curtailing the proliferation of spam in America. Since our review of this issue last May, the volume of spam received by American consumers has risen unabatedly. Spam now accounts for anywhere from 64 percent to 83 percent of all e-mail traffic on the Internet. Just a year ago, spam constituted only 45 percent of e-mail traffic. Additionally, a Pew survey on Internet & American Life released this past March found that 77 percent of e-mail users are receiving the same amount or *more* spam since the law was passed. As a result, 30 percent of those surveyed have *reduced* their use of e-mail, up from 25 percent last year who did the same. The rising tide of spam is driving nearly a third of consumers away from using e-mail, a result that could well impact Internet usage and, consequently, the future financial health of our telecommunications, online retail, and information technology industries.

I am reminded of Commissioner Swindle's apparently prophetic testimony before us last year, when he said, "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 con-

sumers lose confidence in web-based services and turn away, tremendous harm will be done to the economic potential of information technology."

Fraud and the decline of e-commerce are not our only concerns with spam. Because spam is used as a delivery mechanism for pornography, viruses, and applications enabling identity theft and the hijacking of consumers' computers for malicious purposes, every percentage increase in the volume of spam in turn increases the risks and prevalence of cybercrime, as well as cybersecurity threats to our Nation's critical infrastructure. I thank the FBI for appearing today to discuss its efforts to combat these dangers.

While I voted with other Senators to unanimously pass the CAN–SPAM Act by a vote of 97–0 last fall, I remind my colleagues of my repeated statements last year that legislation *alone* would not solve the problem of spam. But the fact that there is no silver bullet to spam does not mean we should stand idly by and do nothing.

We should, at the very least, enforce the Act by the most effective means possible. If spammers continue to win a technological game of hide-and-seek with ISPs, the FTC, and the FBI, then the law will have little effect at stopping spam. I do not believe, however, that authorizing broad private rights of action will improve enforcement efforts. If industry and government authorities spending vast resources in this effort can only muster enough evidence to bring a grand total of 8 spam cases over the past 5 months, then private rights of action will produce little more than expenses for legitimate businesses to fend off opportunistic trial lawyers. Spammers will remain at large.

If the FTC can't find the spammers, it should do the next best thing: go after the *businesses* that knowingly *hire* spammers to promote their goods and services. The Act gives the FTC the tools to do so in Section 6—the FTC should use them. The businesses promoted by spammers take credit cards; they are established businesses; and they are liable under the Act for using falsified e-mail to promote their sites, even if what they sell there is not fraudulent or otherwise illegal. At a minimum, the FTC could put thousands of businesses—many of them online pornography retailers—on notice that using anonymous spam is an illegal means of driving consumer traffic to their websites. Using its authority to get out this message, the FTC could help dry up the market for the use of deceptive spam as a marketing tool, and thereby reduce the amount sent to consumers.

In the long run, though, I continue to believe that dynamic, market-based efforts have a far better chance at defeating the ever-changing, global technological maneuvers of spammers than anything we can write into our static laws. I thank the witnesses for being here today and look forward to their testimony.

The CHAIRMAN. I thank the witnesses for being here today, and look forward to their testimony.

And I am pleased to be with the two major sponsors of this Act, Senators Burns and Wyden, who are here today, and I'll go to Senator Wyden.

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

Senator WYDEN. Thank you, Mr. Chairman. I think you've given an excellent statement to summarize where we are, and I'd just make a couple of points in addition.

What Senator Burns and I have contended for some time is, this is just the beginning, this is just the start of the effort to drain the swamp. And the challenge is to send the strongest possible message to the kingpin spammers, that relatively small number of people, maybe 500 people, who are generating a significant part of the problem. In the past, they have been able to flood America with this garbage and face no consequences. So the challenge now is to come down on the kingpin spammers with hobnail boots so that, for the first time, they understand that when they try to have their way with our computers and America's technology, that they are going to face, for the first time, real penalties.

In addition to that, what we have got to continue to focus on is the correct combination of the legal tools, which is what the Burns-

Wyden legislation tried to zero in on, technological measures, and international cooperation. And there have been some new developments with respect to the international cooperation issue that I'm interested in exploring. Mr. Muris and I have already touched on one. Apparently, there is a new U.K.-based anti-spam company that has found that between 57 and 60 percent, and 57 and 67 percent, depending on the methodology that's being used, that that analysis found that the majority of spam, that large amount, originated within the United States. If that analysis is right, it suggests that most of the kingpin spammers are, indeed, subject to U.S. law and within the reach of U.S. enforcement authorities. But with the right combination of legal tools, technological measures, and international cooperation, I think that there are the possibilities of generating a new day, a day when these kingpin spammers face real consequences, serious risks, and no longer can enjoy an easy ticket to a free lunch.

It is very helpful that you're holding this hearing, Mr. Chairman, in order to be able to keep the heat on, and I look forward to working with you and Senator Burns and Senator Nelson, who's had a longstanding interest in this and added some valuable components to our legislation. I'm glad we're continuing this.

The CHAIRMAN. Senator Burns?

Thank you. Senator Wyden.

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

Senator BURNS. Mr. Chairman, thank you for these hearings, and I'll put my statement in the record, in the essence of time, because we got——

The CHAIRMAN. Without objection.

Senator BURNS.—pushed back a little bit.

But I'd like to make a couple of points here this morning. You know, this Act has been in effect 141 days. And with all the activity—the civil actions brought by the big ISPs, is one of them—and then, in Detroit, whenever the U.S. Attorney's Office in Detroit and the U.S. Postal Inspection Service went through their joint effort of cracking down on some unlawful spammers there, that was—and as long as these headlines hit the newspapers, as long as we keep taking these people out, it makes them a little more expensive to operate, we will finally get to the bottom of all of this.

And so I think it has been effective, and it is a giant first step. We didn't have this before. And as the law matures, as we look at different actions that are being taken, both by the states' attorney generals and the United States Attorney General, and also it empowers the users of computers to also file suits and to get into the Act and take care of part of this, we will see what works and what doesn't work. And maturity actually will tell us what we have to do in the future. It will not be testimony, I think, or changing the law at the present time.

But I still think CAN–SPAM will play a strong role in reducing the amount of spam. I know mine's going down a little bit, but not much. But I just—I'm a great guy on that delete key.

But we said that this is not the law, the end-all of spamming, because it's elusive and it's hard to identify, and it's hard to get

to the perpetrators. But today's—we should learn some more with today's witnesses, and I look forward to hearing from them.

And thank you, Mr. Chairman, for having this hearing.

[The prepared statement of Senator Burns follows:]

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

Mr. Chairman, thank you for holding today's hearing on the implementation of the CAN–SPAM Act.

The proliferation of junk e-mail, or "spam" has been the scourge of the digital age. Billions of e-mail messages per day, more than half of e-mail traffic, are spam. Spam costs consumers and businesses an estimated $10 billion per year due to expenses of anti-spam equipment, manpower, and loss of productivity.

The high cost of spam and the frustration that has been felt by businesses and individuals over the past few years are what prompted my colleague, Senator Wyden, and I to author the CAN–SPAM Act, which was signed into law by the President late last year and went into effect on January 1. The CAN–SPAM Act has empowered consumers and given the Federal Trade Commission and the Department of Justice the tools that are necessary to curb the deluge of spam. Internet Service Providers are also given strong tools to go after illegal kingpin spammers under the Act. While it will still take time before the full effects of the law are known, I would like to highlight the positive action that has taken place since the law went into effect.

Three weeks ago the FTC filed criminal complaints against four Detroit-area men accused of creating massive e-mail chains marketing fraudulent weight loss products. Through the combination of old and new investigative techniques, the authorities were able to gather enough evidence to bring charges against four individuals. All the suspects were surprised by the arrests, and one man in particular was described by his lawyer as being "absolutely shocked."

Kingpin spammers should be shocked no longer that they must pay for their actions. As more and more of these arrests occur and the word gets out that illegal spamming can lead to massive financial and criminal penalties, a significant deterrent effect will take place. Already, some of the Nation's worst spammers have indicated that because of the CAN–SPAM Act, they are looking for new lines of work. I applaud the U.S. Attorney's Office in Detroit and the U.S. Postal Inspection Service for their joint effort in cracking down on unlawful spammers.

I would also like to highlight the civil lawsuits that were brought against hundreds of spammers in March by America Online, EarthLink, Microsoft and Yahoo. I am pleased that these companies were so quick to use the provisions in the CAN–SPAM Act that allowed businesses to fight back against spammers. I look forward to following these cases as they play out in court.

The CAN–SPAM Act has been effective for a mere 141 days. In these short few months, consumers, the Federal Trade Commission, the Department of Justice, Internet Service Providers, and many others have had to digest the new law and learn how to best utilize it to fight the seemingly endless battle against spam. I am pleased that in this time, the FTC, DOJ and others have begun to use the new law to tackle some of the most vicious kingpin spammers. As time passes, I am confident that CAN–SPAM will play a strong role in reducing the amount of spam that Americans are forced to deal with on a daily basis.

The CAN–SPAM Act alone, however, is not the sole solution to unsolicited e-mails. Technology has an important role to play in cutting down on the spam that reaches an individual's inbox. I look forward to hearing about the new anti-spam initiatives that companies are developing to help block unwanted messages.

The CAN–SPAM Act is a valuable piece of legislation that provides consumers, business and the government with the tools necessary to fight spam. But the Act is only as good as the enforcement of the law. Successful enforcement of CAN–SPAM along with new technological advances will bring about the reduction in spam that so many Americans need and deserve. Thank you, Mr. Chairman.

The CHAIRMAN. Senator Nelson?

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

Senator NELSON. Thank you, Mr. Chairman. And my compliments again to the leadership of these three gentlemen seated

here at the dais with me for bringing into public policy something that the American people are so upset about. Thank you for doing all that you've done.

Thank you for letting me participate in the process, of which the Sentencing Commission still is working on their final recommendation, which will be coming in a few months, with regard to higher criminal penalties. And hopefully that will just, all the more, make this legislation effective.

And although we've had some mixed results, clearly there have been some very positive developments. And in the course of this hearing, what I would like is—as the FTC speaks to us, it's my understanding that half of the staff members of the Bureau of Consumer Protection currently are working on CAN–SPAM issues. And I understand that the staff in the regional offices, a good portion of that staff, is working on these issues. And I'm hopeful that these staff resources are adequate to enforce this Act, and, if not, would like to know if you need more resources.

I want to applaud the FBI, as well, the attention that they have given to fighting spam. A lot of this spam originates outside the United States, but it's sent to our folks here. And so I'd like to know to what extent is the FBI able to partner with its foreign counterparts in order to reduce spam? And what do we do through such international crime organizations such as Interpol? And to what degree have you found that spammers are designing new technical methods to evade law enforcement? And is the FBI able to keep up with the technological advances made by spammers? And if the Sentencing Commission comes out with stronger recommendation on sentences, will that help you in the law enforcement community?

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you.

We'd like to welcome our witnesses: Mr. Timothy Muris, who is the Chairman of the Federal Trade Commission; and Mrs. Jana D. Monroe, Assistant Director, Cyber Division, at the FBI.

Before we take your testimony—accompanied by Mr. Larkin, for the record—is Mr. Larkin accompanying you, Ms. Monroe?

Ms. MONROE. Yes.

The CHAIRMAN. Would you identify his position, please?

Ms. MONROE. He is the Unit Chief with our Internet Crime Complaint Center.

The CHAIRMAN. Thank you.

And before we proceed, Mr. Muris, I don't think this will be the last time you testify before our Committee, because you will remain a valuable asset and a source of information and assistance to this Committee for many years, but this may be the last time as Chairman of the Federal Trade Commission—I hope not, but likely it may be—and I want to take this opportunity to thank you for your outstanding service, your honorable work, and your efforts on a broad variety of very important issues to the American people. And I think you can take great pride in the bipartisan support that you have received and the way you have performed your duties, and we thank you for that, and we wish you good luck in your future endeavors.

Mr. Muris?

**STATEMENT OF HON. TIMOTHY MURIS, CHAIRMAN, FEDERAL TRADE COMMISSION**

Chairman MURIS. Thank you very much for those very kind words, Mr. Chairman. I greatly appreciate your support and leadership regarding the Federal Trade Commission; indeed, the support of the whole Committee. I do understand, from the newspapers, I actually may be staying a little longer, so I am certainly willing to do that, and am always available to testify. And I wanted to thank you for this chance to discuss spam, and thank you and the Committee's leadership on these issues.

Spam obviously creates problems well beyond the aggravation that it causes. The problems include fraud and deception, the offensive content, the sheer volume, the security issues that are involved when spam includes spyware or viruses. Combating spam has been one of our top priorities. We have over 50 staff members working on CAN–SPAM. It's half of our largest unit within the Bureau of Consumer Protection that's working on this issue.

We've pursued a threefold strategy. First is a vigorous program of law enforcement against spammers, both before and since the enactment of CAN–SPAM. Second, we engage in extensive education to consumers and businesses. And, third, we study spam extensively, because there's a great lack of reliable information about spam.

We've brought 62 law enforcement actions against alleged fraudulent operations against spam, the vast majority of those in the last few years, since we've—under my chairmanship and the growing problem of spam. Most of these cases obviously predate CAN–SPAM. And we use Section 5 of our statute, which prohibits unfair or deceptive acts or practices.

Our two most recent cases, Phoenix Avatar and Global Web Promotions, were filed last month, that involved extremely prolific amounts of spam. We allege three violations of Section 5(a) of the CAN–SPAM Act, specifically that the defendants failed to provide a clear and conspicuous notice of the opportunity to opt out, they failed to disclose a valid physical postal address, and they used materially false or misleading header information. This last practice, known as "spoofing," the spammers place the e-mail address or domain names of unsuspecting third parties. The complaints also allege violations of the Federal Trade Commission Act.

In Phoenix Avatar, we obtained a PI, preliminary injunction, against the corporations, and a temporary restraining order against the four principals. This stopped further deceptive product sales, froze their assets, and preserved their records. We worked closely with criminal authorities, and the U.S. Attorney in Detroit filed a criminal complaint, executed a criminal search warrant, and arrested the four principals.

Global Web Promotions targets an Australian company and two individuals living in New Zealand who were allegedly responsible for massive amounts of spam to this country. They used the spam to advertise a diet patch similar to the one in Phoenix Avatar, as well as a growth hormone which purportedly would extend your current biological age. Because they used fulfillment houses in the United States to ship their products, we obtained a PI to enjoin

further delivery of those products, and froze their assets that were located here.

Besides enforcement under CAN–SPAM, we've been working hard to complete the rulemakings and reports that are required. On April 13, we issued a final rule with a marker notice to identify spam-containing sexually-oriented material. Effective yesterday, all such messages have to include the warning "sexually explicit" in the subject line, and the rule prohibits sexually explicit material in the subject line or in the part of the message that recipients initially view. And we've already begun searching for enforcement targets.

In March, we issued an advance notice of proposed rulemaking to define the relevant criteria for determining the primary purpose of e-mails subject to CAN–SPAM's provisions. At the same time, we've requested comment on other issues that gave us—for which the statute gave us discretionary rulemaking authority.

We've received over 12,000 comments, and our staff is incorporating the suggestions and recommendations for these comments into the proposed notice of—notice of proposed rulemakings, which they will forward to the Commission for its review.

The Commission is also preparing several reports under CAN–SPAM, and the March ANPR solicited comments on them, particularly a plan and timetable for establishing a National Do Not E-Mail Registry, and an explanation of any—under the statute, any practical technical security, privacy, enforceability, or other concerns about such a registry. We will meet the June 16 deadline, and will obviously be available at your will, Mr. Chairman, to discuss that issue privately or publicly.

We've also engaged in a lot of other endeavors to supplement our knowledge regarding that in our other reports. We've transcribed interviews of dozens—with dozens of interested organizations. We've used compulsory process to several ISPs and other entities. And we've issued a Request for Information from vendors for creating a Do Not E-Mail Registry. We've retained expert consultants. We're also gathering information for other reports.

To conclude, e-mail clearly provides enormous benefits. I think your quotation from my colleague, Commissioner Swindle, was completely on point. The increasing volume of spam, coupled with the use of spam to perpetuate fraud and benefits had put the benefits of e-mail at serious risk, and we will continue our law enforcement education and research efforts to protect consumers and businesses.

Thank you.

[The prepared statement of Chairman Muris follows:]

PREPARED STATEMENT OF HON. TIMOTHY MURIS, CHAIRMAN, FEDERAL TRADE COMMISSION

Mr. Chairman, the Federal Trade Commission appreciates this opportunity to provide information to the Committee on the agency's efforts to address the problems that result from unsolicited commercial e-mail ("spam"), its activities undertaken to date to fulfill the various mandates contained in the Controlling the Assault of Non-

Solicited Pornography and Marketing Act of 2003 ("CAN–SPAM" or the "Act"), and its efforts to enforce the Act's substantive provisions.[1]

Spam creates problems well beyond the aggravation it causes to the public. These problems include the fraudulent and deceptive content of a large percentage of spam messages, the offensive content of many spam messages, the sheer volume of spam being sent across the Internet, and the security issues raised when spam is used to disrupt service or to send spyware or viruses carrying malicious code.

The Commission has pursued a three-fold strategy to combat the plague of spam. First, it has pursued a vigorous program of law enforcement against spammers, both before the enactment of CAN–SPAM and since it became effective on January 1, 2004. Second, we have an extensive education program to alert consumers and businesses about self-help measures they can take against spam. Third, we have studied the problem of spam to inform our enforcement and consumer education efforts, and to remedy the paucity of reliable data about spam.

**Law Enforcement**

The Commission has brought 62 law enforcement actions in recent years against alleged fraudulent operations using spam as an integral component of their scams. Most of these cases predate CAN–SPAM, and were brought under Section 5 of the FTC Act.[2] Two of our most recent spam cases, filed in Federal district court in April, target extremely prolific spammers and allege violations of both CAN–SPAM and the FTC Act.[3]

The Commission's complaint in the first of these cases, *FTC v. Phoenix Avatar, LLC, et al.,*[4] alleges that the Defendants used materially false or misleading header information in their e-mail messages, in violation of Section 5(a)(1) of the CAN–SPAM Act; specifically, the Defendants placed the e-mail addresses or domain names of unsuspecting third parties in the "reply-to" and/or "from" fields of their spam (a practice known as "spoofing"). The complaint also alleges that the Defendants failed to provide the disclosures required by Sections 5(a)(5)(A)(ii) and (iii) of the Act, including the required notice of an opportunity to decline to receive further commercial e-mail from the sender. Further, the complaint alleges that the Defendants made false and unsubstantiated claims about diet patches marketed in part through the e-mail messages, in violation of Section 5 of the FTC Act. The Commission has obtained a temporary restraining order that, among other things, stops further deceptive product sales, freezes the Defendants' assets, and preserves their records.

In investigating and filing this matter, the Commission worked closely with the U.S. Attorney for the Eastern District of Michigan and the Detroit Office of the Postal Inspection Service, who are pursuing a concurrent criminal prosecution of the principals of this scheme. The U.S. Attorney filed a criminal complaint, executed a criminal search warrant, and arrested four principals.[5] The principals have been charged with violations of the Federal mail fraud laws as well as with criminal violations of the CAN–SPAM Act.

The second case, *FTC v. Global Web Promotions Pty Ltd.,*[6] targets an Australian company that the FTC alleges is responsible for massive amounts of spam sent to consumers in the United States. According to the complaint, the Defendants used spam to advertise a diet patch similar to the one in *Phoenix Avatar,* as well as purported human growth hormone products "HGH" and "Natural HGH" that Defendants claimed could, among other things, "maintain [a user's] appearance and current biological age for the next 10 to 20 years." The Defendants sold the diet patch for $80.90 and the HGH products for $74.95. The FTC alleged that these claims are

---

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

[2] 15 U.S.C. § 45. The Federal Trade Commission Act prohibits unfair methods of competition and unfair or deceptive acts or practices in or affecting commerce. *See* 15 U.S.C. § 41 *et seq.* The Commission 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; 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).

[3] *See <http://www.ftc.gov/opa/2004/04/040429canspam.htm>.*

[4] Case No. 04C 2897 (N.D. Ill. filed Apr. 23, 2004).

[5] The caption and case number for the criminal complaint are: *United States v. Daniel J. Lin, James J. Lin, Chris Chung, and Mark M. Sadek,* Case No. 04–80383 (E.D. Mich.).

[6] Case No. 04C 3022 (N.D. Ill. filed Apr. 28, 2004)

false and unsubstantiated, and therefore deceptive in violation of Section 5 of the FTC Act.

The complaint alleges that the Defendants also used materially false or misleading header information of unsuspecting third parties (spoofing), in violation of Section 5(a)(1) of the CAN–SPAM Act, and failed to include required disclosures in their e-mail messages, including disclosure of an opportunity not to receive further e-mail, in violation of Sections 5(A)(5)(a)(ii) and (iii) of CAN–SPAM. Because the Defendants shipped their products using fulfillment houses in the United States, the Commission has obtained a preliminary injunction that, among other things, will enjoin the fulfillment houses from further delivery of the Defendants' deceptively-marketed products. In investigating this case, the Commission received invaluable assistance from the Australian Competition and Consumer Commission and the New Zealand Commerce Commission.

The CAN–SPAM cases the Commission is currently pursuing follow an extended Commission effort to target spam under Section 5 of the FTC Act. One aspect of this effort has been the Commission's two-year Netforce law enforcement partnership with other Federal and state agencies, which has targeted deceptive spam. This partnership includes the Department of Justice, FBI, Postal Inspection Service, Securities and Exchange Commission, and Commodities Futures Trading Commission, as well as state Attorneys General, and local enforcement officials. In four regional law enforcement sweeps, the most recent announced in May 2003, the Netforce partners filed more than 150 criminal and civil cases against allegedly deceptive spam and other Internet fraud.[7] In one recent sweep case, for example, the Commission obtained a permanent spam ban against defendants who allegedly used deceptive "From" lines in their spam to claim affiliation with Hotmail and MSN in touting a fraudulent work-at-home envelope-stuffing scheme.[8]

The Commission remains committed to aggressive pursuit of spammers who violate Section 5 of the FTC Act and the CAN–SPAM Act, and we remain committed to working with our law enforcement partners to find and take action against spammers.

**Consumer and Business Education**

The Commission's educational efforts include a spam home page with links to 15 pamphlets for consumers and businesses, including one in Spanish, and summaries of our partnership enforcement efforts to halt deceptive spam.[9] One of the most important business education efforts was "Operation Secure Your Server," announced on January 29, 2004. Through this initiative, the Commission partnered with 36 agencies in 26 countries to highlight the problem of "open proxies"[10] on third-party servers that spammers use to hide the true source of their spam.[11] This project was an outgrowth of last year's "Open Relay Project," in which 50 law enforcers from 17 agencies identified 1,000 potential open relays.[12] The agencies sent a letter, signed by 14 different U.S. and international agencies and translated into 11 languages, urging the organizations with these open relays to close them and explaining how to do so.

---

[7] More information about the Netforce law enforcement sweeps is available on the FTC's website: *<http://www.ftc.gov/opa/2002/04/spam.htm>* (Northwest Netforce); *<http://www.ftc.gov/opa/2002/07/mwnetforce.htm>* (Midwest Netforce); *<http://www.ftc.gov/opa/2002/11/netforce.htm>* (Northeast Netforce); and *<http://www.ftc.gov/opa/2003/05/swnetforce.htm>* (Southwest Netforce).

[8] *FTC v. Patrick Cella, et al.,* No. CV–03–3202, (C.D. Cal. entered Nov. 21, 2003). *See <http://www.ftc.gov/opa/2003/05/swnetforce.htm>*; *<http://www.ftc.gov/opa/2003/11/dojsweep.htm>*.

[9] The home page is located at *<http://www.ftc.gov/bcp/conline/edcams/spam/index.html>*.

[10] Most organizations have multiple computers on their networks, but have a smaller number of "proxy" servers—the only machines on the network that directly interact with the Internet. This system provides more efficient web browsing for the users within that organization and secures the organization's network against unauthorized Internet users from outside the organization. If the proxy is not configured properly, it is considered to be "open," and may allow an unauthorized Internet user to connect through it to other hosts (computers that control communications in a network or administer databases) on the Internet. In this way, open proxies provide one of several methods that spammers use to hide their identities.

[11] The press release can be found at *<http://www.ftc.gov/opa/2004/01/opsecure.htm>*. Tens of thousands of owners or operators of potentially open relay or open proxy servers around the world received the Operation Secure Your Server business education letter.

[12] An open relay is an e-mail server that is configured to accept and transfer e-mail on behalf of any user anywhere, including unrelated third parties, which allows spammers to route their e-mail through servers of other organizations, disguising the origin of the e-mail. By contrast, a "secure" server accepts and transfers mail only on behalf of authorized users. *See* FTC Facts for Business, *Open Relays—Close the Door on Spam* (May 2003), *available at <http://www.ftc.gov/bcp/conline/pubs/buspubs/openrelay.htm>*.

**Studies and Workshops**

Everybody receives spam, but there is little known about it. Reliable information about spam is extremely limited, although there is much "spam lore" that has little if any basis in fact. For example, some sources in Europe claim that the vast majority of spam originates in the United States.[13] Similarly, some sources in the U.S. opine that most spam in Americans' in-boxes arrives from Asia, South America, or Eastern Europe.[14] In fact, nearly all spam is virtually untraceable, either because it contains falsified routing information or because it comes through open proxies or open relays.[15] Moreover, "spoofing" and "forging"[16] of an e-mail message's "from" line and header information are common spammer stratagems.[17] Even with incredibly painstaking, expensive, and time-consuming investigation, it is often impossible to determine where spam originates. Spammers are extremely adroit at concealing the paths that their messages travel to get to recipients' in-boxes. Typically, the most that can be ascertained with certainty is the last computer through which the spam traversed immediately before arriving at its final destination. To frustrate law enforcers, clever spammers may arrange for this penultimate computer to be outside the country where the spam's ultimate recipient is located.

Another example of "spam lore" is the notion that a handful of "kingpin" spammers are responsible for the vast majority of spam. This may or may not be true, but nobody knows for sure. The Commission recently used its compulsory process authority under Section 6(b) of the FTC Act to require the production of information on an exhaustive list of spam topics from various ISPs and other entities. The Section 6(b) specifications included items focusing on the "kingpin" theory. These requests yielded wildly varying estimates, ranging from the familiar "200 spammers" figure to "thousands" of individuals responsible for the majority of spam.[18] In fact, the low barriers to entry suggest that many individuals, and not just a handful, may engage in spamming and contribute significantly to the volume of spam traversing the Internet.[19]

The prevalence of "spam lore" of questionable validity and the corresponding paucity of reliable data on spam has prompted the FTC's staff to perform research on the issue. In one of the first of these efforts, the Commission's staff, working with a partnership of law enforcement officials in several states and Canada,[20] conducted

---

[13] *See <http://www.informationweek.com/story/showArticle.jhtml?articleID=18200812; http://www.spamhaus.org/news.lasso?article=150>.*

[14] In fact, some sources estimate that anywhere from 30–80 percent of spam is routed through open relays and open proxies, and many of these machines are scattered throughout the world. *See <http://news.zdnet.co.uk/hardware/emergingtech/0,39020357,2122679,00.htm>; <http://www.cnn.com/2004/TECH/ptech/02/17/spam.zombies.ap/>.*

[15] In testimony presented to this Committee last year, Brightmail estimated that 90 percent of the e-mail that it analyzed was untraceable. *<http://www.brightmail.com/pressreleases/102203_senate_bill_877.html>.* At the FTC's May 2003 Spam Forum two panelists representing ISPs estimated that 40 percent to 50 percent of the e-mail they analyzed coming to or through their networks made use of open relays or open proxies, making it virtually impossible to trace. FTC Spam Forum transcript, Day 1*, Open Relay, Open Proxies, and Formmail Scripts Panel,* pp. 257, 274, available at *<http://www.ftc.gov/bcp/workshops/spam/>.*

[16] "Spoofing" and "forging" involve manipulating an e-mail's "from" line or header information to make it appear as if the message were coming from an e-mail address from which it did not actually originate.

[17] At the FTC Spam Forum, Margot Koschier from AOL conducted a live demonstration of how to forge header information. In several minutes, she was able to send a message that appeared to come from FTC Chairman Tim Muris in the year 2024. Other Spam Forum panelists also discussed the prevalence of false "sender" information in spam. For example, an MCI representative stated that 60 percent of the spam complaints received at MCI have false headers, false e-mail addresses, deceptive subject lines, or a combination of all three. *See* FTC Spam Forum transcript, Day 1, *Falsity in Spam Panel,* available at *<http://www.ftc.gov/bcp/workshops/spam/>.*

[18] This uncertainty is reflected, for example, in six lawsuits jointly announced by several ISPs on March 10, 2004. They sued nine individuals, and over 200 unknown "John Does." *See* Joint press release of AOL, Earthlink, Microsoft, and Yahoo!, available at *<http://www.microsoft.com/presspass/press/2004/mar04/03–10CANSPAMpr.asp>.* Similarly, in 60 separate FTC cases targeting schemes that used spam as an integral part of the scam, no two cases had the same spammer.

[19] See remarks of Laura Betterly at the FTC Spam Forum. Betterly stated that she paid $15,000 for her e-mail business and broke even within 3 months. FTC Spam Forum transcript, Day 2*, Economics of Spam Panel,* pp. 28–29, available at *<http://www.ftc.gov/bcp/workshops/spam/transcript_day2.pdf>.*

[20] The "Remove Me" surf was conducted as part of the Northwest 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

Continued

a "Remove Me" surf in 2002 to test whether spammers were honoring "remove me" or "unsubscribe" options in spam. From e-mail that the partnership 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. To test these "remove me" options, the partnership set up unique e-mail accounts that had never been used before and submitted "remove me" requests from these accounts. The staff found that 63 percent of the removal links and addresses in the 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. In no instance did we find that any of our unique e-mail accounts received more spam after attempting to unsubscribe. This finding is inconsistent with the common belief that attempting to unsubscribe guarantees that consumers will receive more spam.

Another study in 2002, the "Spam Harvest," examined what online activities place consumers at risk for receiving spam.[21] We discovered that all of the e-mail addresses that we posted in chat rooms received spam. In fact, one address received spam only eight minutes after the address was posted. Eighty-six percent of the e-mail addresses posted in newsgroups and Web pages received spam, as did 50 percent of addresses in free personal Web page services, 27 percent in message board postings, and 9 percent in 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.

A third study focused on false claims in spam by analyzing a sample of 1,000 messages drawn from three sources.[22] The Commission staff issued a report on April 30, 2003, explaining that two-thirds of the sample contained indicia of falsity in the "from" lines, "subject" lines, or message text,[23] and that in a smaller random sample of 114 pieces of spam taken from the same set of data, only one came from an established business in the *Fortune* 1000.[24] This study, the first extensive review ever conducted of the likely truth or falsity of representations in spam, underscores both the potential harm to consumers from spam and spammers' willingness to ignore the law.

One of the most important projects in our ongoing effort to study and understand the phenomenon of spam and its impact on the Internet and the economy at large was the Spam Forum, a three-day public forum from April 30 to May 2, 2003. This Forum provided a wide-ranging public examination of spam from all viewpoints.

The Spam Forum was organized into twelve panel discussions covering the mechanics of spam, the economics of spam, and potential ways to address the problem of spam.[25] 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 panels. First, there was much discussion about the increasing amount of spam. Second, spam imposes real costs. The panelists offered concrete information about the costs of spam to businesses and to ISPs. Spe-

---

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. See <*http://www.ftc.gov/opa/2002/04/spam.htm*>.

[21] The"Spam Harvest" was conducted as part of the Northeast Netforce, an enforcement sweep in which the FTC was joined by the Connecticut Attorney General, the Maine Attorney General, the Massachusetts Attorney General, the New Hampshire Department of Justice, the New Jersey Division of Consumer Affairs, the New York City Department of Consumer Affairs, the New York State Attorney General, the New York State Consumer Protection Board, the Rhode Island Attorney General, the United States Attorney for the District of Massachusetts, the United States Postal Inspection Service, and the Vermont Attorney General. See <*http://www.ftc.gov/opa/2002/11/netforce.htm*>.

[22] The study's sources were the FTC's database of millions of spam forwarded to the Commission by consumers, messages received in the "Spam Harvest," and messages delivered to FTC employees' e-mail accounts.

[23] *False Claims in Spam:* A Report by the FTC's Division of Marketing Practices (April 30, 2003), available at <*http://www.ftc.gov/reports/spam/030429spamreport.pdf*>.

[24] None of the spam in this sample was sent by a *Fortune* 500 company. The sample provides 95 percent confidence that less than 5 percent of the 11.6 million pieces of spam then in the FTC's database of spam forwarded by consumers came from a *Fortune 1000* company, and a 95 percent confidence that less than 3 percent of the e-mail in our database was sent by or on behalf of a *Fortune* 500 company. The database now contains approximately 100 million messages.

[25] In addition to the 87 panelists who participated, 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 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.

cifically, ISPs reported that costs to address spam increased dramatically in the two years immediately preceding the forum. ISPs bear the cost of maintaining servers and bandwidth necessary to channel the flood of spam, even that part of the flood that is filtered out before reaching recipients' mail boxes. At the Forum, America Online reported that it blocked an astonishing 2.37 billion pieces of spam in a single day.[26] Third, spam is an international problem. The panel discussing open proxies and open relays and the international panel described spam's cross-border evolution and impact. Most panelists agreed that any solution will have to involve an international effort.

The Commission convened this event for two principal reasons. First, as noted above, spam is frequently discussed, but facts about how it works, its origins, and what incentives drive it are elusive. The Commission anticipated that the Forum would generate an exchange of useful information about spam to help inform the public policy debate. Second, the Commission sought to act as a potential catalyst for solutions to the spam problem. Through the Forum, the Commission brought together 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. The panelists contributed valuable information from various viewpoints to the public record. In addition, the Forum spurred both cooperation and action among a number of participants. Most notably, on the eve of the Forum, industry leaders Microsoft, America Online, Earthlink, and Yahoo! announced a collaborative effort to stop spam. This promising effort continues today with participation from additional industry leaders.[27] 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. We believe that the Forum contributed significantly to the ongoing effort on the part of industry, consumers, and government to learn how to control spam.

**Efforts Since CAN–SPAM Went Into Effect**

To provide additional tools to fight spam, Congress enacted the CAN–SPAM Act on December 16, 2003.[28] The Act took effect on January 1, 2004, and the Commission immediately sought to enforce the Act, to meet the aggressive deadlines it set for the completion of several rulemakings and reports, and to develop national and international partnerships to help combat deceptive spam. The Commission filed its first two CAN–SPAM cases within four months of the Act's effective date. As mentioned earlier, combating spam has been one of the Commission's top priorities for several years, and currently half of the staff members in the Bureau of Consumer Protection's largest enforcement division work on CAN–SPAM issues, as do staff in all of the Commission's regional offices and additional lawyers, investigators, and technologists throughout the FTC.

Moreover, to facilitate enforcement by other law enforcement agencies, we have consulted with our partners at the Department of Justice and have organized a task force with state officials to bring cases. The Task Force is co-sponsored by the FTC and the Attorney General of Washington, and is comprised of 136 members representing 36 states, several units within the Department of Justice, and the FTC.[29] The FTC staff so far has conducted two training sessions on investigative techniques for the Task Force, each of which was attended by approximately 100 individuals representing about 35 different states. The Task Force conducts monthly conference calls to share information on spam trends, technologies, investigative techniques, targets, and cases.

The Commission is also on target to complete the rulemakings and reports required by CAN–SPAM. On January 28, 2004, the Commission issued a Notice of Proposed Rulemaking for a mark or notice that will identify spam containing sexu-

---

[26] FTC Spam Forum transcript, Day 1, *Introduction to Spam Panel,* p. 39, available at *<http://www.ftc.gov/bcp/workshops/spam/transcript_day1.pdf>*.

[27] *See, e.g.,* "ISPs Sue Spammers," Article dated March 12, 2004, reporting on CAN–SPAM cases brought by four ISPs, available at *<http://www.pcmag.com/print_article/0,1761,a=121533,00.asp>*.

[28] Pub. L. 108–187 (codified at 15 U.S.C. § 7701 *et seq.*).

[29] The Commission continues to try to recruit representatives from the remaining states.

ally oriented material.[30] The Commission received 89 comments in response.[31] We issued a final rule in advance of the statutory deadline of April 14.[32] Effective May 19, the rule requires all messages containing sexually oriented material to include the warning "SEXUALLY–EXPLICIT: " in the subject line. This rule also prohibits these messages from presenting any sexually explicit material in the subject line or in the portion of the message initially viewable by recipients when the message is opened.

In addition, on March 11, 2004, the Commission issued an Advance Notice of Proposed Rulemaking ("ANPR") to define the relevant criteria to be used in determining "the primary purpose" of a commercial electronic mail message subject to CAN–SPAM's provisions.[33] The ANPR requested comment on this issue, as well as a number of other issues for which CAN–SPAM has provided the Commission discretionary rulemaking authority, such as modifying the definition of "transactional" e-mail messages;[34] changing the 10-business-day statutory deadline for e-mailers to comply with consumers' opt-out requests;[35] and implementing other CAN–SPAM provisions.[36] The Commission received over 12,000 comments in response.[37] Commission staff is incorporating suggestions and recommendations from these comments into its Notice of Proposed Rulemaking.

The Commission is also actively preparing several reports required by the CAN–SPAM Act. The March 11 ANPR solicited comment from interested parties on a plan and timetable for establishing a national Do-Not-E-mail Registry, and an explanation of any practical, technical, security, privacy, enforceability, or other concerns commenters may have about the creation of such a registry, for a report to Congress due on June 16.[38] To supplement information collected from this public comment process, the staff has used additional tools to enhance its understanding of all relevant issues. First, the staff has held meetings on the record with more than 80 interested parties representing more than 60 organizations to explore all aspects of the concept of a "Do-Not-E-mail Registry" from as many viewpoints as possible. Second, the Commission also issued compulsory process to a number of ISPs and other entities under Section 6(b) of the FTC Act to obtain information relevant to this report and other reports required by CAN–SPAM. Third, the Commission issued a Request for Information from vendors for creation of such a registry, and obtained assistance of expert consultants to assess vendors' submissions. Through these efforts, the Commission has received invaluable information that will allow us to prepare a comprehensive report.

In addition, the staff is actively gathering information for and preparing:

- a report due September 16, 2004, setting forth a system of monetary rewards to encourage informants to report the identities of violators of CAN–SPAM;[39]

---

[30] 69 Fed. Reg. 4263 (Jan. 29, 2004). Section 5(d)(3) of CAN–SPAM requires that "[n]ot later than 120 days after the date of the enactment of this Act, the [Federal Trade] Commission in consultation with the Attorney General shall prescribe clearly identifiable marks or notices to be included in or associated with commercial electronic mail that contains sexually oriented material, in order to inform the recipient of that fact and to facilitate filtering of such electronic mail. The Commission shall publish in the Federal Register and provide notice to the public of the marks or notices prescribed under this paragraph." (codified at 15 U.S.C. § 7704(d)(3)). Under CAN–SPAM, the term "sexually oriented material" is "any material that depicts sexually explicit conduct (as that term is defined in § 2256 of title 18, United States Code), unless the depiction constitutes a small and insignificant part of the whole, the remainder of which is not primarily devoted to sexual matters." *See* 15 U.S.C. § 7704(d)(4). 18 U.S.C.§ 2256, in turn, provides that "sexually explicit conduct means actual or simulated (A) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (B) bestiality; (C) masturbation; (D) sadistic or masochistic abuse; or (E) lascivious exhibition of the genitals or pubic area of any person."

[31] Available at <*http://www.ftc.gov/os/comments/adulte-maillabeling/index.html*>.

[32] *See* <*http://www.ftc.gov/opa/2004/04/adultlabel.htm*>.

[33] Pub. L. 108–187, § 3(2)(A) (codified at 15 U.S.C. § 7702(2)(A)). The rulemaking is required by § 3(2)(C) (codified at 15 U.S.C. § 7702(2)(C)), and is on track for completion by the statutory deadline of December 16, 2004.

[34] Pub. L. 108–187 § 3(17) (codified at 15 U.S.C. § 7702(17)). Transactional messages must comply with the Act's prohibition against deceptive headers, *Id.,* § 5(a)(1) (codified at 15 U.S.C. § 7704(a)(2), but are otherwise exempt from the Act. *Id.,* § 3(2)(B) (codified at 15 U.S.C. § 7702(2)(B)). A rulemaking is permitted by § 3(17)(B) (codified at 15 U.S.C. § 7702(17)(B)).

[35] *Id.,* § 5(a)(4)(A)-(B) (codified at 15 U.S.C. § 7704(a)(4)(A)-(B)). A rulemaking is permitted by § 5(c)(1) (codified at 15 U.S.C. § 7704(c)(1)).

[36] *Id.,* § 13(a) (codified at 15 U.S.C. § 7711).

[37] Available at: <*http://www.ftc.gov/os/comments/canspam/index.htm*>.

[38] *Id.,* § 9 (codified at 15 U.S.C. § 7708).

[39] *Id.,* § 11(1) (codified at 15 U.S.C. § 7710(1)).

- a report due June 16, 2005, recommending whether or not commercial electronic mail should be identified as such in its subject line by the use of a label like "ADV";[40] and
- a report due December 16, 2005, on the efficacy of the Act .[41]

**Conclusion**

E-mail provides enormous benefits to consumers and businesses as a communication tool. The increasing volume of spam, coupled with the use of spam as a means to perpetrate fraud and deception, has put these benefits at serious risk. The Commission intends to continue its law enforcement, education, and research efforts to protect consumers and businesses from the current onslaught of unwanted spam messages. The Commission appreciates this opportunity to describe its efforts to address the problem of spam and its activities to fulfill the mandates of CAN–SPAM.

The CHAIRMAN. Thank you very much.

Ms. Monroe, welcome.

## STATEMENT JANA D. MONROE, ASSISTANT DIRECTOR, CYBER DIVISION, FEDERAL BUREAU OF INVESTIGATION; ACCOMPANIED BY DAN LARKIN, UNIT CHIEF, INTERNET CRIME COMPLAINT CENTER

Ms. MONROE. Thank you.

Good morning, Chairman McCain and other Members of the Committee. On behalf of the FBI, I would like to thank you for this opportunity to address the FBI's role in anti-spam initiatives.

Cybercrime in its many forms continues to receive priority attention from the FBI. A paramount objective of the Cyber Division has been to arm field investigators with the necessary resources to identify and combat evolving cybercrime matters. Over the past 18 months, the FBI has supported the establishment of more than 50 multi-jurisdictional task forces nationwide. Partnerships with Federal, state, and local law enforcement are vital to the success of these teams, because cybercrime, by its nature, does not respect jurisdictional boundaries, and we need to leverage existing resources to effectively and efficiently fight cybercrime.

In addition to law enforcement partnerships, another prime objective of the FBI's Cyber Division is to develop active partnerships with subject matter experts from the private sector. Such experts are often better equipped to identify cybercrimes at their earliest stages. Early identification of cybercrime is an absolute must, and directly correlates to ultimate success in investigating and prosecuting cybercriminals.

In keeping with this approach, and even before passage of the CAN–SPAM Act by Congress, the FBI had begun work in a public/private alliance to specifically target the growing spam problems. The Internet Crime Complaint Center, working in coordination with the industry, developed Slam Spam, an initiative that began operation last fall. This initiative targets significant criminal spammers, as well as companies and individuals that use spammers and their techniques to market their products. This initiative also investigates the techniques and tools used by spammers to expand their targeted audience, to circumvent filters and other countermeasures implemented by consumers and indus-

[40] *Id.,* § 11(2) (codified at 15 U.S.C. § 7710(2)).

[41] *Id.,* § 10 (codified at 15 U.S.C. § 7709). The agency is gathering baseline data for this report through the § 6(b) requests for information and other activities.

try, and to defraud customers with misrepresented or nonexistent products.

Before Congress passed the CAN–SPAM Act of 2003, some schemes perpetrated by spam could have been pursued as violations of statutes such as Title 18 United States Code Section 10–30, which is fraud and related activity in connection with computers; Title 18 U.S. Code Section 23–19, criminal infringement of a copyright; or Title 18 U.S. Code Section 13–43, which is wire fraud; as well as through several other existing criminal or civil statutes. However, no existing statute directly addressed some typical behaviors of spammers, including widely used available open proxies to bounce e-mail traffic through intermediary computers with the intent to hide the true location of the sender, the abuse of free e-mail services to send out spam from accounts with false registration information, and the use of tools to forge the return address and other headers associated with the e-mail.

Prior to the CAN–SPAM Act, law enforcement lacked the legal tools to address the spam problem directly. Because of this, many investigators and prosecutors viewed cases primarily on the sending of spam as unlikely to result in successful investigations and prosecutions. However, as the economic impact attributable to spam and the use of spam to send unwanted pornographic images became known, law enforcement interest increased.

Similarly, investigations of computer intrusions and viruses have uncovered that infecting computers with viruses is now often being done to facilitate spam. In the Sobig.F computer intrusion investigation, we learned that millions of computers were infected globally, primarily to convert those computers into spam relays. The CAN–SPAM Act now allows law enforcement to apply criminal leverage to spammers who previously were viewed as facilitators or fraudulent schemes, but who would disclaim any knowledge of the fraudulent or pornographic nature of the products they were advertising. CAN–SPAM's provisions address the most significant fraudulent and sexually explicit spam, and both provide civil and criminal tools to combat them.

Once again, I appreciate the opportunity to come before you today and share the work that the FBI's Cyber Division has undertaken to begin to address the problem of spam. Our work in this area will continue, and we will keep Congress informed about our progress in overcoming the challenges in this area.

[The prepared statement of Ms. Monroe follows:]

PREPARED STATEMENT OF JANA D. MONROE, ASSISTANT DIRECTOR, CYBER DIVISION, FEDERAL BUREAU OF INVESTIGATION

**Introductory Statement**

Good morning Chairman McCain, and other members of the Committee. On behalf of the FBI, I would like to thank you for this opportunity to address the FBI's role in anti-spam initiatives.

Cyber crime, in its many forms, continues to receive priority attention from the FBI. A paramount objective of the Cyber Division has been to arm field investigators with the necessary resources to identify and combat evolving cyber crime matters. Over the past 18 months, the FBI has supported the establishment of more than 50 multi-jurisdictional task forces nationwide. Partnerships with federal, state, and local law enforcement are vital to the success of these teams, because cyber crime, by its nature, does not respect jurisdictional boundaries and we need to leverage existing resources to effectively and efficiently fight cybercrime.

In addition to law enforcement partnerships, another prime objective of the FBI's Cyber Division is to establish active partnerships with subject matter experts from the private sector. Such experts are often better equipped to identify cyber crimes at their earliest stages. Early identification of cyber crimes is an absolute must, and directly correlates to ultimate successes in investigating and prosecuting cyber criminals.

In keeping with this approach, and even before passage of the CAN–SPAM Act by Congress, the FBI had begun work in a Public/Private Alliance to specifically target the growing spam problem. The Internet Crime Complaint Center (IC3), working in coordination with industry, developed "SLAM-Spam," an initiative that began operation last fall. This initiative targets significant criminal spammers, as well as companies and individuals that use spammers and their techniques to market their products. It also investigates the techniques and tools used by spammers to expand their targeted audience, to circumvent filters and other countermeasures implemented by consumers and industry, and to defraud customers with misrepresented or non-existent products.

**Enforcement Before and After the CAN–SPAM Act**

Before Congress passed the CAN–SPAM Act of 2003, some schemes perpetrated by spam could have been pursued as violations of statutes such as Title 18, United States Code, Section 1030 (fraud and related activity in connection with computers) Title 18, United States Code, Section 2319 (criminal Infringement of a copyright) or Title 18, United States Code, Section 1343 (wire fraud), as well as through several other existing criminal or civil statutes. No existing statute, however, directly addressed some typical behaviors of spammers, including: using widely-available "open proxies" to bounce e-mail traffic through intermediary computers with the intent to hide the true location of the sender, the abuse of free e-mail services to send out spam from accounts with false registration information, and the use of tools to forge the return address and other headers associated with the e-mail. Prior to the CAN–SPAM Act, law enforcement lacked the legal tools to address the spam problem directly. Because of this, many investigators and prosecutors viewed cases based primarily on the sending of spam as unlikely to result in successful investigations and prosecutions. As the economic impact attributable to spam, and the use of spam to send unwanted pornographic images have become known, however, law enforcement interest increased. Similarly, investigations of computer intrusions and viruses have uncovered that infecting computers with viruses is now often being done to facilitate spam. In the SoBig.F computer intrusion investigation, we learned that millions of computers were infected globally, primarily to convert those computers into spam relays.

The CAN–SPAM Act now allows law enforcement to apply criminal leverage to spammers, who previously were viewed as "facilitators" of fraudulent schemes, but who would disclaim any knowledge of the fraudulent or pornographic nature of the products they were advertising. CAN–SPAM's provisions address the most significant fraudulent and sexually explicit spam, and provide both civil and criminal tools to combat them.

**Project SLAM-Spam**

In response to the growing number of complaints it was receiving about fraudulent and pornographic spam, the Internet Crime Complaint Center began development of a project to address the spam problem. The Center has developed extensive experience in taking complaints relating to all types of crime occurring over the Internet, analyzing them for significant patterns, and then referring appropriate case leads out to the field for further investigation. The IC3 receives more than 17,000 complaints every month from consumers alone, and additionally receives a growing volume of referrals from key e-commerce stakeholders. The use of spam is a substantial component of these schemes, which includes reports of identity theft schemes, fraudulent pitches and "get rich quick" schemes, and unwanted pornography. Currently, over 25 percent of all complaints to the IC3 involve some use of spam electronic mail.

To develop the project, the IC3 coordinated with industry Subject Matter Experts and representatives of the Direct Marketing Association (DMA), which have provided essential expertise and resources to the project. The IC3 has also consulted with the Federal Trade Commission, which has several years of working with consumers on the spam problem. This project has also identified a significant list of the methods used by subjects to advance their individual schemes. I will describe some of the efforts and summarize the primary accomplishments of this project over the past six months, and project future accomplishments, consistent with the overall project plan. This include a national initiative in which suitable cases developed or

advanced through this project, will be highlighted as part of our overall effort against those who have committed criminal and civil violations of the CAN–SPAM Act.

The first several months of the project focused on building support structures to support the initiative. The IC3 identified and consulted with Subject Matter Experts from Internet Service Providers, anti-spam organizations, and other groups. They defined responsibilities of participants, and began weekly strategy meetings to ensure that progress and priorities were consistent and clear. Experts developed communications channels and databases to exchange information quickly and robustly among the experts in the alliance. Finally, a list of potential subjects was developed by analysts from the Internet Crime Complaint Center (IC3), and compared against existing IC3 referrals to determine if law enforcement had already initiated investigations of subjects, and if those investigations were making progress.

After the effective date of the CAN–SPAM Act, the IC3 helped organize and participated in three regional training conferences on a number of subjects relating to cybercrime. At these conferences, representatives of the FBI and Department of Justice gave presentations designed to familiarize agents specializing in cyber crime with the SLAM-Spam initiative, the techniques used by spammers to falsify their identity, and the additional criminal prohibitions in the CAN–SPAM Act.

Identifying the most significant subjects involved in criminal spam scenarios is a prime objective of the SLAM-Spam initiative. Equally significant has been developing those cases so that they can be further investigated and prosecuted by field offices, cyber task forces, and United States Attorneys' Offices around the United States. Accordingly, while a growing number of Internet crime schemes use spam to target larger pools of victims, the Cyber Division's task force capabilities have increased as well. Cyber Crime squads in our field divisions are trained in quickly investigating computer intrusions and virus attacks. When they are available, these resources can also be used to investigate the source of unwanted fraudulent and pornographic spam.

Project SLAM-Spam is on course and on schedule to achieve substantial results against individuals and organizations that are complicit in criminal (and potentially civil) schemes where spam is used. As a result of these activities, more than 20 Cyber Task Forces are actively pursuing criminal and in some cases joint civil proceedings against subjects identified to date. We expect that this number will continue to rise, as successful actions are brought under this act.

We are also improving our cooperation with the FTC, State Attorneys General, and industry partners, because we understand that criminal enforcement is only one aspect of the fight against spam. While we cannot share every detail of ongoing criminal investigations, we can and will share our knowledge about tools and techniques used by spammers, their current primary targets of opportunity, and the types of schemes they are favoring.

**Notable Early Accomplishments of SLAM-Spam**

The SLAM-Spam initiative has now moved beyond the planning stages, and has begun identifying and packaging investigations from the field. Within the last few months, the Initiative has:

- Identified over 100 significant spammers
- Targeted 50 Spammers so identified as points of focus for the SLAM-Spam project.
- Developed ten primary subject packets developed and for referral to Law Enforcement
- Linked three groups of subjects into potential organized criminal enterprises
- Referred five significant ongoing investigations linked to spammers.
- Over 350 compromised and misconfigured resources identified, including 50 government sites.
- Engaged military criminal investigators to help identify criminal acts associated with compromised Government sites.
- Identified common denominators relating to spam both domestically and internationally.
- Catalogued numerous exploits and techniques being used by spammers, including e-mail harvesting, use of viruses, and turn-key tools to bypass filters.

**Future Initiatives**

The FBI, via the IC3, periodically coordinates National Investigative Initiatives, together with our Federal, State, and Local partners. Such initiatives are designed to highlight escalating areas of cyber crime, and demonstrate decisive action taken

by law enforcement to combat it. These events also serve to alert the public to new and evolving cyber crime schemes, such as criminal spam. Three such initiatives have been carried out over the last 2 ½ years, including Operation Cyber Loss, Operation E-Con, and most recently Operation Cyber Sweep. A succeeding initiative is being projected for later this year in which it is anticipated that criminal and civil actions under the CAN–SPAM Act of 2003 will be included.

We have begun preliminary notification to our field offices of our newest initiative, underscoring our emphasis on cases involving criminal uses of spam. Such cases may be investigated and prosecuted as computer intrusion matters, or as on-line cyber frauds which may lend themselves to a variety of existing state and/or Federal statutes, including the recently passed CAN–SPAM Act. Similar notifications have been or will be made through appropriate channels to the U.S. Secret Service, U.S. Postal Inspection Service, the FTC, the Department of Justice, and in the state and local agencies that are members of the National White Collar Crime Center. We are already planning meetings to ensure that this initiative is on track, and to further define the scope and packaging of this activity are being planned. We will be happy to brief you on the results of this initiative when it has been completed.

**Conclusion**

Once again, I appreciate the opportunity to come before you today and share the work that the Cyber Division has undertaken to begin to address the problem of spam. Our work in this area will continue, and we will continue to keep Congress informed about our progress in overcoming the challenges in this area.

The CHAIRMAN. Thank you very much.

Chairman Muris, I mentioned, in my opening statement, that in the CAN–SPAM Act we gave you the authority to go after the businesses that hire spammers to promote their goods and services. The intent of that provision, as you know, is to allow you to more quickly respond to spam by allowing them to stop chasing spammers and directly enforce the law against their clients. Why haven't you acted more in that direction?

Chairman MURIS. Well, in fact, Mr. Chairman, we have. Of our 62 cases, 59 were against sellers. Many of them were against sellers and spammers. We've also found, in our first two cases, which are initially primarily against sellers—we believe we'll find out who the—there's an enormous amount of spam in those two CAN–SPAM cases—we believe we'll find out who the spammers were. But one reason that Section 6 was put in there was—and we thought there might be some difficulty in using Section 5 against sellers, and at least with our initial cases and initial investigations, that did not turn out to be the case. I think going against sellers is an important road. We will continue to do that.

Of course, the underlying problems of spam, the very low cost, and the absence of effective enforcement, and effective ISP screening, and the anonymity of the Internet are not directly addressed.

I do agree with the remarks that we just heard, that the criminal parts of spam, in the end of the day—I mean, of CAN–SPAM—may be the most important aspects of the statute.

The CHAIRMAN. Ms. Monroe, how significant a problem is the promotion of child pornography in spam?

Ms. MONROE. Very significant. I think that is one of the primary means in doing that. It's a significant problem.

The CHAIRMAN. As we all know, the U.S. Supreme Court has said that child pornography is beyond any constitutional protections. It seems to me, then, that you would really want to make that a priority for—in your efforts.

Ms. MONROE. Yes, sir. We are making it—it has been a priority, and we're continuing to make it a priority.

The CHAIRMAN. Have you undertaken any special efforts?

Ms. MONROE. In what means?

The CHAIRMAN. To eradicate the promotion of child pornography in spam?

Ms. MONROE. Well, in working on this whole spam issue, what we have done is, we're in the process of providing training to our field offices. And, as I had indicated, we have approximately 50 task forces that we have trained, and we're continuing to do this in our 20 field offices, and that is a part of the pornography that's included in our training, and are addressing the issue.

The CHAIRMAN. Well, I hope you'll give it some special priority. It's obviously the most disgusting aspect of this whole spam situation.

Ms. MONROE. Yes, sir.

The CHAIRMAN. Mr. Muris, what accounts, in your view, for the continuing rapid increase in the volume of spam?

Chairman MURIS. The reason spam is such a difficult target are the two problems that I alluded to a few minutes ago. In the absence of effective screening and enforcement—and that's related to the second problem that I'll get to—the additional cost of sending spam is very close to zero. When you make an additional—if you're a marketer and you make an additional 10,000 phone calls or send out an additional 10,000 letters, that costs real money. In the absence of those factors that I discussed, sending out an additional 10,000 spam does not, which means that—and your testimony has alluded to this, as our 3-day spam forum did—that the response rates can be extraordinarily trivial, and spam can still be a profitable endeavor.

The second problem is the anonymity. The Internet was set up to be anonymous, and it's why going after the seller is an important thing to do. The problem is, is that the overwhelming amounts of the spam are—involve obviously fraudulent products or products that are otherwise offensive or illegal—you know, pornography—and there's a lot of spam that will sell you prescription drugs without a prescription, which is illegal. So you have people who have the incentive to hide and the anonymity of the Internet allows them to hide.

There are technological solutions, perhaps. The filtering is clearly better. There is a movement toward authentication, at least at the domain level, which will be helpful. But there is—and you alluded to this—there's an arms race obviously going on between the spammers and the ISPs, and the spammers are certainly at least holding their own.

The CHAIRMAN. Senator Wyden?

Senator WYDEN. Mr. Muris, what's the strategy for going after the kingpin spammers? I think it's clear that people can differ how many of them there are, and there has been some discussions of 500 or 1,000. It's not an unlimited universe. What's the strategy for going after the kingpin spammers?

Chairman MURIS. Well, the underlying point is obviously an excellent one. We've asked—I mean, as in so many areas of spam, no one knows—we ask, as part of the compulsory process that I mentioned—we asked ISPs, and we got—you know, we got differences of opinion that ranged by a factor of ten.

An example of how hard this is, one of the many good parts of CAN–SPAM was to allow this right of action by the ISPs. When they filed—a bunch of them have filed actions recently—they were almost all against John Doe defendants, because they don't know who they are.

We are collecting spam. We ask to receive spam. We get 200,000 to 300,000 a day. One of the ways we found these targets was looking at the extraordinarily large volume. There are organizations out there that claim that they know who some of these large spammers are. We're working with them, we're working with ISPs. Quite frankly, there are still some problems, some statutory problems, that could be corrected. Some of those are corrected in our proposed Cross-Border Fraud legislation, which I know you support and this Committee supports, and we hope that we can move that legislation very quickly, because it will help us cooperate internationally, which is becoming very important, and it will help us reduce these barriers. Right now, the ISPs have some limits on what they can share with us, and we think the Cross-Border Fraud legislation will help there.

Senator WYDEN. In addition to using the large volume as a criteria for selecting a case, what can you tell us about the criteria you're going to choose from this point on, in terms of bringing cases?

Chairman MURIS. We will continue to—as the Chairman asked, we will continue to follow the money trail and go after the sellers. And that, unfortunately—I mean, there's both the good news and bad news there. The good news is that you can sometimes find the sellers. The bad news is, it can be very cumbersome. In our two CAN–SPAM cases, we, surprisingly, only had to use six, what amounts to subpoenas, each, which is much lower than in the typical case.

And a reason, Senator, to focus on the volume is, when you do these cases—unlike when someone robs a bank and you know how much money they've taken, when you do these cases, you don't know, until you get to the end, how much commerce is involved.

We've done two phishing cases—you know, phishing, with a "ph"—where someone is sending you spam, claiming they're AOL. We've worked with criminal authorities. In one case, we found a minor, on a lark, who had stolen a grand total of $8,000. Criminal authorities do not normally prosecute minors for that kind of offence. The other case, it involved much larger sales, and there have been criminal penalties assessed, and we just—a very long sentence was just entered into.

But we will continue to look at the volume, look at the amount of commerce, look at the sellers, work with other people, especially the ISPs. Unfortunately, it takes all those tools, Senator.

Senator WYDEN. I was pleased that one of the cases you filed targeted a company based in Australia. And so it seems to me, with that kind of message, we say, "Look, we're not just going to let you leap offshore, and you can go about your dirty deeds that way." Even before we get the cross-border legislation—which I do support, and there's strong bipartisan support for—can you commit to trying to continue those kinds of actions? Because, of the three pieces—enforcement in the United States, international coopera-

tion, and technology-based solutions—we don't want to throw up our hands and just say, "There's nothing we can do."

Chairman MURIS. Senator, absolutely. We have an enormously large number of people working on this effort. International enforcement against fraud—and spam is one of the main ways to transmit the fraud—has been one of the highest priorities I've had as Chairman. That's why I've spent so much time working with you on the Cross-Border Fraud legislation, and we greatly appreciate your support.

I was recently in Europe. The European Commission in the European Union is about to require individual member states to have enforcement agencies. We provided technical assistance to some of the new members. We've engaged in massive training of people all over the United States. We've created a task force working with criminal and state partners on spam. And I can guarantee that it will continue to be a major effort of ours.

Senator WYDEN. A last question, if I might. I think I described in my opening statement that I see this as the beginning of the long march to get the swamp drained. I mean, this is going to be a problem where we're up against sleazy characters who are not technological simpletons. I mean, what they're going to constantly be trying to do is get out in front of any kind of piece of legislation or any kind of enforcement action. So as part of this effort to try to get out in front of what the next approach will be, tell us, if you would, Ms. Monroe and Mr. Muris, what you've learned—what are the most important lessons you've learned thus far, in terms of trying to tackle this scourge?

Ms. Monroe, why don't you start, and then we'll have Mr. Muris.

Ms. MONROE. Sir, the FBI——

Senator WYDEN. Wouldn't want to leave you without a question.

Ms. MONROE. I'm sorry. The FBI met recently with the G8 and Interpol in, I think, addressing what you said in your opening statement. They are very willing to work and cooperate with the spam issue. They had not necessarily viewed it as spam or call it spam, so I think, at this point, we're in the initial stages of educating them and bringing them onboard as to how we define our problem, and what it means, and globally how they can be of some assistance. And they are extremely encouraged by that.

And on the technical aspect of it, I think, within our Cyber Division within the FBI, we have our Special Technologies Applications section and our Investigative Technology Division, which are very technologically advanced and have provided tools to us to help combat this. And I'm very confident that, as an investigative agency, we are ahead of the game on that.

Senator WYDEN. Mr. Muris, what have we learned so far?

Chairman MURIS. Well, we've learned a lot, but a couple of things. On enforcement, we've learned that because of the anonymity problem, we have to follow the money trail. We've learned that it's difficult. I think we are gaining experience and learning by doing.

I recently met—I forgot to mention—I made a significant pitch to a group of United States attorneys about this problem and about the problem of fraud, in general. And I talked to them about how this problem is not just in the English language. We're actually

now looking at Spanish language. We're about to start a pilot program—and, Mr. Chairman, we're going to Phoenix as one of our cities in the pilot program—to try to get more interest in the Spanish-speaking media and the Spanish-speaking community about telling us—the Hispanic community—about telling us the problems of fraud. And spam is a significant part of that in that language, as well.

The other thing that we've learned is that law enforcement itself—and I think you've all echoed this—is not the only solution. We've learned a lot about the potential of domain-level authentication as helping. I expect that our report to you next month will discuss those issues.

Senator WYDEN. Thank you, Mr. Chairman.

The CHAIRMAN. Senator Burns?

Senator BURNS. Thank you, Mr. Chairman.

I want to continue along the same lines as my friend from Oregon. If estimates point to the stark fact that 200 spam operations are responsible for nine-tenths of the spam, it would seem like it would contradict some arguments that it's not as widespread as one would think, and we could probably narrow and zero in on these larger spammers and take care of the situation.

I want to say that Senator Wyden and I, we have had conversations with the British—the Parliamentarians in Britain, also in Australia and in Japan. The U.S./Asian network is aware of this problem—and that includes a lot of the Pacific Rim countries, including the PRC—that we have a problem here. And I think those discussions could continue to move forward and to coordinate yourself with some international organizations, agencies, for the fight.

Let me ask—as of yesterday, the Commission issued the final ruling on—it requires that all sexually oriented spam be labeled with the warning "sexually explicit" on the subject line. Are you confident that that will withstand a court challenge, Mr. Muris?

Chairman MURIS. I am not a constitutional scholar, and I have no basis to be confident or not confident. We have made what we think are sound constitutional arguments, but this is an area where the efforts to write law have frequently been overturned.

Senator BURNS. Well, I just noticed that, and I congratulate you for your bold step. I congratulate you for that.

And tell me, again—you know, when we started talking about the Do Not Spam list, after 141 days and after you've seen the law into effect, would you—are you more confident now, or less confident, that that approach is technically feasible? And how would the list be maintained? And what would happen to such a list if it were to become available to spammers?

Chairman MURIS. Well, we have—let me give you a very preliminary answer——

Senator BURNS. Yes.

Chairman MURIS.—because the staff has just sent a report to the Commission, and the Commission needs to digest that report, and I would be—as I mentioned in my opening remarks, I would be more than glad to come and discuss it privately or publicly, however the Committee desires.

On the last point, it is clear that—from the evidence I've seen, that a list of valid e-mail addresses is very valuable to spammers,

and that's obviously one of the serious issues about a Do Not E-Mail Registry that the report addresses, and that we'll be reporting to you on soon.

Senator BURNS. Well, but are—have you solidified—found out anything different than, say we—when we studied that before the law was actually put into effect?

Chairman MURIS. Well, I think we will have—the report contains—and, again, we haven't passed on it. It just—it literally went to the Commission—today is Thursday—I think Monday or Tuesday. We have learned a fair amount about the ISPs' efforts in the—you know, which have occurred in the last year, and the report, you know, will comment on that. There are efforts underway at authentication at the domain level, and that, I think, could be a very useful step, although nothing is a silver bullet here, and that would not be, as well, given the so-called zombie drone problem.

Senator BURNS. Well, I—again, I want to applaud your working so far. I don't know of anything that we've hit the ground running—141 days is not very many days, as you well know, and so I appreciate that.

Ms. Monroe, I understand that the—every time we start talking about Internet, marketing on the Internet, Internet taxes, all this such thing, we always come up with the organization called the Direct Marketing Association. And I understand—and, to their credit, have been very instrumental in working with the National White Collar Crime Center to begin in your Slam Spam. Can you explain how that information is useful in prosecuting spammers, the information that reaches the FBI?

Ms. MONROE. I'm going to ask Dan Larkin to respond to that question, since he works directly with that on a daily basis.

Senator BURNS. OK, thank you.

Mr. LARKIN. Yes, Senator. The information that we—or the partnership we developed with industries through the Direct Marketing Association enabled us to leverage very significant industry intelligence on the crime problem. As we've found, and I think one of the foundations of the FBI's cyber strategy is that we've got to partner with industry much more regularly and effectively than we have in the past. And this subject is one of the ones that they have significant intelligence and resources that have helped us identify the spammers, the techniques that spammers are using, and to help us kind of refine the list of priority subjects to go after.

Senator BURNS. Well, I applaud the Direct Marketing folks, and as they—you know, when Senator Wyden and I were talking about this—it only took us 4 years to pass the bill. We've had a lot of time to talk about it. But we thought, you know, basically if the industry comes together, because the industry understands that they've got a problem, the ISPs think that they have a problem in dealing with this. And it was to bring people together to formulate some standards of marketing on the Internet. Other words, there is a market out there, and legitimate marketers who identify themselves, we don't have any problem with that. And the general American public does not have a problem with that. It's the unwanteds—like the Chairman wants to do away—and child pornography, and he's right on point on that—is to take this illegitimate and this trash stuff off of there. So I just wanted to congratu-

late the Direct Marketing in the actions of partnering up with the FBI and the industry to clean that up.

And thank you for coming today. I appreciate all the remarks that all of you have made.

The CHAIRMAN. I thank you.

Thank you for coming, and we appreciate all your efforts. And I guess your message is that we should keep hope alive?

Ms. MONROE. Definitely so.

The CHAIRMAN. OK.

Chairman MURIS. And please pass the Cross-Border Fraud legislation.

The CHAIRMAN. Thank you.

Ms. MONROE. Thank you all very much.

The CHAIRMAN. Thank you for coming today.

Our next panel is Mr. Ted Leonsis—he is the Vice Chairman of American Online, and President of AOL Core Service; Mr. Shinya Akamine, who is President and CEO of Postini, Incorporated; Mr. Hans Peter Brondmo, Senior Vice President of Digital Impact, Incorporated; Mr. James Guest, the President of the Consumers Union; and Mr. Ronald Scelson, the President of MicroEvolutions. And would you all please come forward?

[Pause.]

The CHAIRMAN. We'll begin with you, Mr. Leonsis. Welcome back, and I see your old friend, Mr. Scelson, is here, as well.

[Laughter.]

Mr. LEONSIS. Thank you, Mr. Chairman.

The CHAIRMAN. We look forward to the testimony of all the witnesses. And, again, I want to apologize for the delay, and we hope we haven't disrupted your schedule for the day because of the meeting with the President this morning.

Mr. Leonsis?

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

Mr. LEONSIS. On behalf of the people of America Online and our 31 million worldwide members, I'd like to thank you for the opportunity to testify again before the Committee on the issue of unsolicited commercial e-mail.

My name is Ted Leonsis. I'm Vice Chairman of America Online, Incorporated, and President of the America Online Service. I want to thank the Committee for inviting me back to testify again, almost one year to the day after my first appearance. And let me tell you what a positive difference a year makes.

When I was here last year, we all sounded an alarm for action. Spam was exploding exponentially, and online users were drowning in a torrent of spam. We elevated the call for action against spam, and you responded, and you did a great service to the online medium and online consumers by adopting the CAN–SPAM law, and we thank you for that.

I want to thank you for doing so. In particular, I want to commend the leadership of Senator Burns and Wyden on this issue. CAN–SPAM was the right bill at the right time for all the reasons that we've discussed, and we look forward to measuring its success with more time.

But I am here to tell you, very affirmatively, that we've also done our part as a company. We're now veteran spam-fighters, and we've gone to the next level in our battle against spam.

First of all, we joined all of our members on a crusade against this blight. We turned our members into spam-fighters. We launched very comprehensive and expensive education and awareness campaigns to tell our customers how to fight spam in their own terms and on their own time, creating an anti-spam community where members help other members roll back spam by clicking on their "Report Spam" buttons. AOL members responded so enthusiastically to our call for action that, as we just announced this morning, two million of them signed our online spam-fighters petition in the past year alone in order to make their voices heard on spam.

And while we gave our members hope on the one hand, with the other we were arming them with great anti-spam tools. We launched new software last fall, and, in so doing, revolutionized spam-fighting on our service. We did so with adaptive spam filtering that is tailored to each member. We improved mail controls with an individualized permit/deny list. We unveiled a spam folder for every inbox. And we introduced a custom word list to block the most reviled spam terms.

And because you know and I know how critical it is to protect our children from porn and predators, we gave our members the ability to disable offensive images in their e-mail, and we enhanced our parental controls to allow parents to determine who can and can't contact their children by e-mail. We provided a report-card feature called AOL Guardian that tells parents who their children have communicated with each time they've gone online.

Second, we enhanced and improved our spam filtering, making the process the most accurate, effective, and efficient that it has ever been, thanks to our mail operations and anti-spam teams. And we expanded our postmaster team to a 24/7/365 operation to help to deliver the good mail to our members while keeping the spammers at bay.

We learned from spammers, and we're using their own tricks and ploys against them. Instead of strictly being in a reactive position, we are now, today, doing things proactively to disarm them before they try and click on the "Send" button.

Third, we are aggressively pursuing spammers in a series of lawsuits. We successfully concluded about a half-dozen Federal lawsuits against spammers, filed last April. We sued a group of spam conspirators in Florida, known as the Sunshine State Spammers in February of this year. We've collaborated with the Attorney General of Virginia on the first ever criminal state indictments of spammers. And, most importantly, we filed the first ever industry lawsuit using the new Federal CAN–SPAM law in March of this year, in cooperation with Earthlink, Microsoft, and Yahoo. Bottom line, we're finding the spammers, we're taking their spam gear and their spam toys, like their Porsches, and helping to put them in jail one by one.

Fourth, AOL is diligently and passionately working in state capital after state capital to encourage the swift adoption of tough, targeted anti-spam laws that mirror the Federal CAN–SPAM law at

the state level. This is very important, because it provides the one-two punch against spammers by also empowering state law enforcement to pursue spammers with criminal charges. Already, we're showing results, as Maryland has now just adopted the toughest state spam law in our country.

Fifth, we've even cast aside our competitive differences and come together as an industry, with partners, in conjunction with Microsoft, Yahoo, and Earthlink. We've teamed up for the sake of the entire online medium to fight the spammers with one voice, and combined our talents and resources in the areas of enforcement and technical solutions to spam.

As you know, Yahoo and Microsoft have developed their own technical proposals regarding e-mail authentication, and we're proud to say that AOL was at the forefront of testing new identity technologies, announcing last January, not today, that we would begin testing a new technology called SPF to help prevent domain-name spoofing.

As you can tell, Mr. Chairman and Members of the Committee, we've been very, very busy. And I'm optimistic. We had to be. Spammers aren't taking a break, and we aren't either.

Now, why are we doing this? We have to. We don't have a choice. Inaction on spam is a luxury we cannot afford at AOL, and it's something our members don't tolerate. And the action is paying dividends. Eighty percent of our members are now aware of our anti-spam efforts and agree that we are making efforts to reduce spam. That's up from about a 40 percent level in February of 2003. And clearly, the more we do on spam, the more we can positively impact customer satisfaction. And member satisfaction with our service is up, because the amount of spam reaching members has gone down.

Since this time last year, the volume of spam e-mails getting through to our members' inbox has dropped by up to 30 percent, even while the number of attempted spam messages has still increased. This means one thing. While the spammers are getting more desperate and aggressive, AOL spam-fighting is getting better. But, make no mistake, we're not going to rest, we're not in any way finished. My confidence is high. But the mission is not complete, and there's much more work to be done. The menace of bad spam still lingers.

As you may hear this morning, spammers and direct marketers would still like you to think that they are innocently trying to make a buck and live out the American dream, and that ISPs aren't delivering their goods. Don't be fooled. Many of them break the rules. They violate the integrity of our covenant with our members. They plague our children. And they cause millions and millions of online complaints every day. They are not part of the American dream. They are cause of a long, long, long nightmare for our consumers. Most of all, many of these outlaw spammers are still out there, and they're using the same old devious, deceitful, fraudulent, and evasive maneuvers. They're lurking and threatening, and they're not giving up. But we're ready and prepared. We have more tools, we have more weapons, and we're making the investment. But, most importantly, we have the passion and the will

to do this, and we have 31 million foot soldiers, our customers, leading the way.

In conclusion, while we still have a long way to go, these efforts are starting to pay off. Thanks to the hard work of you and your colleagues, in partnership with the industry and our consumers, many spammers are on the run. We look forward to building on the success in the year ahead.

Thank you very much.

[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, my name is Ted Leonsis, and I am Vice Chairman of America Online, Inc. and President of the AOL Core Service. I appreciate the opportunity to testify before the Committee on the issue of unsolicited commercial e-mail, or "spam." I testified before this Committee last year on this matter, and I am grateful for the Committee's continued attention to this important issue.

Although spam continues to be a huge problem facing Internet users and Internet service providers (ISPs), I believe that there have been significant developments in fighting spam over the past year that demonstrate that progress is being made. Thanks to Senator Burns, Senator Wyden, and other key Members of this Committee, a new Federal law known as the "CAN–SPAM Act" has provided some important enforcement tools in the fight against spam, as well as a heightened awareness of the need for cooperation between industry and government in the fight against spam. I would like to describe some of the ways in which these tools are starting to be used, as well as some other technology and policy initiatives that are helping to address the spam problem.

At this time last year, it appeared that the onslaught of spam was growing exponentially in a manner that threatened the vitality of Internet networks. Surveys at that time indicated that spam was doubling in overall volume every 4–6 months. While the statistics of spam volume have historically shown some ebb and flow, AOL spam data in the past several months has shown a decline in the spam growth rate that we are hopeful signals progress in the anti-spam war.

AOL continues to devote significant resources to the battle against spam. We have a team of anti-spam fighters on call 24x7 to fight spammers' varied and changing tactics. We continually adapt the strong technologies on our network to block and filter spam. Since the hearing last year, AOL has introduced new tools in the 9.0 version of our software to help our members, both in the U.S. and internationally, reduce spam to their inbox. AOL's Mail Controls allow our members to block e-mail from specific mail addresses or entire domains, or to create a "permit list" of addresses from which they will accept mail. We also are providing our members with important consumer safety tips that can help them reduce spam and improve the security of their online experience.

Included in AOL 9.0 is our "spam folder" feature. Beginning in October of 2003, AOL began transferring e-mail messages with characteristics indicating that the e-mail was likely to be spam to the "spam folder." This feature separates spam from the user inbox and allows the recipient to view such messages in a separate folder, or not view them at all. Between our spam folder and our anti-spam filters, we are now keeping up to 2.5 billion pieces of unwanted mail per day out of our members' inboxes.

We believe that our members' experience with spam is improving, based on information gathered through customer satisfaction surveys, as well as the number of complaints we are receiving through our "Report Spam" feature. However, even though subscribers to the AOL service may experience a decrease in the amount of spam that reaches their inbox, the total volume of spam that senders attempt to deliver to our networks continues to increase. Spam is still a major problem for online users and ISPs.

Last year, I testified that it is our belief that a large part of the overall spam problem is caused by "outlaw spammers," those who engage in fraudulent tactics such as hiding their true identity or the true source of their messages. We believe that outlaw spammers continue to be responsible for the majority of the spam problem that consumers and ISPs face today.

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 Internet domain names using a false identity for the sole purpose of transmitting spam.

We believe that more than 80 percent of the current spam problem comes from other ISPs and hosting companies that are infested with viruses. These software viruses, or "trojans" as we refer to them, typically make their way onto machines via vulnerabilities in end-user software and the absence of firewalls or anti-virus software. These viruses/trojans infect users' computers without their knowledge and allow spammers to use the infected machines to initiate or relay spam. We believe that most of the viruses/trojans are developed by the spammers themselves or hackers being paid by spammers.

Last fall, we supported the CAN–SPAM Act because it offered critical tools to ISPs and law enforcement to deter "outlaw" spam by imposing strict penalties on spammers who engage in techniques of fraud and falsification. Now that these tools are being utilized, we are optimistic that this new law will produce some positive results. Developing criminal cases against spammers and preparing civil litigation against them take time. However, we and our ISP colleagues, as well as the Federal Trade Commission, have announced major actions in the months following enactment of CAN–SPAM. Several recent announcements provide a glimpse of the significant efforts underway in this regard:

In March of this year, AOL, Earthlink, Microsoft, and Yahoo! announced the coordinated filing of the first major industry lawsuits under the CAN–SPAM Act. The country's four leading e-mail and Internet service providers filed six lawsuits against hundreds of defendants, including some of the Nation's most notorious large-scale spammers.

Similarly, the FTC made a major announcement at the end of April of its first set of enforcement actions using the CAN–SPAM Act against two spam operations that the FTC had found to have clogged the Internet with millions of deceptive messages in violation of CAN–SPAM and other Federal laws. AOL was pleased to cooperate in these investigations, and we look forward to continued cooperation with both the FTC and DOJ on spam enforcement.

AOL is pursuing other civil actions aggressively, and is also expanding its cooperation with state law enforcement to assist them in prosecuting spammers. In December of 2003, AOL collaborated with Virginia Attorney General Jerry Kilgore and others to announce the first-ever indictments under Virginia's tough, new anti-spam statute. Two out-of-state spammers from North Carolina who stand accused of spamming AOL members could face jail time, asset forfeiture, and monetary penalties in these cases.

Thanks to the attention and efforts of lawmakers on this issue last year, new legislation like the CAN–SPAM Act has spurred increased enforcement initiatives by ISPs and government. We are also seeing the level of enforcement on the rise in Europe, with the FTC cooperating with European agencies to bring legal action against spammers.

We are continuing to work with state lawmakers to support legislation to reduce "outlaw" spam. We are delighted that Maryland has passed a criminal spam law modeled on the criminal provisions of CAN–SPAM and that other states, including New Jersey and Ohio, are likely to follow suit later this year. These legislative initiatives show increasing recognition that the spam problem can best be addressed by providing specific enforcement tools that can be used to pursue spammers who engage in fraud and deception.

Ultimately, in order to radically reduce spam, we must know who the senders are. Spammers could not do what they do without hiding behind false names, trojan horses, and the like. That's why, in addition to enforcement and legislation, we are excited about the development of promising new technological advancements focused on authentication of senders. These technologies would allow ISPs to identify e-mail in order to prevent spam from entering our networks. A variety of different technologies and approaches are now being tested, all with the same goal of eliminating spam. AOL is participating in a number of working groups to discuss the development and application of new industry standard technologies for e-mail identity.

Specific technologies that appear promising are SPF (Sender Permitted From), CallerID, and DomainKeys, as well as variations or combinations of these approaches. These technologies aim to reduce the domain name spoofing that is central to many forms of spam by confirming that an e-mail is actually coming from the domain it claims to be from. The Internet Engineering Task Force (IETF), which is the standard-setting body for the Internet, is working to set technical standards using a combination of these technologies. AOL is currently testing the SPF tech-

nology, and we believe it can be implemented quickly due to its readily available software and already widespread adoption. Our assessment is that all three technologies can work well together and should be implemented quickly on a broad scale.

AOL has joined with other leading ISPs, including Earthlink, Microsoft, and Yahoo, to study ways in which we can make use of new technologies to reduce spam. In addition to working together to test authentication approaches, this ISP working group is discussing other types of best practices that industry can employ to fight spam. Potentially effective spam fighting methods that deserve further attention include: (1) for all ISPs to confirm that their members who are sending e-mail have accounts and are allowed to send mail; and (2) for abuses indicated by ISP members to be handled as quickly as they arise. We are continuing to work with our ISP colleagues to develop additional solutions to the spam problem, both from a technology and enforcement perspective.

In conclusion, we believe that industry and government have made great strides in fighting the spam problem over the past year, although there is much more work to be done. Professional spammers are always on the cutting edge of technology, which means that staying ahead of them requires extensive time, resources, and cooperation. The CAN–SPAM Act has provided some important tools for pursuing spammers; we believe we will start to see additional progress in the war against spam as these tools start to be employed.

AOL is committed to protecting our members and maintaining our leadership role in the fight against spam. We recognize that the goodwill and trust of our members depend on our continued focus on developing solutions to the spam problem. We continue to believe that 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 look forward to continuing to work with this Committee and other lawmakers, as well as with our Internet service provider colleagues, to stop spammers in their tracks.

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

The CHAIRMAN. Thank you very much.

Mr. Akamine?

**OPENING STATEMENT OF SHINYA AKAMINE, PRESIDENT AND CHIEF EXECUTIVE OFFICER, POSTINI, INC.**

Mr. AKAMINE. My name is Shinya Akamine. I'm President and CEO of an e-mail security company called Postini. We are a leading provider of e-mail security technologies. In my testimony today I'd like to comment on our experience with the effectiveness of the CAN–SPAM Act, as well as some suggestions for future improvements, what directions we'd like to see it go. And I'd like to spend the bulk of my time speaking about the state-of-the-art and recent technical developments in anti-spam technology. We're at the forefront of it in Silicon Valley and I'd like to share some of that with you. And just to summarize here, the point of view that I'd like to get across is that the technical solutions that are being presented by the private sector today already work, and for the customers who are using them there is no spam problem. For our customers, we're seeing a decrease of 90 to 99 percent of spam.

I'm going to base the rest of my testimony today on the data that we collect by operating the world's largest e-mail security system. We process about 1.5 billion e-mails a week; only AOL, Yahoo and Microsoft process more mail than Postini. By processing that much mail, we can see the kind of attacks and techniques that spammers are using, and our customers, including companies like Merrill Lynch, Circuit City, *The Washington Post,* United Nations and even, interestingly enough, Hormel, the makers of the canned Spam variety, are using our technologies to basically protect them-

selves from the Internet. But in the process, we get to see what the spammers are up to.

Okay so, in terms of commenting on the CAN–SPAM Act, we believe that it's very valuable, and of the 37 or so other laws that I've seen, this has been one of the most well-conceived and well-thought out statutes out there. And in particular, one of the reasons that I like it a lot is that it's one of the few laws that comprehends not only dangerous and objectionable spam content, like sexual content, but it's one of the few laws that also comprehends and prohibits abusive e-mail activities that are not related to content, and specifically by that I mean things like Directory Harvest Attacks, where a spammer will connect to a mail server and try to steal, essentially harvest, valid e-mail addresses, not for the purpose of sending a message at that time but to sell those addresses on the Internet and cause spam attacks to happen. So that is a threat that is not related to the content of the e-mail, it's related to the transport behavior of SMTP e-mail on the Internet, and this law is one of the few laws that comprehends and prohibits those kinds of abusive behaviors.

Paradoxically, although we think it's a good law, the spam rate that we have been observing, based on our 1.5 billion messages a week, has increased from 78 percent just prior to the enactment of the law to 83 percent as of this month. So in one sense the spam rate has increased 5 percent in 141 days but I think that the effectiveness of the law is basically indicated by the fact that without the law I think the spam rate would have increased faster.

Looking forward, there's kind of a couple of suggestions that people make about improving the CAN–SPAM Act and I think a large number of casual observers of the industry say, "It's a great law but you need to beef up the enforcement aspect." We actually don't agree with that. We think that it's a great law; it prohibits illegal activities, or defines illegal activities, now we believe it's the role of the private sector to actually go out and secure the customers' mail servers. In fact, one of the things, with all due respect, I'd like to comment on is earlier, two of the Senators commented about the idea of kingpin spammers or, I often hear at cocktail parties, there are ten spammers that make up 90 percent of all the spam in the world. It could be true. However, I've yet to see any data that actually supports that viewpoint and we are the fourth largest processor of e-mail in the United States and we don't have the evidence to support that viewpoint. The reason I make this point is that if one believes that there are ten, 100 or even 1,000 spammers responsible 90 percent of spam, enforcement may be the right way to go. But imagine is the world looks another way, which is, there are tens and thousands of spammers out there using cable modems and DSL lines to do distributed spam attacks. In that case, enforcement may not be the way to go. In that case, making private sector technological advances may actually be the right way to go. This is our viewpoint.

Okay, last I'd like to touch on where the state-of-the-art of spam technology is. Point number one, we believe that spam is a symptom. It's one of the most visible and painful symptoms but we think it's a symptom of the fact that e-mail today is fundamentally not secure. And so to use an analogy, if you have a dark house and you

don't have any locks on your house, you may have problems with burglary, with vandalism and trespassing. But do you have a burglary problem or do you actually have a security problem? E-mail servers today are completely open to the Internet and so without security and management layers, symptoms like spam come about. But if you think about it, there are other symptoms that are indicating the same root problem. There are e-mail-borne viruses, there are Directory Harvest Attacks, there are attachments that are being sent along with e-mails in all kinds of violation of corporate e-mail policy. So we would like to address the problem technology at the root level, which is the fundamental security of e-mail.

Second of all, there was a comment earlier about the fact that there is a bit of tit-for-tat, or an arms race aspect of the spam wars. So you know, when the spam filter companies figure out that spammers are trying to spam about Viagra, then spammers turn around and they start misspelling the word Viagra so that our filters won't catch them. So it's a bit of an arms race. But something fundamentally is changing in the private sector, and that fundamental change is the rise of companies like Postini which are taking a service model to the anti-spam problem. And by doing that we can aggregate so many customers and so much traffic that we've turned the scale advantage on its head and now we have more scale than the spammers. So, another way to think about it is, if you're a big spammer and you're sending hundreds of millions of messages a week, Postini is seeing 1.5 billion messages a week so the chances of being able to slip something by us is actually much more difficult today than it was before companies of our scale came into being.

So in the interest of time I'm going to wrap up here. But essentially I'd like to just summarize by saying that we think it was a very well written law. We think the value of it going forward is going to be not to enhance enforcement but rather to stay on top of new kinds of abusive behaviors and categorize them and include them in the law so that they are legally prohibited. Then, we think that the private sector, with technologies like the ones I've described today that Postini is providing, can essentially provide the locks to the doors of the Internet.

[The prepared statement of Mr. Akamine follows:]

PREPARED STATEMENT OF SHINYA AKAMINE, PRESIDENT AND CHIEF EXECUTIVE OFFICER, POSTINI INC.

**1. Effectiveness of the CAN–SPAM Act**

To date, the CAN–SPAM act has had no beneficial impact on the flow of spam. In fact, in the four months since CAN–SPAM went into effect, spam has increased from 78 percent to 83 percent of messages processed by Postini. Postini processes 1.3 billion messages per week, so the numbers are statistically significant.

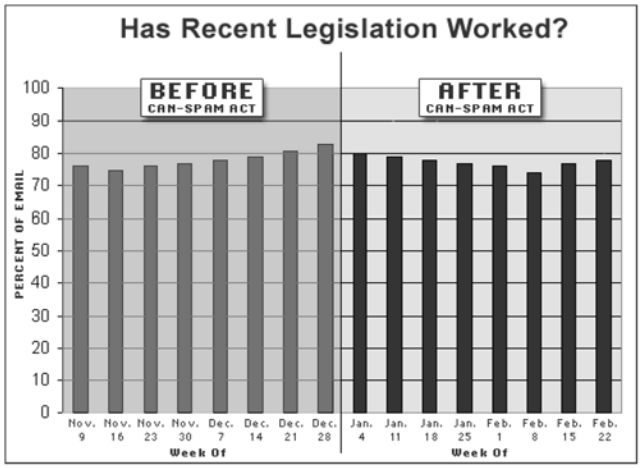



**Figure 1: The Amount of Spam Has Increased Since CAN-SPAM Went Into Effect**

*Suing John Doe*

Although they have garnered headlines, ISPs' recent lawsuits against alleged spammers are mostly "John Doe" lawsuits—215 out of the 220—highlighting the root problem: proficient spammers know how to hide their identities by using a variety of techniques including:

- Spoofed, or forged, message headers.
- Open relays to send messages.
- Open proxies to send messages.
- Viruses like Mydoom to infect people's PCs, turning them into "spam zombies," that send spam for the spammer.

*Jurisdiction*

In addition, many spammers are offshore, so they're beyond the reach of U.S. law enforcement.


**Figure 2: Spam Comes From All Over The World (Spam Sources, May 12 2004, taken from http://www.postini.com/stats)**

*Arrests Catch Small Spammers*

Recent arrests (Virginia and Detroit) are catching smalltime operators who are sending an insignificant amount of spam compared to the daily deluge clogging mailboxes. For example, the Virginia couple were charged with sending 100,000 spams in one month. Even if all of those messages were sent through Postini, it would represent just 0.0025 percent of all the spam we catch every day.

**2. Suggestions to Improve CAN–SPAM**

CAN–SPAM is a good law to have. The government should continue to enforce it and punish those spammers that can be found. CAN–SPAM should be left as is. Postini does not see any ways at this time to improve it. But Americans should not rely solely on laws. Although it's beneficial to have the laws on the books making spamming a crime, most spammers are criminals who are unconcerned about breaking the law. To use an analogy, even though burglary is illegal, private citizens still buy locks and alarms for their homes. Similarly, e-mail users need to take steps to protect themselves from spam and other e-mail threats. The nature of Internet e-mail protocols make sit easy for committed spammers to hide themselves from detection.

**3. Recent Developments in E-mail Threats and Anti-Spam Technology**

The problem with e-mail goes beyond just spam. Other malicious threats hurt the utility of e-mail, which is the most important form of communication in the world today.

- Viruses are delivered primarily via e-mail, and they are getting more frequent and

more destructive. Many new viruses turn people's PCs into "spam zombies" that send out more spam.

- Denial of Service (DoS) attacks, aka "e-mail bombs," are malicious attempts to crash e-mail servers and disrupt communications.
- Directory Harvest Attacks (DHA) are attempts to steal corporate directory information. They lead and fuel spam attacks.

*Spammers Are Changing Their Tactics*

Spammers are aggressively modifying their messages to defeat traditional, or first-generation, anti-spam technologies that were primarily based on content analysis. They use techniques like:

- Hash Busting—making slight changes to spam messages to fool signature, or hash, based spam filters.
- Bayesian Poisoning—inserting innocuous words into spam to fool Bayesian spam filters.

These techniques are relatively easy to spot and program around, but spammers are becoming even more covert.

Spam is becoming more personalized and unique. The following example has very few typical spam identifiers in it, making it difficult for ordinary content-based spam filters to catch.

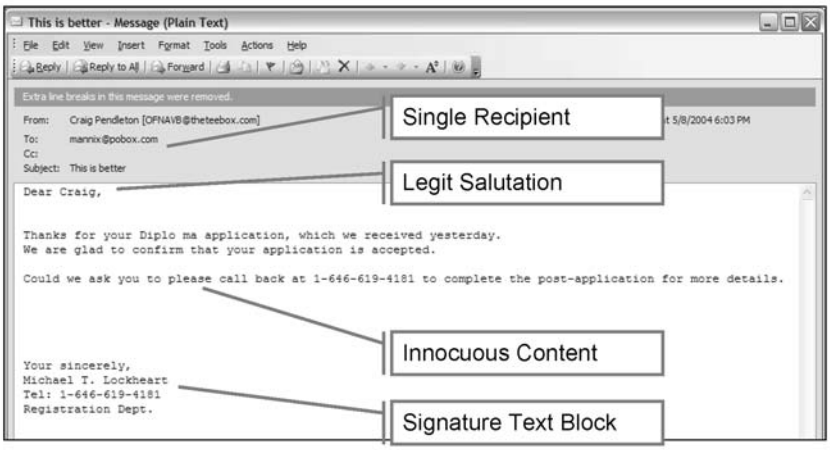



**Figure 3: Spam Messages Are More Personalized, With Few Telltale Signs of Spam**

Spammers are putting less and less content in their messages. Less content means less context for typical spam filters to assess, making it harder for such filters to accurately assess whether a message is spam or not.

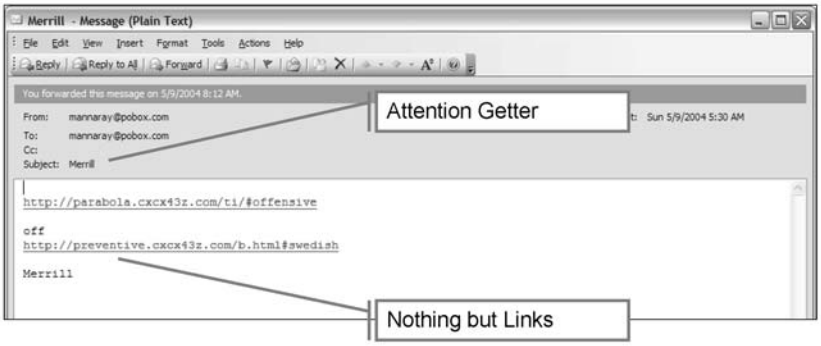



**Figure 4: Less Content Means Less Context And Greater Difficulty In Identifying Spam**

*Directory Harvest Attacks*

Directory Harvest Attacks (DHAs) are designed to net spammers lists of valid e-mail addresses to which they can send spam. They have a very nasty side effect: consuming enormous amounts of e-mail server resources while they deal with the DHA. Postini's average customer receives 40,000 invalid address lookups every day from attempted DHAs. (Postini blocks all of them.) In the last six months, Postini has observed spammers attempting to "fly under the radar" by launching more, but smaller, DHAs at their victims, in hopes of stealing data before being caught.

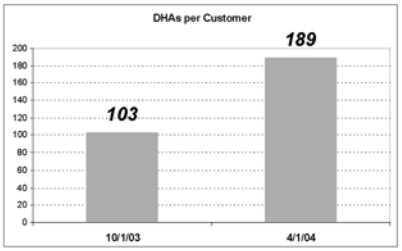



**Figure 5: More Directory Harvest Attacks Every Day**

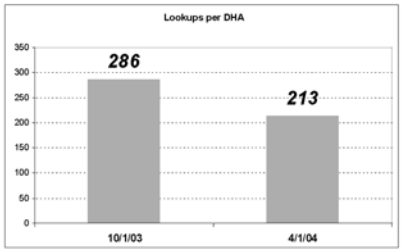



**Figure 6: Each DHA Is Smaller, To Avoid Detection**

These DHAs are often launched simultaneously, from many different computers. The spike in traffic from the DHAs can knock a mail server offline.

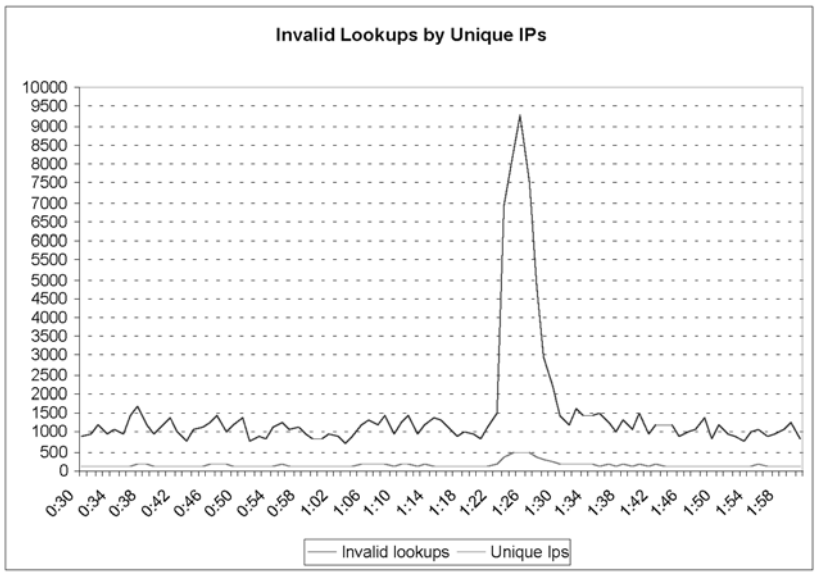



**Figure 7: DHAs Are "Bursty" and Cause Harmful Traffic Spikes**

*Second-Generation Solutions Are Here Today*

Private sector companies like Postini have developed second-generation E-mail Security & Management solutions that render the spam problem, as well the other e-mail threats, moot for their customers.

*Managed Services Are More Secure*

Postini is a managed service provider (MSP). By sitting "out in the cloud" of the Internet, Postini can protect its customers from threats before they ever reach their firewall. This means reduced traffic, reduced burden on mail servers, and better protection against threats.

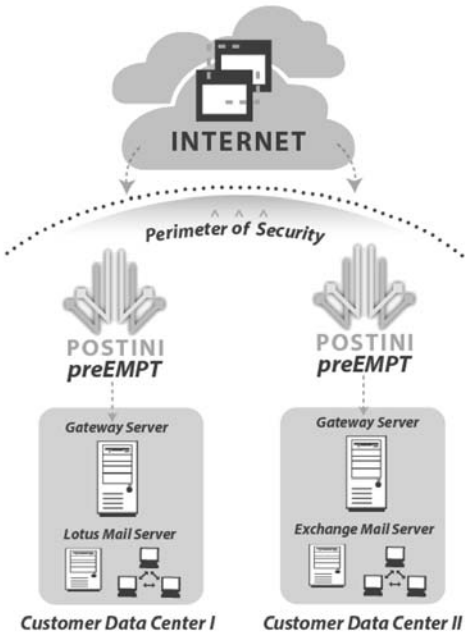



**Figure 8: Postini's Managed Service Sits Between Customers and Threats**

*Three Layers of Protection*

Postini has combined Connection Management, Content Filtering, and Delivery Assurance to provide powerful, effective protection to its customers.

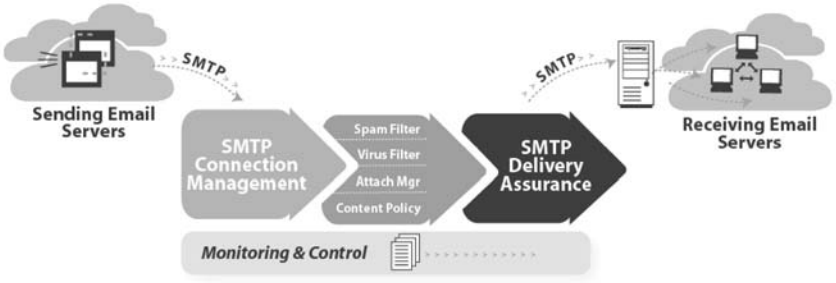



**Figure 9: Postini's Three Layers of Email Security**

*Connection Management* detects and blocks Directory Harvest Attacks and Denial of Service Attacks, as well as some spam, all without ever looking at the message contents. This is possible by looking at the behavior of the sending computer. Certain SMTP connection patterns are indicative of malicious behavior, enabling Postini to block connections without seeing the actual message. Currently, Postini blocks 53 percent of SMTP connections without examining the message itself. This is a powerful way to deal with spam messages with little content in them.

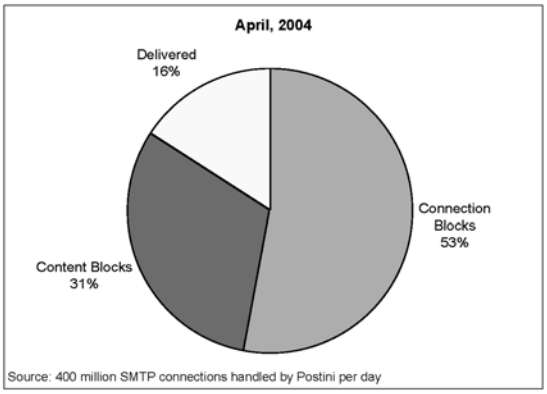



**Figure 10: Postini Blocks More Than Half of SMTP Connections Without Looking At The Message**

*Content Filtering* looks at messages for viruses and spam, using thousands of rules, or heuristics, constantly updated by Postini to reflect new spam types. New rules are always immediately available to customers without the need for them download or install any software.

*Delivery Assurance* ensures that when legitimate messages are delivered by Postini to our customers, they are delivered in a way that helps their mail servers perform at peak efficiency.

Sender Authentication Schemes Won't Actually Stop Anti-Spam

Much has been made lately of "sender authentication" by industry giants like Microsoft, AOL and Yahoo. While all of them have proposed different variations, they all have the same basic idea: if you can confirm that the sender of a message is permitted to send messages from the machine he's using, then you can eliminate a lot of spam. Bill Gates is apparently so excited by the idea that he made a speech in February, 2004 in which he said that spam would be eliminated in two years. There are many faults with these proposals that make them, we believe, unrealistic solutions to today's spam problem.

Each big company is pushing a different alternative that isn't compatible with the others. This lack of a unified standard will hinder widespread adoption. Microsoft is supporting "Caller ID"; AOL is putting its weight behind "SPF"; Yahoo has announced "Domain Keys".

All of the proposals require changes to every mail relay and domain name server on the Internet. A massive change like that takes a minimum of 5–10 years to happen. Until such a protocol change is fully deployed, it won't work—too many legitimate messages, sent from non-Caller ID computers, will be rejected by receiving mail servers.

If and when Caller ID is adopted, it won't actually stop spam. It is designed to authenticate that the sender of a message is allowed to send the message through the mail relay he's using to send it. The idea is to prevent the use of open relays by spammers. But spammers already have techniques to get around this type of defense.

- Spammers set up accounts with ISPs and use those to send their spam. Eventually the ISP may shut down their account, but they just move on to another ISP and another account. Just because something comes from its proclaimed domain, that doesn't mean its not spam. "Just because you are who you say you are, doesn't mean I want to listen to you."
- Spammers use viruses like Sobig and MyDoom to infect peoples' PCs, turning them into "spam zombies." The spam can be created to be "Sent From" the PC's owner, so it will be allowed to be sent, even under the sender authentication schemes.

The sender authentication proposals also have flaws that will block some legitimate e-mail. If you send e-mail from a Starbucks or an Internet café, whose mail relays belong to an ISP other than your normal one, your message will be rejected by the receiving mail relay.

In summary, it makes no sense for anyone to postpone the purchase of an enterprise class spam filter. Spam will continue to get worse during the next 5–10 years. Sender authentication is interesting, and probably useful, but it can't do what some people claim it.

**4. Summary**

Spam is a problem today only for companies and organizations that are unaware of—or unwilling to implement—one of today's second-generation spam blocking solutions. Spam filters can cost just $1 per user per month, and the payback period for companies installing such filters is typically just 3 months.

Postini has more than 3,000 customers today, with more than 5 million users, who have no spam problem. The bad guys are still out there, sending spam and other malicious forms of e-mail, but they can't get past Postini's defenses to attack its customers.

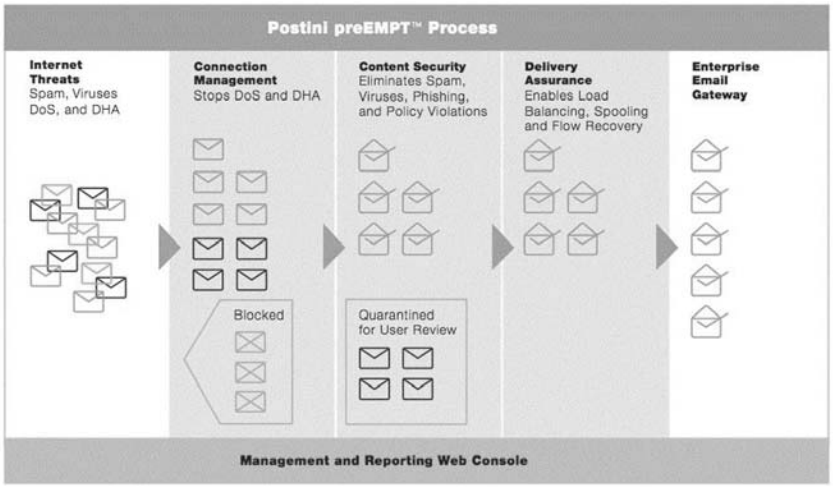
Postini appreciates the Senate's recognition of the important role that e-mail plays in our world today and the passage of CAN–SPAM. Free enterprise will do the rest.

POSTINI, INC.

*http://www.postini.com*

*Overview:* Postini, Inc. is the industry's leading provider of e-mail security and management solutions that protect e-mail communications infrastructure by preventing spam and other SMTP attacks from reaching the enterprise gateway. Postini's patented managed services model utilizes exclusive preEMPT™ technology to eliminate spam and viruses, stop DoS and directory harvest attacks, safeguard content, and improve e-mail performance. Founded in 1999, Postini processes more than one billion e-mail messages per week for more than 3,000 companies. By blocking spam, viruses and attacks before they can reach the enterprise e-mail gateway, Postini Perimeter Manager™ assures complete e-mail security while saving bandwidth, conserving server capacity and minimizing administrative costs.

*Services: Postini Perimeter Manager* provides preemptive e-mail management solutions that secure the productivity of your e-mail communications by eliminating threats before they impact your network. Unlike any other vendor, our patented managed service provides connection management, content security, and delivery assurance—offering the most comprehensive protection available.




Over the past four years, our customers, analysts, and the media have recognized Postini for its innovative leadership in e-mail security and management.

- *Recognized by Gartner as Leader:* Postini has been designated as a Leader in both vision and execution in Gartner Group's Enterprise Spam Filtering 1Q 2004 Magic Quadrant.

- *Assured accuracy in blocking spam and viruses:* Postini Perimeter Manager customers typically see 98 percent or better accuracy in blocking spam using our exclusive Preemptive E-mail Protection Technology (preEMPT).
- *Rated #1 in reviews and tests:* Several major industry publications—including Network World, InfoWorld and PC Magazine—have given Postini Perimeter Manager top ratings for accuracy and effectiveness.

*Superior administrative control and user flexibility:* Postini's spam and virus filtering engines apply e-mail security policy at highly granular levels that can be configured to user groups or individual users—all managed through a convenient web-based console. Users have the flexibility to review quarantined e-mails and customize filter settings as permitted by the administrator.

*Rapid activation with no upfront capital expense or ongoing maintenance:* A simple MX redirect activates the Postini e-mail security and management service. There is no hardware or software to buy, and no ongoing maintenance.

*No security or latency issues:* Because Postini does not rely on a store-and-forward process typical of other vendors, you avoid security and privacy issues. Our exclusive "zero-drag" pass-through technology eliminates any latency concerns.

*Ideal for heterogeneous and complex e-mail environments:* Larger enterprises gain the simplicity of blocking spam and viruses at the SMTP connection point before they can enter the network. For example, a recent USA Today article featured Postini as the ideal anti-spam e-mail security solution for Merrill Lynch.

*Confirmed policy enforcement:* Postini provides highly granular enforcement of policies for both inbound and outbound e-mail traffic. You can determine and enforce policy violations according to attachment types, message content, size and count limits, as well as specific recipient lists.

*E-mail Processing Statistics:* Postini processes more than 1 billion e-mail messages every week, sent to over 5 million e-mail users. More than 80 percent of these messages are classified as unsolicited e-mail or "spam."

*Customers:* Over 3,000 companies, representing a wide range of industries, and ISPs. Postini has developed a very satisfied customer base, with nearly 100 percent of customers renewing their services each year.

The CHAIRMAN. Thank you very much. Mr. Brondmo.

**OPENING STATEMENT OF HANS PETER BRONDMO, SENIOR VICE PRESIDENT, DIGITAL IMPACT, INC.**

Mr. BRONDMO. Mr. Chairman, Senator Burns, thank you for inviting me to participate in the review of the CAN–SPAM Act today. My name is Hans Peter Brondmo and I'm a Senior Vice President with Digital Impact, the Nation's largest e-mail service provider. Our company powers the customer communications and marketing e-mail infrastructure for over 100 large organizations, ranging from The Gap, Hewlett Packard, Yahoo, Marriott, Washington First Mutual Bank and many others. I'm also the Co-Chair of the Technology Working Group for the E-mail Service Provider Coalition, representing over 45 e-mail service providers, in turn representing over 250,000 American businesses.

Let me begin my remarks with a very simple observation; we've heard some of this already this morning. Spam exists because it is very, very easy to fake the origin of the e-mail, making it impossible to determine whether an e-mail comes from a good or a bad source. The consequence is that there is no way for senders to establish a reliable history of behavior; there's no trust and there's no accountability. It is not possible to hold those sending e-mail accountable for their actions because anyone who wants to avoid accountability can simply morph and change their identity at will. In order to stop spam, organizations sending legitimate e-mail must be able to step into the light, be securely identified, earn reputations and be held accountable for their actions. By leveraging the openness of the Internet, we can ensure that those abusing the e-

mail medium for what amounts to e-mail broadcasting can no longer do so while hiding in the dark corners of cyberspace.

The CAN–SPAM Act is an important contribution to the war on spam and I commend Senator Burns and Wyden for their leadership in this effort. Still, while modifying the code of law to impact behavior of spammers is necessary, it is not sufficient. Regrettably, the CAN–SPAM Act is unlikely to eliminate the hardcore spammers, especially those sending viruses and, as we've heard about earlier, perpetrating the phishing attacks, the most dangerous forms of spam, in my opinion.

I recently received a fraudulent e-mail pretending to be from CitiBank. It was a cleverly designed attempt at identity theft. I dug around the bid and discovered that the perpetrators of the scheme were running their operations from an ISP in Russia. I mention this example because it illustrates the breadth and severity of the threats to e-mail and reminds us that cyberspace knows no boundaries. E-mail is a very simple, open and vulnerable system. If the chairman would give me his e-mail address after this hearing, I could, from my laptop computer, with no special software and minimal technical expertise, send an e-mail that looks like you sent it yourself. If we cannot trust the sender of a message that may contain important, sensitive, personal or harmful information, that that message is in fact from who they say they are, we cannot trust the medium itself. The only way to solve spam is to change the e-mail infrastructure to support authentication and to facilitate accreditation and reputation services; credit scores for e-mailers, if you like.

Consider the evolution of another important communications infrastructure—air travel. Not long ago, I'm sure most of the people in the room remember, all you needed to board an airplane was a valid ticket. It didn't even have to have your name on it. A ticket was simply a proof of purchase, there were no security checkpoints and no I.D. checks. Then one day people realized that they could board airplanes carrying guns and explosives and hijack the planes. The response was to erect security barriers, yet just scanning people and their bags was not enough. Travelers are now asked to show government-issued identification, travelers' identities are matched against databases of known suspected people who could represent a future threat. The Internet's evolution has striking parallels to air transportation. Both the Internet and air travel infrastructure started out insecure and unregulated; both grew to become mission critical to the way we communicate and conduct business; both were abused due to security vulnerabilities. Yet we are still living in a world where no I.D. check is required in order to board a computer with an e-mail message. In the future, I posit it will be different. Just like we must present a valid I.D. in order to board an airplane, the e-mail infrastructure will require the equivalent of an I.D. to be presented by the sending computer in order to deliver its e-mail. If my computer tried to deliver the above e-mail to the chairman, using his own e-mail address under the scenario described earlier, it would fail because my computer would not be able to present legitimate credentials.

Several solutions, as we've heard referenced earlier, are in fact under development to support new authentication, accreditation

and reputation services for e-mail, spearheaded by industry players such as Microsoft, with their Caller I.D. proposal; Yahoo, with domain keys; SPF, as we heard referenced to, adopted by AOL, an open source initiative; Verisign, Bright Mail and Bond send it with accreditation and reputation services; Good Mail, with e-mail stamps, and others. Pre-market forces are alive and well and addressing the problem. The United Engineering Task Force of the ITF is in fact meeting in San Jose, California, as we speak to discuss, coordinate and review existing initiatives. And I got an e-mail this morning indicating that those conversations are going very well and that there's some very good progress being made between SPF and Microsoft's Caller I.D. proposal to create a single, unified standard to address this problem.

In closing, making hijacking a crime does not make our air transportation infrastructure safe. To make e-mail secure we must upgrade the e-mail ecosystem to support authentication, accreditation and reputation while also protecting the power of open, anonymous access to the information and communication services that makes the Internet what it is. Only then can we give back control of the in-box to the individual user. The emerging structural changes to e-mail will have wide-ranging consequences. In fact, accreditation and reputation systems have many similarities to credit ratings. There will be a need for transparency, fair and equal access, and this is better guaranteed through regulation and technology. While far to early to act, I believe this is where lawmakers should be focusing on e-mail as they set their sights to the future.

Thank you again for inviting my participation. I look forward to your questions and comments.

[The prepared statement of Mr. Brondmo follows:]

PREPARED STATEMENT OF HANS PETER BRONDMO, SENIOR VICE PRESIDENT, DIGITAL IMPACT, INC.

My name is Hans Peter Brondmo and I am a Senior Vice President with Digital Impact the largest e-mail service provider in the country. Our company powers the customer communications and marketing e-mail infrastructure for over one hundred large organizations such as the Gap, Hewlett Packard, Yahoo, Washington Mutual Bank and Verizon. In other words, we send e-mails that notify you about sales at your local Gap store, updates to your Hewlett Packard printer software and keeps you in touch with your bank. I am also the co-chair of the technology working group for the E-mail Service Provider Coalition, an industry coalition representing over 45 e-mail services providers.

It goes without saying that the spam problem is of great significance to Digital Impact, our customers and the ESPC. When we began to understand the scope of this problem a few years ago we decided that spam can be solved and that the solution can be summarized in one word: accountability. In order to stop spam, organizations sending legitimate e-mail must be able to step into the light to be identified and held accountable for their behavior. Any organization sending e-mail but not willing to be identified can then be treated with suspicion or may simply be blocked altogether. By leveraging the openness of the Internet we can ensure that those abusing the e-mail medium can no longer do so while hiding in the dark corners of cyberspace.

In order to hold senders accountable for the e-mail they send we need to update the e-mail infrastructure to support a new set of authentication, accreditation and reputation services. I will share some of the most recent developments in this space and describe why I agree with the claim made recently by Bill Gates that we will rid the world of the spam plague within two to three years. My perspective on how this is done differs slightly from Mr. Gates, but we agree on the objective and timeframe.

E-mail is a powerful, timely, efficient, cost effective, convenient and environmentally friendly way to communicate. Those abusing the e-mail infrastructure to spew out unwanted, unsolicited commercial e-mails by the billions and using e-mail to attack computer users with viruses and identity theft schemes are abusing a public commons for personal gain. I have been an e-mail user since 1982 and have come to rely on it more than any other tool of communication. E-mail has in fact become the number one preferred medium for business communications and one of the top three for personal communication. The abuse by those using e-mail to broadcast nefarious payloads is threatening the medium. We all agree it must be stopped. Yet the question still remains: how?

The CAN–SPAM Act is an important contribution to the war on spam and I commend Senators Burns and Wyden for their leadership in this effort. While modifying the code of law to impact the behavior of spammers is necessary, it is not sufficient. It is probably too early to determine the effectiveness of the CAN Spam Act, but there does seem to be evidence that the new law has turned up the heat on spammers who prior to January 1st 2004 were able to operate with impunity. Recently there have been media reports of spammers who have taken down their "shingles" because they do not want to risk jail time. Yet according to anti-spam firm Brightmail 64 percent of all e-mail in April was spam, a record high number. Regrettably the CAN Spam Act is unlikely to eliminate the hard core spammers, especially those sending viruses and perpetrating "phishing" attacks—the most dangerous form of spam.

I received an e-mail recently regarding my Citibank credit card. It claimed that there was a problem with my account and requested that I click on a link verifying my username and password. This cleverly designed message—a phishing e-mail—was designed to capture my username and password to steal personal account information. It was an attempt at identity theft. As I clicked on the link in the e-mail it took me to a fake web page that looked identical to the Citibank web-site. I dug around a bit and discovered that the page was hosted by an ISP in Russia. I have received similar e-mails over the past year purportedly from eBay, Visa, Earthlink and several other companies with whom I have business relationships. As you may be aware the IRS was recently attacked in similar fashion. Unsolicited and deceptive spam, while annoying and offensive, is no longer my biggest concern. My greatest worry is spam's evil cousins, phishing and computer viruses.

E-mail is a carrier of payloads. These payloads take many different forms. They may take the form of a written message from a colleague or a long lost friend, a digital photo from a family member, or a web page with clickable links and images from a company we do business with. As we all know, e-mails can also contain payloads that we don't expect, welcome or desire including offers for body altering herbs or undesired lewd images. The worst payloads contain computer worms and viruses that rapidly infect millions of computers and cause enormous economic harm and they contain schemes designed to play on our fears or abuse our trust while attempting to steal our identity in order to defraud us.

I mention these examples because they illustrate the breadth and severity of the threats to the e-mail infrastructure and to remind us that cyberspace knows no boundaries. A recent study conducted by the Anti-Phishing Working Group described 282 unique e-mail phishing attacks in the month of February 2004 alone. Brightmail reports a ten-fold increase in the volume of fraudulent e-mails from August 2003 to April 2004. Even if the law were to be effective in reducing unsolicited, deceptive commercial e-mail solicitations, the really bad guys will continue to operate without regard for U.S. law. Laws alone will not enable us to solve the core problems we are facing—we must look to changes to the technology infrastructure to address the structural vulnerabilities of e-mail.

E-mail is currently a very simple and open system. The simplicity of the e-mail protocols is probably responsible for its explosive growth and broad adoption. Yet with the simplicity of e-mail come vulnerabilities. The engineers that designed the protocols used by every e-mail system could not have foreseen the types of uses and the scale of deployment we have today. The vulnerabilities of e-mail are being exploited by spammers and only a change to the e-mail infrastructure can solve this problem and ultimately rid the world of spam, making it safe from identity thieves and making it much more difficult to distribute computer viruses. Such structural changes to e-mail will have wide ranging consequences. I believe that the current discussion needs to shift, and that the legal debate should now be focused on the new changes happening to the way e-mail will work in the future.

Consider the Nation's air transportation infrastructure. It was not very long ago when getting on an airplane was as simple as having a valid ticket and showing up at the airport on time. The ticket did not even have to have your name on it. It was simply required as a proof of purchase. No ID was necessary to fly, nor were

there security checks and luggage scans. Today things are very different. Why? Because the security of the infrastructure was compromised by passengers with anti-social motives. They carried dangerous payloads, hijacking planes for financial and political gain. A few bad passengers and their payloads threatened our safety by compromising air transportation. Airplanes were eventually even used as weapons threatening our very national security.

Making hijacking a crime does not make our air transportation infrastructure safer. While it is illegal to carry a weapon onboard a commercial airplane, it does not protect us from true harm. A multitude of security measures have been put in place to ensure that it is difficult to compromise the safety of the air transportation infrastructure. In order to board an airplane today we must present a valid government issued ID and we may be subject to screening to ensure that we don't have a history of anti-social or threatening behavior.

Returning to e-mail, we are still living in a world where no ID check is required in order to "board" a computer with an e-mail message. We do have the equivalent of airport screeners for e-mail in the form of computer programs, typically called filters, that scan the content of our e-mails attempting to determine whether the mail is spam or not. In essence, a computer is "guessing" whether e-mails are spam based on statistical analysis and rules applied to the contents of the message. Unfortunately, screening is far less effective for e-mails than for passengers boarding an airplane. Even if a great filter catches 99 percent of all spam, hundreds of millions of junk e-mails will still get through. Unlike a scanner at the airport, it is not economically feasible for a filter scanning electronic mail to request that a person look at every suspicious e-mail. When a computer is left to guess whether a message is spam based on scanning the content of an e-mail message it will not only miss unwanted messages, but also misclassify wanted mail as spam resulting in a false positives problem. Like spam itself, false positives reduce the value of e-mail and make the medium less reliable. According to research recently commissioned by Goodmail, sixty eight percent of e-mail users reported not having received important e-mails due to spam filters. A staggering forty eight percent reported not having received personal e-mails, twenty five percent said they had lost order and shipment confirmations and seventeen percent missed important work e-mail.

Spam continues to persist because it is impossible to trust the origin of e-mail and therefore impossible to determine with certainty whether an e-mail is from a good or bad source. The computer protocols that power our the foundation of our e-mail infrastructure are flawed because they make it very easy for any sender of e-mail to pretend to be whomever they want to be and to continuously change their identity. I can from my laptop computer, with no special software and minimal technical expertise send an e-mail that looks like it comes from any e-mail address of my choosing. In other words, it is trivial to spoof, or fake, the identity of the sender of an e-mail message. If we cannot trust that the sender of a message that may contain important, sensitive, personal or harmful information is in fact who they say they are, we cannot trust the medium. This is the essence of the problem we are faced with, a problem that legislation cannot address. Until we can trust and rely on a message in our inbox to be from the sender that shows up on our computer screen, we will not solve the spam problem. Worse we will continue to be vulnerable to the really bad stuff: phishing and virus attacks.

As mentioned above we can solve the e-mail security and spam problem by making a few changes to the Internet, upgrades that in fact are under way. Here is how it will work: Just like we must present a valid ID in order to board an airplane, the e-mail infrastructure will require the equivalent of an ID be presented by the sending computer in order to deliver mail. If I try to send e-mail using an e-mail from-address that I do not have control of under this scenario it will no longer work because my computer has to present its secure credentials and those credentials will not match the sending address. When I am sending from my own e-mail address, my secure credentials would validate that I am indeed who I claim to be. This is a good first step but the recipient may still not know who I am and therefore not know whether to trust me not to be a spammer or virus hacker. It is therefore also necessary to keep track of the history and reputation of senders, so all recipients can look up the past behavior of unknown senders once they've been authenticated. By checking the reputation of a sender, his e-mail credit score if you like, a determination would be made as to whether to let messages from that sender through, quarantine them for further investigation or simply reject them outright. Over time good senders would earn a good score (a good reputation) and spammers with their bad scores would fail to get their mail delivered. We would have accountability because we would have an accessible history of behavior.

Let me emphasize that this is not some academic pipe dream. A number of solutions are already under development by large and small industry players such as

Microsoft with its Caller-ID proposal, Yahoo! with Domain Keys, Verisign, Brightmail and Bonded Sender with accreditation and reputation services, Goodmail with e-mail stamps and others such as Sender Policy Framework (SPF) being spearheaded through an open source initiative. The Internet Engineering Task Force (IETF) is playing an active role to standardize the various authentication proposals currently being discussed. As a matter of fact, the IETF is meeting in San Jose, California as we speak to discuss these very issues and coordinate and review existing initiatives.

Let me in closing point out that the authentication proposals outlined above are not intended to track the behavior of individuals. They are intended to authenticate computers and domains, not individual e-mail users and addresses.

The real challenge we face is to facilitate the continued evolution of an e-mail ecosystem that supports authentication, accreditation and reputation services, while also protecting the power of open access to information that makes the Internet what it is. Technology and market forces will solve, in fact are now solving, the authentication and reputation problem. Authentication will enable law enforcement to do a better job and in combination with emerging accreditation and reputation services it will also allow the Internet to be more informed and individuals or organizations to make decisions about what sources of e-mail they should trust. The emerging accreditation and reputation systems have many similarities to credit ratings, and there will be a need for transparency, fairness, and equal access that is better guaranteed through regulation than technology. While too early to act, I believe this is where regulatory action and oversight in the e-mail space should be setting its sights.

Updating the Internet as I have described in my comments means that we must create an infrastructure that supports accreditation of senders, implements authentication of the computers sending e-mail and provides generally accessible reputation services. This is no small task, but it can and will be done. And once computers have identities and reputations, we will be able determine whether to trust the source of incoming e-mail allowing desired messages into our inbox or throwing junk it the proverbial bit-bucket based on the recipients' personal preferences and taste, not laws and regulation.

The CHAIRMAN. Thank you very much. Mr. Guest, welcome back.

**OPENING STATEMENT OF JAMES GUEST, PRESIDENT, CONSUMERS UNION**

Mr. GUEST. Thank you, Mr. Chairman, for the chance to appear here again, and members of the Committee. I'm Jim Guest, President and CEO of Consumers Union, Publisher of *Consumer Reports* and *ConsumerReports.org*. And this is an issue of great interest and importance to consumers, obviously, around the country.

We start with the key question, are consumers today getting less unsolicited commercial e-mail since the anti-spam law went into effect in January? And it's—as you point out, Senator Burns—it's too early to have definitive results on something like this but at least the early returns are that there certainly has not been a substantial reduction in e-mail and in fact, there is indication that consumers are receiving even more spam than ever, as your earlier witnesses alluded. This past March *Consumer Reports* did a survey, commissioned a survey on spam drawn from a nationally represented panel of more than 2,000 on-line users and here's what we found, kind of supplementing and confirming the Pew study that you referred to earlier, Mr. Chairman. In our study, four out of five respondents, 80 percent, reported that they had not seen any reduction of spam compared to 3 months earlier, before the CAN–SPAM Act went into effect. More than two out of three of the respondents, 69 percent, noted that spam comprised at least half of their e-mails, and a majority of respondents found that the unsubscribe, or opt-out links, were not very effective in stopping spam from reaching their mail boxes.

When we did the article last August in *Consumer Reports* on spam, this issue here, which I think we provided to members of the Committee, our recommendation to policymakers for legislation attempting to reduce spam, was to create two things—an opt-in system coupled with a private right of action to allow individuals to bring suits. Obviously, the law that passed Congress went a different direction with a mechanism for opt-out rather than opt-in. In that same article, and today as well, our recommendation to consumers is that they not click on unsubscribe or opt-out links because this may well signal to the spammer hey, I've found a live e-mail address, and that can lead to more spam rather than less spam. There's simply no way for consumers, as you've heard from all of us here, to distinguish from legitimate marketers and rogue spammers who will misuse that unsubscribe link. And so there is a catch-22 really, for consumers, where the main remedy that the law provides, which is an opportunity to opt out, is a remedy that we advise against and caution against because it can invite more spam, not less.

So imagine, for example, that you put a sign out on the front door of your house, "Do not solicit." But still, every company in the world was allowed, nevertheless, to knock on your door once, but to knock on your door despite the sign and then, at that point, you can tell the salesperson, "Please don't knock again." And then you wait for the next salesperson to knock on the door. Obviously this is an absurd burden to place on people; we all know that "do not solicit" means exactly that—you do not want to be solicited—and you ought to be able to say that once and clearly and have that block unwanted solicitations. Consumers can say "no" to advertising at their front door, period, but not so in the case of spam.

And I'll take another example, which we have talked about earlier, the "Do Not Call" list and the enactment of the FTC's implementation of that, where consumers now have a real, effective tool to say, "No advertising at the dinner table." Congress should provide consumers with the same ability to say "No advertising on our computers." If we can stop people from ringing our doorbell, if we can stop people from ringing our phone at dinner, if we can stop people from sending unwanted faxes, all by an opt-in or just a one-step-blocks-all, there ought to be the same protections, in our view, with regard to spam. So the Congress should put the burden on spammers to get permission to intrude, not on consumers to fend off the intrusions and the filter of junk mail.

Now, the ingenuity of spammers appears to be bottomless and it will be an enormous challenge for Congress to keep pace, as you've heard from all of us here. They're finding novel ways to spam us; they've figured out myriad methods to avoid being filtered by the ISPs and consumers; they've discovered how to commandeer our computers to send spam for them, and they're even now finding new ways to use devices besides computers where they can send spam. We're looking, for example—a hard look—now at wireless spam, the act of spamming cell phones and pagers. Congress, with the leadership of this committee, was wise to attempt to ban wireless spam completely in the CAN–SPAM Act; we've actually submitted comments early this week to the FCC about the problem, where we urge the Commission to insure that certain kinds of wire-

less spam don't fall through the cracks, and it's a danger that they will.

So we would suggest, Mr. Chairman and members of the Committee, and we're pleased to see that you are monitoring the progress here and we think you're going to need to monitor during the rest of the year, because there's not a lot of time. The studies are all showing spam is still going up and the early returns, I think, may well turn into a lasting trend. So Congress needs to take fine-tuning this law seriously, as I know you are, because spam may not only make wireless devices less useful but e-mail in general. And that gets into the situation where—you gave the numbers earlier—52 percent of users a year ago said they are less trusting of e-mail because of spam; today 63 percent, up from 52 to 63 percent, are less—well, 63 percent are less trusting of e-mail due to the in-box that's crammed with spam. And that has all kinds of potential implications about trust in the Internet, trust in doing business over the Internet, e-commerce, all kinds of implications farther on.

So our bottom line, speaking for consumers, Consumers Union, is that Congress should not place the burden on consumers to fight the flood or spam. No matter how skillfully you try to provide more and more tools to the consumers, it should place the burden on the marketers. And again, if you can stop faxes and phone calls and visits, knocks on the front door, by one step to block all those unwanted intruders, there ought to be a similar response on spam. You talked about keeping hope alive. Well, our hope is that you will, in fact, and I'm confident that you will, continue to monitor this, make the further adjustments that are needed so consumers finally can say no to spam, generally, and it means no.

Thank you.

[The prepared statement of Mr. Guest follows:]

PREPARED STATEMENT OF JAMES GUEST, PRESIDENT, CONSUMERS UNION

Chairman McCain, Ranking Member Hollings, and other distinguished members of this committee, I would like to thank you for inviting me to address you again today on behalf of Consumers Union,[1] the non-profit publisher of *Consumer Reports* magazine.

Are consumers getting less unsolicited commercial e-mail since the new anti-spam law went into effect in January? While it is still early to have definitive results, the answer unfortunately seems to be no—in fact, consumers appear to be receiving even more spam than ever. And just to provide some perspective on the volume of spam consumers are barraged with on a daily basis, Brightmail, a producer of anti-spam software, recently measured 63 percent of all Internet e-mail as spam, compared to just seven percent in March of 2001.

The CAN–SPAM law has not yet achieved its intended aim, but we should all acknowledge that this is a dynamic process. Much as it took a decade to enact a meaningful Federal "do not call" list, in passing the spam law, this Committee needs to monitor developments with spam carefully and continually look for ways to fine-tune the "CAN–SPAM" Act. In order to truly "CAN–SPAM," Congress will need to

[1] Consumers Union is a nonprofit membership organization chartered in 1936 under the laws of the State of New York to provide consumers with information, education and counsel about goods, services, health, and personal finance; and to initiate and cooperate with individual and group efforts to maintain and enhance the quality of life for consumers. Consumers Union's income is solely derived from the sale of *Consumer Reports,* its other publications and from noncommercial contributions, grants and fees. In addition to reports on Consumers Union's own product testing, *Consumer Reports* and *Consumer Reports Online* (with approximately 5 million paid circulation) regularly carry articles on health, product safety, marketplace economics and legislative, judicial and regulatory actions which affect consumer welfare. Consumers Union's publications carry no advertising and receive no commercial support.

update the law to keep abreast of new developments in technology, such as wireless spam, and keep on the trail of elusive spammers who are every day finding new ways to beat spam filters and evade anti-spam technologies.

But first, let's look at what's happened since the law went into effect in January.

This March, *Consumer Reports* commissioned a survey on spam drawn from a nationally representative panel of more than 2,000 online users. Our September 2004 issue of the magazine will include more in-depth reporting and spell out more details from the survey, but I wanted to provide a snapshot of what we found to help inform the discussion today:

- Most (80 percent) respondents reported that they had not seen any reduction of spam compared to three months ago—before the CAN–SPAM law went into effect.
- About two thirds (69 percent) of all respondents noted that spam comprised at least half of their e-mails.
- A majority of respondents found that the "unsubscribe" or "opt-out" links were not very effective in stopping spam from reaching their mailboxes.

Another survey conducted in March by the Pew Internet & American Life Project also shows that spam does not appear to be on the decline. They found that:

- 24 percent of respondents are receiving more spam than before January 1
- 53 percent have not noticed any change
- 3 percent do not know
- Only 20 percent report that they are receiving less spam.

When our magazine reported on spam last August, our recommendation to policymakers for any legislation attempting to reduce spam was to create an opt-in system coupled with a private right of action to allow individuals to bring suit. We were pushing this solution rather than legislation relying on Internet service providers (ISPs), the Federal Trade Commission (FTC), and state attorneys general for enforcement. The law that this Congress passed went a different direction, with a mechanism for consumers to "opt-out" of unsolicited commercial e-mail.

Our recommendation to consumers at the time was that they not click on unsubscribe or "opt-out" links, as this may signal a spammer that the user's e-mail address works and cause them to get more spam. And our recommendation has not changed—leaving users in a difficult position with perhaps no real remedy against spam for the time being.

We still believe that "opt-out" creates a tremendous burden on consumers, because they have to say no to each and every piece of unwanted e-mail—which results in a big loss in time and a big increase in frustration. And as I indicated earlier, our survey results show that "opting out" has not even been effective in stopping the flow of spam.

But even worse, there's simply no way for consumers to distinguish between legitimate marketers and rogue spammers who will misuse an unsubscribe link. The result is a consumer catch-22, where the main remedy the law provides—an opportunity to opt-out—is one consumers shouldn't use.

We believe the core improvement necessary in the spam law is to change the model from "opt-out" to "opt-in." The law as it stands puts too much burden on consumers to block spam and makes it too difficult to hold spammers legally accountable for their inappropriate interference with consumers' e-mail.

Imagine that you put a "do not solicit" sign at the front door of your home, and every company in the world could only ring your doorbell once, at which point you could tell that salesperson not to bother you anymore. You would need to keep track of each company you told not to solicit you, and if a company violated your request, you could petition the Federal Trade Commission to take up your case. Of course, this is an absurd burden to place on people. We all know that "do not solicit" means exactly that. Consumers can say no to advertising at their front door, period. The Federal Trade Commission's enactment of a robust "do not call" list means that now consumers have a real tool to say no advertising at the dinner table. Congress should provide consumers with a similar tool to say no to advertising on our computers.

To be clear, the law as passed had several excellent achievements: it prohibited senders from falsifying their identities, using misleading subject lines, and from harvesting e-mail addresses in certain ways. By requiring that spam is clearly labeled and that pornographic e-mail is effectively in an "e-mail envelope," over time this law may reduce the amount of obscene and objectionable content that parents and children have to see.

However, the ingenuity of spammers appears to be bottomless and it will be an enormous challenge for Congress to keep pace with them. They find our addresses in novel ways. They have figured out myriad methods to avoid being filtered by ISPs and consumers. They have discovered how to commandeer our computers to send spam for them, and they are even finding new devices, besides our computers, where they can send us spam.

For example, Consumers Union is also taking a hard look at wireless spam—the act of spamming cell phones and pagers. It's a practice that's more distracting and invasive than computer spam, since phones receiving messages beep or vibrate with each message. And the economics of wireless spam are different, since the costs of these messages are often borne solely by the consumer—at the rate of up to 15 cents per message.

Congress was wise to attempt to ban wireless spam completely in the CAN–SPAM Act. Consumers Union submitted comments in the Federal Communications Commission's wireless spam proceeding this week, where we urged the Commission to ensure that certain kinds of wireless spam don't fall through the cracks. While wireless spam sent to an *e-mail address* is prohibited under the CAN–SPAM Act, and wireless spam sent to a *telephone number* is under the purview of the National Do Not Call Registry (under the Telephone Consumer Protection Act), wireless spam sent to a *5-digit "short code"* that some wireless carriers now use may fall into a regulatory no-man's land. Wireless carriers are now pushing to explicitly exempt these 5 digit "short codes," though our position is that they should be covered either by the Do Not Call Registry or covered by the CAN–SPAM Act.

However, cell phone carriers may have a way around even these protections. Wireless companies are aggressively trying to get consumers to "opt-in" to business relationships with marketers, for example by getting them to vote on the TV program American Idol using 5 digit "short codes." Consumers should beware that simply by playing along with a TV show, they may unwittingly be signing up for loads of wireless spam.

Congress needs to take fine-tuning this law seriously because spam may not only make wireless devices less useful, but e-mail in general as people are trusting it less—spam may "kill the killer application," as FTC Commissioner Swindle put it. The Pew survey shows a jump in e-mail users who have reduced their use of e-mail because of spam—from 25 percent last June to 29 percent at present. A year ago, 52 percent of users said that they are less trusting of e-mail because of spam; today, 63 percent of users report they are less trusting of e-mail due to inboxes crammed with spam.

As our *Consumer Reports* investigation last August confirmed, spammers are difficult to prosecute because they are often impossible to find. They hide behind an untraceable tangled web transcending national borders, leaving few—if any—virtual footprints. Right now, national opt-out legislation is trying to curb an international problem perhaps without the full resources necessary to track violators of the law. An opt-in system would mean spammers would be forced out of hiding and forced into accountability.

Our bottom line is that Congress should not place the burden on consumers to fight the flood of spam, it should place the burden on marketers to woo consumers in a permission-based marketing model, enticing them with attractive, selective offers, not bludgeoning them with an enormous volume of junk. We look forward to continuing to work with this Committee to keep pace with technology and to help this law achieve its full potential. Thank you.

The CHAIRMAN. Thank you very much, Mr. Guest. Mr. Scelson. Welcome back.

## OPENING STATEMENT OF RONALD SCELSON, PRESIDENT, MICROEVOLUTIONS.COM

Mr. SCELSON. Hello, Senator McCain, Chairman. This is going to be long.

The FBI, as far as enforcing and trying to catch people sending pornographic spam, etcetera, AOL, Hot Mail, MSN, all these people pay top dollar to some of the top people in the world to stop them. They don't do really good. The FBI pays minimum wage to people that, for the most part, that really aren't that computer savvy. We had our systems hacked in heavily about 3 years ago. I went to the

FBI with logs and everything to prosecute this. I've seen the best people the FBI has for computers. You're going to get the little mailers but the people that really know what they're doing—the FBI—needs a lot of training. And they need to employ people that know what they're doing to catch these type of people.

Last year when I was here, I was sending 100 percent spam because I was forced into it. Since December 15 until now, I am now sending within canned spam 100 percent legal mail. Now, just working my way down the line, from the order the people came in, AOL gives a nice representation of such a perfect, innocent company doing everything it can to help stop spam. Just last year, Mr. Leonsis stood up in front of everybody and admitted they do send bulk e-mail like us but they provide, quote, "opt-out." Those were his own words. Well, my company went to AOL for a white list, not letting them know it was me, of course. And they put us on their white list. Now, the white list says you have to be opt-in, which is not what the law says and not what Mr. Leonsis admits they do. Once again, the big companies are taking added power to this than what they should be doing. When we sent mail into AOL we only sent mail for 4 days. We had a 98 million database that had been gathered and built since I started mailing. Part of this was sold, as everyone knows, from AOL years ago when they did this. And those mailings, it was reduced down to 27 million, with less than 1,000 complaints per million. That is a significant increase of how much the lists were cleaned and how much the law did help. When AOL found out it was me—and I have the gentleman's name that's their head postmaster—basically I was told that either I have to prove 100 percent opt-in, they don't care who we are or how light we mail, and they're going to send it over to their legal department. Now, when I was contacted about coming here I started researching all this stuff. And I found out that AOL has seven injunctions against them since this new law. Mandatory court orders to accept mail. And they have totally ignored every one of these court orders. And I've passed some evidence files to you of this today from these court orders. So the company that wants to look the best and try to act like they're the best and so innocent, when the law works against them, they don't want to hear that because they're so big. And this is not fair to bulk companies.

As far as the new spam filters. You know, it was really getting annoying every 2 or 3 weeks to have to update our mailers and figure out a new way to get in. This was really getting old quick; it was a pain in the butt for a while there. So we sat down and looked at Bayesian and how the system works; we actually dissected a bunch of games like Dune because the IA system that it all works on is all the same thing. Well, we know have a new mailer, it's 98 percent complete—we're still debugging parts of the code in it—but this new mailer basically generates anywhere to one sentence to 30 sentences, perfect punctuation, perfect words, all of which are not in the blacklisting or key spam words, and adapts to compensate for any filter they put against it. We also found out a new system that we work with that gives us IP addresses, legally, of voice-over IP telephone systems, which are worldwide. We have roughly five e-mails per IP address goes out before we hit that IP again in a month; there are that many IPs available to us. So based on this,

no e-mail we send will ever be identical. But we still stay 100 percent in compliance with the law. The IPs are ours to use, we are paying for the right to use them.

Headers being forged. There are 5 true standards of ways to send mail. Our system changes our headers constantly but like the "received from" line of the header, we'll have our own IP addresses in there. So even though we're changing the headers to get through the filters, all the information that's being used is 100 percent ours, we own and paid for.

I'm so tired of hearing so many people stand up and say, "No matter how much mail you send it doesn't cost anymore." Gentlemen, you all have made it very far in life and are very intelligent. Simple math will tell you, if it takes a T–1 to send a million e-mails a day, if I pump out 50 million, I need a lot more T–1s. T–1s can cost anywhere from $350 to $3,000, $4,000, depending on loop charges, etcetera. So obviously, the cost for me to send e-mail does not stay the same; the more I send, the more it costs. From the smaller mailers in the industry that don't develop own software and all and they buy the stuff that's available, spam for them has gone up 200 to 300 times more than what they used to send. Because these people do not know how to penetrate most of the filters, their logic is, OK, if I sent one million e-mails last time to make X amount of dollars, well because the filters, even when they sent legal were tearing them up so bad, they decided, OK, we'll send three to four times as much e-mail to still make the same amount of money. So spam in that sense is on a major increase.

A lot of the carriers, like WorldCom, there has been a debate back and forth whether or not they're a common carrier, if they are or are not, AOL got the standard that they're not a common carrier. In 1997, there was a little girl in a sexual incident that occurred and a lawsuit placed against AOL. And I think this was before Mr. Leonsis was at his position over there. And AOL stood up and said, "We're a common carrier, we can't do anything about it." And they won the lawsuit. In 2000, FCC stood up on behalf of AOL and testified that they are not a common carrier. Well, at that time they didn't own an Internet company like Charter, so technically no, I guess they wouldn't be a common carrier. Now they have their own dial-up in Internet service and cable lines. The carrier I was on, WorldCom, when I was mailing to AOL and under their white list, AOL was nice enough to send me a letter saying that we are on their white list, we are not spamming, this is not unsolicited and I have full permission to mail there, which a copy of this was also given to you. WorldCom's reply was, they don't care what your law is, they don't care what they do or how they do it—meaning AOL—we cannot send bulk mail. Period. And if we send another piece of it they're going to pull the plug on us. Well, WorldCom is definitely, without a doubt, a phone carrier. They provide me not Internet service but they provide me bandwidth, loop charge basically, as far as the pipe to me, which under the FCC regulations is a common carrier. Another thing in the research I found out on common carriers is, FCC does not have the right to decide if AOL is a common carrier or not, or any Internet company; only an act from Congress can make this difference. And to my knowledge and in all the research I've found, Congress has made

no acts to this. So if this is the case then the filtering, reading and destroying the people private e-mail is wrong.

As far as the forging headers and forging subjects. One of my other IP ranges that I mail to AOL is not blacklisted—or Hot Mail or any of these—which is MicroEvolutions. If I use my valid from address of *MicroEvolutions.com,* AOL is blocking this, which by law I'm supposed to do. If I use my company signature and a disclaimer at the bottom with a remove link, I cannot deliver into AOL without taking that out of there. Once again, they're interfering with the new law. But they turn around and say spam's on an increase. Well, does the government want us to mail legal or not? And if they do want us to mail legal, the laws don't necessarily need to be increased toward us as they do toward the ISPs that are interfering with us to do legal business.

As far as a way to solve the problem. The new ways are definitely a good way to go. Personally, the reason that most of the ISPs and spam groups and anti-spam groups don't want a global remove is because, as these gentlemen said, if some stupid mailers—and that's the only way I can word it—in the world will take these addresses and mail to it. Now personally, when I mail to carriers like AOL, I get as undeliverables. I know who's a good user and who's not a good user. If I mail to Hot Mail, their server tells me whether this user's good or not. So I know without a doubt if your address is good or not; I don't need a remove to tell me that's a good address. I need a remove to take people off my list. Well, the anti-spammers don't want mailers to use this. The mailing association don't want us to upload our list to you because now you have all of our data bases and you can make money with this. The solution I found is a system that we can put together very shortly, that the minute a person submits a remove address to a government server—government site—it encrypts this data, 128 bits, same stuff your military works on right now. A program is given to the bulk mailers, which is what they use to do their removes. When the addresses are sent to this remove program, they're all encrypted, the mailers themselves never get to see the addresses; all it does is remove those users out of their list. This protects the identity of the person being removed and gives the mailers a way to be removed. With the current law, AOL has a nice little system they're working on in place they call their SCOMP system, or report spam button. Now, to stay in compliance with the law, if I send e-mail to them, they send me a message back, telling me this person reported spam. Not staying in compliance with the law, AOL does not tell me who this user is that complained, thus I cannot remove this user. If you can't remove the people then I'm violating the law but AOL's not telling me who it is that wants this. So it makes it really hard to pull these people out of the list.

On the remove side of things the—I'm sorry, I lost track for a second—the government basically needs a way to make things look good to the people. Right now you passed a law that looked good but it hasn't done a whole lot and this isn't what you're looking for. You're looking for the people to praise you. That's what it all boils down to. If I send—3,000 bulk mail companies send you e-mail, you don't want to go to each of these people and be removed. That's a real time consuming pain in the butt. So by having the global re-

move, you remove yourself once, problem solved. People sending mail not using that system would be in violation. Another thing that would be really nice to add to this is—Hot Mail and MSN and a few other companies like Yahoo—they're using third party companies, like Bonded Sender, that white list your IPs. The problem with these companies are—I'm sure you remember back in the days of the mafia. I have a legitimate business, sending e-mail 100 percent legal. But I've got to pay this third party company—the mafia—to give me protection in order to mail into their network. The problem is, for $25,000 a year, there's no guarantee they're even going to let you send mail there. They can shut you down at any time so you have no guarantee. And they talk about us scamming people?

The CHAIRMAN. Are you paying that now?

Mr. SCELSON. No sir, I will be at the end of this week, though. I was actually just working with them so—I'm trying every way I can to stay white listed. I'm still working with AOL's department on getting re-white listed. The last conversation I had was either back off or we're going to sue you. I'm not afraid of people. The worst they can do is take everything I have and auction it away and what's this do? It puts me back on food stamps. I've lived that life already so this is no big fear to me. If I go to jail over this, to me it's the stupidest thing you can go to jail on but because I am staying in compliance with the law I don't see any, at this point, criminal actions that I'm doing wrong to be put in jail for. Now, they on the other hand, are ignoring court orders. To me, this is wrong.

Bonded Sender has one feature that is nice about them. If the government was to do this type of global remove, the company that's using the remove would have to post all their information to the government, provided they get their updates daily to do the removes for the people, and the government white lists their IPs so that carriers like AOL and stuff know these people are working with the government, they're getting the government's removes and these people are mailing legally, to let the mail in. Everyone else out in the world is spamming, and it's a lot easier to track down people that are spamming than ones that are not spamming. But as long as we're doing it the right way we're going to be blocked, interfered and shut down, people are going to go around it. Right now there's a major security leak we recently came across. In Windows XP 2003 and Linux, we are now 100 percent of not only forging the person's from e-mail address, whatever IP your computer is on in your office, I can make the originating IP that IP. Now, if I can become any IP in the world, how do you block or stop that? Now, luckily we don't do this as of yet; we stumbled on this by accident. But it's a matter of time before some other company realizes this as well. And not only can this technology be used for mail, credit cards, hacking, anything, if you can forge your originating IP you can't find that person.

Thank you, gentlemen, for your time.

[The prepared statement of Mr. Scelson follows:]

PREPARED STATEMENT OF RONALD SCELSON, PRESIDENT, MICROEVOLUTIONS.COM

To the Honorable Senator McCain and the Subcommittee on Commerce:

I am greatly honored to be invited to speak before this subcommittee today and would like to thank Senator McCain for inviting me.

As we have worked under the new CAN–SPAM Law a few issues have arisen.

**CAN–SPAM Can Work**

I would like to begin however by stating that there are a few reasons why the new CAN–SPAM Act is working and working well.

It is very promising to see our government working to do something about fraudulent activities on the Internet. It is very good to see companies that are identifying themselves. It has helped tremendously in the following areas:

- Repeat business and
- New business for the mailing companies.
- It has helped the recipients who are familiar with the law to identify U.S. companies working to be legitimate from non-compliant companies both abroad and in the US.
- Finally, it has helped those Internet Service Providers who do wish to work with mailing companies to know whom they can offer services to without violating any laws themselves.

**All New Things Have A Rough Time**

Despite all this good news, there are still many problems with implementation, cooperation, interpretation, and fraudulent or misleading practices—many stemming from the ISPs or their providers.

Following are some examples and issues that need to be looked at and resolved for the Internet community to work in harmony.

Since the enactment of the CAN–SPAM Act, my company and several others have all worked in compliance of the new law, which has been an extremely difficult task each day.

When we mail under the new law the major ISPs focus on our from addresses, subjects lines, our company information, and our disclaimers on the bottom of the e-mail as well as our IP address. They use this information to block our e-mails. Thus the Act that is to curtail fraud, is in fact curtailing our ability to engage in free enterprise and our business is greatly hindered.

With this situation, many mailers—especially in foreign countries still have not been able to fully implement all steps of the new law. They are faced with the problem of how to comply with the law when the ISPs and backbones themselves are not being respectful of the new law. Although it is clear that the CAN–SPAM law does not dive into the legalities or illegalities of the practices of ISPs, many mailing companies are still—simply put—backed into a corner. Shall they comply and go out of business due to ISP filtering or shall they attempt to comply partially, hoping that it will be clear that they have the intent to follow the law and remain out of trouble with the U.S. regulating bodies. This is the dilemma for many.

Of course foreign companies have mainly chosen to follow the laws of their land and disregard the laws of the United States—especially with the actions of the ISPs to put all bulk e-mail in the trash.

**Shut Down = Automatic Non-Compliance**

Every time a registrar shuts off a domain, an ISP closes a connection, or a hosting company shuts off or blocks an IP Address of a mailing company, there is a non-compliance issue. According to CAN–SPAM of 2003, all mailing companies are to keep their removal systems active for 30 days after the e-mail was sent. Every company including my own has had a major situation complying to this part of the law because ISPs, Registrars or hosting companies shut down the services without providing 30 day notice and keeping our connections active so that we can remain in compliance. Often we even lose our remove lists that were contained on the equipment that they now deny us access to.

**Block, Tackle and Throw**

Here is an example of what our company and many others have experienced.

AOL, Hotmail, Yahoo and other major carriers have blocked our network based on our company information. The larger anti-spam groups have done the same.

These anti-spam groups act like vigilantes now more than ever before. They put you on their blacklists—often networking these blacklists to other anti-spam groups as well. It is possible to have both your company name and IP addresses completely

blocked in as little as 4 hours, thus preventing you from delivering your mail to more than ½ the Internet. These groups will not remove the blacklist even if you prove to them that you are compliant with the new legislation. These organizations are not government backed or funded. They do not identify themselves like we do so pursuing legal action against them is nearly impossible. Many of these groups are not even on U.S. soil. These are the same people who want our information published on the web. Nothing is done to stop them or interfere with them.

The ultimate blow for the mailing company however is how many of these groups also use automated systems to generate multiple complaints to the Internet service providers. They make it look like one person received numerous copies of the advertisement, or like the mailing company has generated a large amount of complaints and thus should be shut down.

For the Backbones and the ISPs the issue has always been how to engage in business without generating too many complaints. Since, with most of these groups, the number of complaints is the determining factor on when to leave services on or when to shut them off, many of the vigilante groups now have set up anonymous and multiple complaint sending automated systems. In fact, you will find that very few of the complaints that are generated today come from the intended recipient of the e-mail as compared to the number that come from the automated anonymous complaint-sending systems. Interestingly, there are some vigilante groups that encourage people to purchase and use their software with proxies to prevent detection when sending in complaints!

In February of this year, the ISP I am currently with (WorldCom) received notice that I had joined AOL's whitelist and was mailing non-unsolicited e-mail and had AOL's full permission to send mail into their domain. This was not spam. Because AOL's automated remove system sent a copy of the undeliverable e-mails not only to us but also to WorldCom, WorldCom told us to stop mailing or they were going to shut us down. What was the logic in this action by WorldCom? AOL had granted us permission to mail into their domain. We were fully compliant with the law, and we were offering products and services that were a) in great demand and b) not fraudulent. And this was not even because of complaints. It was ONLY non-deliverable addresses in our list.

**What About That Common Carrier Law?**

When we review the FCC Communication Act, the above actions show that the ISPs are unjustly denying us service. In many cases, these groups are in fact common carriers providing us nothing more than a way to connect to the Information Highway. WorldCom is in violation of the FCC Communication Act, which clearly states that common carriers cannot tamper with, read, or alter the communications that they transmit. This includes communications across data lines.

The issue of whether or not an ISP is a common carrier has been argued in the courts as far back as 1997. In one suit, AOL claimed that they were a common carrier, yet just a short while later they claimed that they were not a common carrier. The FCC supported AOL's claim that they were not common carriers and thus set a precedent that many ISPs have followed since. Interestingly, as we understand the charter of the FCC, they do not have the authority to determine who is or is not a common carrier. This is the job of Congress.

According to section 3 47 USC 153—Section Ten of this act: "Common Carrier: the term of a "common carrier" or "carrier" means any person engaged as a common carrier for hire in interstate or foreign communication by wire or radio or in interstate or foreign radio transmission of energy, except where reference is made to common carriers not subject to this act; the persons engaged in radio broadcasting shall not, insofar as such person is so engaged, be determined the common carrier." At the time of this submission, I have yet to locate any ISP not subject to this act.

I located more information on common carriers at a website that detailed a lawsuit against Western Union a while ago.

> "A 'common carrier' has a legislatively-granted monopoly over a particular route, region, or type of communications. In return, the carrier must carry everything and has no right to reject particular passengers or communications.
>
> "Congress made Western Union a common carrier, for example, when it refused to carry cables from reporters to their newspapers because they competed with its own news service.
>
> "It seems obvious that services which sell only a connection to the Internet should be treated as common carriers. While Compuserve and AOL should have a right to edit and refuse to carry speech they do not like, ISPs should have no more right to do so than Western Union or the phone companies."

Of course, this statement was made about AOL and Compuserve before they owned their own carrier lines. Thus it no longer holds true for these groups either.

**Let Them Be Removed**

The CAN–SPAM Act also calls for the FTC to implement the Global Remove System. Absence of this removal system has allowed problems with removal to persist; its implementation could result in a much calmer Internet environment much faster than anything else we have available to us today.

For example:

1. A recipient who wishes to receive no advertisements at all must remove himself from any advertisement that arrives in his inbox. This could quickly add up to a lot of extra work. With the Global Removal system, he would have to only remove himself once.
2. An Internet Service Provider continually gets complaints from the same person who enjoys sending such complaints and will not remove himself from a mailing list—the ISP can enter his e-mail address into the removal system, thus putting an end to the problem, while maintaining his privacy.
3. By giving the rights back to the individuals, there is no need for any ISP to subscribe to the vigilante groups that filter and file multiple reports anonymously.

Yet, many of the anti-spam groups are strongly opposed to such a system. There are reasons for this: Just as commercial bulk e-mail is big business, so is anti-spamming. With software and services to be sold to stop the flow of commercial e-mail, their sales would be interrupted if the public had an easy and effective way to remove themselves from receiving Internet e-mail advertisements.

Additionally, the anti-spammers claim that there are people who would mail to the remove list—I have never met one however. Yes, there is a solution to this problem if it did exist. When a recipient of an e-mail receives unwanted advertisements they click the remove link. This link takes them to a government site where they submit their e-mail address, which will be encrypted. Software would be available to the mailers for doing removes. The software would retrieve the remove list while encrypted and remove the people without the mailer ever seeing the actual e-mail address.

A program could be implemented where bulk mailers could sign up with the government and their IP address and Domains would be whitelisted with the ISPs allowing people who send compliant mail to get in while being able to stop spam.

**Above The Law?**

While we worked to get whitelisted with AOL, here is what we experienced:

> Things started out well, AOL was willing to work with us as we worked to deliver our list into their domain and get our non-deliverables removed. After just 3 mailings we were receiving virtually no undeliverable e-mails and very few complaints. The majority of this list was undeliverable mainly because the list had been built since I started mailing years ago. Obviously many e-mail addresses changed over the years. The only way to get the bad addresses out of the list was to deliver into AOL and pick up their non-deliverable reports back to us.
>
> WorldCom stepped in and tried to shut me down even after AOL sent proof of our whitelist classification. However, it seems that AOL found out who I was and denied me the whitelisting after this exchange of information between AOL and WorldCom. Charles Stiles, postmaster for AOL denied the whitelisting based on my list not being "true opt-in" and threatened to bring in their legal department. Yet, Opt-In had never been a part of the original whitelisting agreement with AOL.
>
> The problem I have with this is just last year Ted Leonsis with AOL stated in front of Congress that they send bulk e-mail but they provided a way for there receivers to opt-out, which of course I do too. I fail to see the difference.

While small companies are often thwarted in their attempts to follow the laws of the land and the rules of the ISP, which do not align at this time, they are hard-pressed to stay in business. Large corporations however, not only disregard the laws of the land as passed by Congress, they ignore rulings by judges.

Recently I hired an attorney to sue the large carrier Covista. This resulted in an injunction that demanded they turn my service back on. Covista just ignored it.

AOL was recently sent an order to allow CI host to send mail to AOL's network. AOL just like Covista is ignoring the judge's order.

Scott Richter of Opt-In Real Big has been involved in an ongoing legal battle to allow him to send compliant e-mail through his two providers. He too was awarded an injunction against one of his carriers. I do not know if his provider is abiding by the injunctions or not.

Evidence suggests that the ISPs think they are above the law and can sue us for failure to abide by the law while they simply ignore them.

All the large companies like AOL, Hotmail, Yahoo, MSN, Charter, and others are working together on an anti-spam system, while they continue to send e-mail advertisements. If bulk mailing is so bad and so wrong, why are they engaged in it?

Is it bad and wrong as they say or is it merely that we needed to curtail fraudulent practices? If the problem was that of fraudulent practices, then that problem was solved with the new law. Yet ISPs stop our compliant mailings while they mail themselves. Begins to look like small business against big business . . . It has long been said that the Internet is the first place where small business had the opportunity to play in the same field as big business . . . perhaps this is the threat?

President Bush is sending non opt-in bulk e-mail, abiding by the new laws, into Hotmail and AOL. His message ended up in the bulk folder at Hotmail and the spam folder at AOL. In my mind, a message from the President should be given a level of courtesy and respect in keeping with his position. Apparently, AOL and Hotmail do not hold the same respect.

**Bonds Do Not Solve Any Problems**

A new trend is popping up for companies like Hotmail and Yahoo. They are contracting with third party companies such as Habius, and Bonded Sender. These third party companies are charging as much as 25,000.00 a year, non refundable to bond your IP addresses. However, there is no guarantee other than to take your money with only the possibility of allowing your mail in.

It seems no different than paying the mafia for protection to do legitimate business (legal definition of racketeering and fraud).

**Truth In Reporting—Truth In Delivering**

Although we have a law against fraudulent practices on the Internet, it seems, that this law is not written well enough to include those who are using automated systems to identify, and file multiple complaints anonymously (often with proxies) against people who are sending e-mail. Also, with ISPs any complaint is taken as a good reason to shut down services. Following are some recommendations of what could be done.

1. Complaints should be limited to being classified as valid only if they come directly from the intended recipients.
2. Automated reporting systems should be limited to one complaint and not sent with the use of proxies. Complaining Agency should be clearly identified.
3. ISPs and their providers should show respect toward the CAN–SPAM law by only classifying as a valid complaint those which do not comply with the law.
4. Those Agencies or individuals doing the complaining or with any kind of ability to interfere with legal mail should have to fully identify themselves just like we have to identify ourselves. Appropriate e-mail address should be provided for removal.
5. ISPs should not be allowed to filter what is required by law to be in our e-mail advertisements.
6. ISP's should not be allowed to shut our circuits down and discriminate against us when we send legal mail.

**Summary**

*The CAN–SPAM Act of 2003 has brought promise and hope to the Internet, yet adjustments still need to be made:*

1. Rapid implementation of a Global removes system, which ISPs are required to add chronic complainers to.
2. ISPs to be treated as common carriers or minimally respect the laws that Congress has passed.
3. Companies interfering with these laws like Spews, Spam Cop etc. should be made to file only one complaint and reveal their identity.
4. People complaining should have to identify themselves (e-mail address).
5. Mailing companies who comply with the law should not be at risk of losing their systems or services. They should not be forced into non-compliance due to instant shutdowns, and violation of 30-day remove systems.

The CHAIRMAN. As always, very interesting.

Mr. SCELSON. Sorry I rushed through.

The CHAIRMAN. Can you tell us what has happened to you since you testified before this committee?

Mr. SCELSON. Well, so far the only carrier that has been at all willing to work with people until they found out who I was, was AOL. I give them full credit there. As of right now, unfortunately for the first time ever, Hot Mail MSN's filters appear to be a whole lot better than AOL's, and this is a first ever. Once AOL realized who I was is when they sent me to this postmaster that's like, oh well, you are a spammer, you can't use us. I'm mailing legal now; that's the reason the law got passed, so I wouldn't have to spam.

The CHAIRMAN. What has happened to you since you appeared here last? You changed your address.

Mr. SCELSON. Yes sir. Not too long after the reporters and incidents like, you know, dealing with the press and all, someone went to my house, set a doll out on my front door, said this would be my children if you don't quit spamming. So basically what I did was, the government has—I'm sure you're familiar with, in Conroy, Texas—an underground fallout shelter there that we just recently leased and turned into an ISP. We can run up to 4 years on generator power. It's pretty much undefeatable, we have five gigabite fiber connections there. Eventually where I'm going with my company is, we'll be out of the e-mail business and people that want to also secure servers and things will be delivered and safe underneath the ground. And we're safe under there as far as anyone threatening us or doing harm to us.

The CHAIRMAN. Mr. Leonsis, as usual, this is your turn to respond to—and if you'd mention the issue of the injunctions as well.

Mr. LEONSIS. There are no injunctions against us. He's misinformed. I enjoy the theater, I admire your patience. We would put him on the white list. We have thousands of companies on our white list. He was on our white list; he mailed his mail, got 137 times the complainant standard than our typical white mail mailers. So we said, obviously there's something you're doing that isn't meeting the standard of our community so just work with our postmaster. And this is a much bigger issue than Ronnie's beef with our postmaster; this is about the quality of life.

The CHAIRMAN. Could I interrupt. Your previous answer—my staff hands me a news article from April 23, says CI Host, one of the world leader's—web hosting and Internet system was awarded temporary restraining order against America On Line to keep it from illegally blocking all e-mail from CI Host IP addresses to AOL subscribers.

Mr. LEONSIS. April 23 of this year or last year, sir?

The CHAIRMAN. April 23, 2004.

Mr. LEONSIS. Well, I've been given a note from our staff that there are no active injunctions against us to actively deliver the mail. We've complied with all of the court orders.

The CHAIRMAN. All right. I think that's important for the record. Thank you.

Mr. SCELSON. And you see where I've got this information from was a straight—normal, everyday newspaper.

Mr. LEONSIS. And we know the newspapers never misinform, either.

The CHAIRMAN. Please proceed, Mr. Leonsis.

Mr. LEONSIS. So, CAN–SPAM Act was terrific. And as we talked about a year ago that it really is to work in conjunction what the technology providers would do in the ISPs. And we've looked at the CAN–SPAM Act as kind of being a baseline. And there were places above that baseline where carriers such as ourselves will be very, very aggressive and our white lists work. And our spam complaints are down; our mail being delivered into our mail boxes is down. We feel we are making progress. And I'm not sure what all the points Ronnie is trying to make; we would like for him to be on our white lists. We don't consider him the worst of the bad actors; we are more concerned with the bad actors.

Mr. SCELSON. Like I say, when I did mail there, we started out with 98 million in the database that goes all the way back from when I first started mailing. From 98 million to 27 million in three mailings is a significantly high number. I don't deny that one bit. But AOL's white list is supposed to give you 30 days to get your list straight, and in three mailings we went from 98 to 27 million. That is a significant——

Mr. LEONSIS. What he is referring to, Senator, is that our basis is that if you have a relationship with a recipient that you should be able to do business with them. So when someone comes to us and says, "We have a relationship here. We should be allowed to mail," we believe them. When 40 percent of the mail is undeliverable, I would submit if you had a database of Christmas card respondents of your good friends and 40 percent came back, you would have to say they're not your friends. And so, that's what we're dealing with here.

The CHAIRMAN. Mr. Guest, do you have a comment on this exchange? From the consumer's standpoint?

Mr. GUEST. Well my comment, listening to all the back and forth and the different ways that people might be able to filter out some of the spam messages and let other unsolicited e-mail go through, is to step back and say, "That's not what consumers are looking for." Consumers are looking for the ability to just simply no longer get unsolicited commercial e-mail. And so, you know, kind of rather than haggling about the details, that's why we recommend an opt-in policy or ways I've said before, as we can do with faxes and we can do with phone calls and things like that by taking one action, we can block it all. And that's really, from a consumer point of view, the bottom line.

The CHAIRMAN. Go ahead, Mr. Akamine.

Mr. AKAMINE. You can see from this conversation that this kind of discussion of "I'm a spammer" or "You're a spammer" could go on for days. But if I can take kind of the technological viewpoint and kind of break the discourse here. The way that Postini offers a solution to this kind of problem—whether somebody should be on the white list or not—is we actually give the power to the recipient. So we have maybe five or six million end users on our system and those end users can set their own spam filters. So if a person is a civil libertarian and wants to see everything, they can turn their spam filters completely off, regardless of what the ISP setting is.

On the other hand, if you happen to be working for a law firm like Baker McKenzie, and your client is a real estate company, you might want to turn your mortgage spam filter so you can be reading e-mails about mortgage, but turn your sexual filters all the way up so you don't get objectionable sexual filters. Once you give the power, the technological power, to the end user like that, you don't have the discussion between somebody who claims they're a spammer and the administrator of the mail system trying to keep white lists updated. So, this is the kind of example of working, real world private solutions that are in place today.

The CHAIRMAN. Mr. Brondmo.

Mr. BRONDMO. Just building on those comments for a moment. There's no filter that works today. A filter, however good your technologists are, a filter is still guessing. It's making an educated guess and those guesses are getting increasingly good. And when I hear numbers like 90 to 99 percent, those are impressive numbers but even 99 percent of billions and billions of messages lets a lot through. And occasionally the filters guess wrong and they put an important mail in your in-box—that should have gotten into your in-box into the bit bucket. There was some recent research by Good Mail Systems that indicated that 68 percent of all e-mail users have seen a drop-off in e-mail, legitimate e-mail, e-mail they wanted, because of spam filters, of which 50 percent were personal e-mail. So the point being, what we need to do is we need to fix the infrastructure. We need to make changes so that when I get an e-mail from Scelson, I know who he is, I can turn it on or I can turn it off. AOL can do that for me at their gateway, at their filters, or I can do it on my desktop. But the choice has to be with the consumer. A "do not e-mail" list is not a good idea because guys like Scelson will not honor that list, a lot of people out there will not, and the ones who do will have increasing problems with getting their mail through in legitimate fashion.

The CHAIRMAN. I'd like to just have the panel, beginning with you, Mr. Brondmo, discuss very briefly, the severity of the problem of wireless spam and how we're going to confront that issue.

Mr. BRONDMO. Well, very briefly on wireless, the wireless network itself is a closed network. So the devices themselves cannot receive spam unless you get the gateway, say the e-mail gateway, into that network. Once it's in the network it can be controlled, not unlike the AOL network where internally at AOL they can control the network, but it's when they open it up to the broader Internet they have a problem. Again I get back to my core thesis—authentication is the answer. If we can authenticate and if we can build histories—if I need a persistent identity in order to send mail and if I have a history of behavior, then I can basically make decisions at the gateway, when I make the handshake to the incoming server. Do I trust you or do I not? And based on that I can determine whether to make the bridge. It's not very different from the e-mail problem.

The CHAIRMAN. Mr. Akamine.

Mr. AKAMINE. Specifically to your question about wireless devices, everything that we're seeing today in spam at your desktop will also happen at the wireless devices. I mean, that's what makes them useful. So, there is no Blackberry device out there that's

closed to itself, or if I have a cell phone that has an SMS message system. They all have gateways to the Internet and to SMTP e-mail; that's what makes them useful. Therefore, all the kind of content abuses, as well as Directory Harvest Attacks and all the transport abuses will also occur.

The CHAIRMAN. So it's just a matter of time.

Mr. AKAMINE. Well, unless the system operators basically start to protect their mail systems. And again, it's not about protecting the end hand devices; it's not about putting a little piece of software there, it's actually about securing the system at the core.

Mr. LEONSIS. I think it'll be less aggressive on wireless, less graphics. Usage in the handset is, you know, the footprint is smaller. With AOL, if you're an AOL member, its mail is mail. And so we won't have that issue. And I think I'm more optimistic, I think there are more companies, the authentication movement in technologies will be helpful and I think that we have the willpower and the dollars to invest and that we will make progress. We'll come here a year from now and it will be better, not worse.

Mr. AKAMINE. Senator McCain, I just want to make one point of fact here.

The CHAIRMAN. Yes.

Mr. AKAMINE. We do have one antecedent that we can point to, which is in Japan, the largest Internet service provider is actually a wireless provider called NTT DoCoMo. They have something on the order of 50 million wireless cell phones that are all Internet-enabled. They approached us a couple of years ago and told us that in that period of time they were getting one billion e-mail connections today to their wireless users, just to deliver 5 percent of those to be legitimate messages. So when I say that I'm concerned about all of the current e-mail abuses occurring to wireless, we have one model in Japan that already has gone that way.

The CHAIRMAN. Mr. Guest.

Mr. GUEST. *Wireless Week,* just this week, has a survey which says, and I'm quoting, "Adult content for wireless devices is a billions of dollars business in Europe and Asia," close quote. And they pose the question, who should be the gatekeeper when it comes to the United States? We know that it's coming; I don't have a solution to propose today but it is certainly something, clearly you're aware of, Mr. Chairman, and the Committee is aware of, that you're going to have to pursue along with the other problems that spam is still going up.

The CHAIRMAN. Mr. Scelson.

Mr. SCELSON. Mr. Postini—how do you pronounce it?

Mr. AKAMINE. Akamine from Postini.

Mr. SCELSON. Postini. Remember last year when I was in here I was telling you gentlemen that as long as ISPs are reading and filtering peoples' mail, it's taking away from the user? And the only filter that will ever work and ever have any fighting chance is a filter that each user controls their own filters; there's no reason for ISPs to filter this. So the system that he's working on, if any system has a chance as far as that filtering method, his is the best one. I don't see where ISP should decide who's going to get what mail. Just recently Google and the government had a little battle over what information Google was taking from people in order to

advertise to these people. Well, a spam filter reads your mail without your permission to decide what you're going to get. It's no different than what Google's proposing. But the government's coming down on Google. It's the same thing.

As far as the wireless industry of it, personally I can see it being a total nuisance going down the store and having a pager or something go off. As much as I believe in advertising and marketing, as far as the cell phones, that is one that should be just straight illegal, you cannot advertise on it. And it's just because of the nuisance, everywhere, no matter where you're at, even driving down the road, it can cause accidents, people thinking it's something important. So I'm in agreement that something should be done before it even gets here.

The CHAIRMAN. Well, Mr. Scelson, I had heard because of your appearance before this committee that it had caused you some serious problems and I want to apologize for that. And I thank you for coming back and I hope that your future is bright and that you will not suffer any repercussions because of your willingness to come forward and help us with the information that's vitally necessary if we're going make proper decisions. So again, please accept my apologies on behalf of the Committee for anything that happened to you as a result of your testimony before this committee.

Mr. SCELSON. Thank you, Senator McCain.

The CHAIRMAN. I want to thank the witnesses and I'll turn to Senator Burns but it seems to me that in a couple or 3 months, Senator Burns, we better have another hearing since this thing is evolving in a rather rapid fashion.

Senator BURNS. Well, it is, and we thought it would because any time that you—there is cause and effect, as you well know, around here, and for every action there's an opposite and equal reaction to it. So that should not surprise anybody. I'm a great admirer of Mr. Scelson for the simple reason I don't think he has to build anymore bomb shelters or do anything; I think the FBI ought to hire him. I think your employment is—or I think maybe Ted will hire him.

Mr. LEONSIS. We're fully staffed right now.

[Laughter.]

Senator BURNS. So, I think, you know, your employment is secure for the rest of your life, as a young man, I can see that. I have no questions other than the fact that I just take all the information that I've heard here; I think the Chairman asked all the right questions. And are you going to shut this thing down or am I going to shut this thing down? Sounds like I'm going to shut.

Thank you all for coming today. If we have questions from other members of this committee, please respond to them and the Committee. And thank you for coming. We're adjourned.

[Whereupon, at 12:05 p.m., the hearing was adjourned.]

○

This page intentionally left blank.