S. HRG. 107–1135

SPAMMING

HEARING

BEFORE THE

SUBCOMMITTEE ON COMMUNICATIONS

OF THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION UNITED STATES SENATE

ONE HUNDRED SEVENTH CONGRESS

FIRST SESSION

APRIL 26, 2001

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

U.S. GOVERNMENT PRINTING OFFICE

88–536 PDF WASHINGTON : 2006

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED SEVENTH CONGRESS

FIRST SESSION

JOHN MCCAIN, Arizona, *Chairman*

TED STEVENS, Alaska	ERNEST F. HOLLINGS, South Carolina
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 SMITH, Oregon	RON WYDEN, Oregon
PETER G. FITZGERALD, Illinois	MAX CLELAND, Georgia
JOHN ENSIGN, Nevada	BARBARA BOXER, California
GEORGE ALLEN, Virginia	JOHN EDWARDS, North Carolina
	JEAN CARNAHAN, Missouri

MARK BUSE, *Republican Staff Director*
MARTHA P. ALLBRIGHT, *Republican General Counsel*
KEVIN D. KAYES, *Democratic Staff Director*
MOSES BOYD, *Democratic Chief Counsel*

SUBCOMMITTEE ON COMMUNICATIONS

CONRAD BURNS, Montana, *Chairman*

TED STEVENS, Alaska	ERNEST F. HOLLINGS, South Carolina
TRENT LOTT, Mississippi	DANIEL K. INOUYE, Hawaii
KAY BAILEY HUTCHISON, Texas	JOHN F. KERRY, Massachusetts
OLYMPIA J. SNOWE, Maine	JOHN B. BREAUX, Louisiana
SAM BROWNBACK, Kansas	JOHN D. ROCKEFELLER IV, West Virginia
GORDON SMITH, Oregon	BYRON L. DORGAN, North Dakota
PETER G. FITZGERALD, Illinois	RON WYDEN, Oregon
JOHN ENSIGN, Nevada	MAX CLELAND, Georgia
GEORGE ALLEN, Virginia	BARBARA BOXER, California
	JOHN EDWARDS, North Carolina

CONTENTS

WITNESSES

APPENDIX

SPAMMING

THURSDAY, APRIL 26, 2001

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

The Subcommittee met, pursuant to notice, at 2:35 p.m. in room SR–253, Russell Senate Office Building, Hon. Conrad Burns, Chairman of the Subcommittee, presiding.

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

Senator BURNS. We've got a Congressman on his way, but I'm going to open these hearings this morning, or this afternoon on the CAN-spam bill. We welcome everyone today to this hearing, which concerns a matter I think of critical importance to the future development of commerce on the Internet. How to control the explosion of unsolicited e-mail, or commerce mail known around the industry as spam. Specifically, we here are here to address the CAN-spam bill that Senator Wyden and I have introduced. Senator Allard of Colorado is also a co-sponsor of this bill and I thank him for his support.

The CAN-spam bill would require e-mail marketers and spammers to comply with a straightforward set of workable common-sense rules designed to give consumers more control over spam e-mail. Specifically, it would require a sender of marketing e-mail to include a working return address so that the recipient can send a reply e-mail demanding not to receive any more messages. The marketer would be prohibited from sending further messages to that consumer who had informed them they wanted it to stop. Further, the bill would also prevent e-mail marketers from using deceptive headers or subject lines so the consumers will be able to tell who initiated the solicitation.

The bill includes strong enforcement provisions to ensure compliance. The Federal Trade Commission would have the authority to impose steep civil fines up to $500,000 on spammers. This fine would be tripled if the violation is found to be intentional. In short, this bill provides broad consumer protection against bad actors while still allowing Internet advertisers a justified means of flourishing.

Senator Wyden and I have taken great care to make sure that this bill does not harm legitimate advertising. In fact, we are trying to help the Internet advertiser by allowing them to reach people who want to learn more about their product. If I open up my e-mail

and find 100 messages, and they're all advertisers, chances are I'll never read one of them. However, if I have 10 that I want to receive their mail, advertisers, they might find a sale there. This is how a legitimate system should and would operate under the CAN-spam bill.

Spamming is really a problem. And I believe it's absolutely critical that we address it now so that the Internet is allowed to reach it's full potential. Because of the vast distances in my home state of Montana, many of my constituents are forced to pay long distance charges for their time on the Internet. Spam makes it nearly impossible for these people to enjoy the experience, and it makes it even harder for them to see how this will help rural America flourish in the 21st Century.

Also, Internet service providers are bombarded with spam that often corrupts and shuts down their systems. In today's information age, where beating a competitor to the next sale is absolutely critical to survival, these shutdowns can cause real economic damage. We may be in a down-turned American economy, and especially in the high-tech sector, we're going through a little shake-out and nobody has to read a newspaper to find that out. But the efficiencies created through the vast information-sharing are here to stay and will help propel our economy to levels beyond our imagination. But in order to reach its potential, we must eliminate the bad actors and those who threaten these efficiencies.

I had initially hoped that the technology would solve the problem that it created. However, for every filter, there is a quick response by spammers to beat the filter. Where have I heard that argument before? I think we were talking about schools and libraries at one time and the use of filters. And this is—and we're finding out that it doesn't take much, just the change of a numerical, a number or a letter, and you're around the filter. It seems like a big game to them, and to us it's a bad game.

I just recently read, and I would have most of you pick up a Monday, last Monday's Wall Street Journal which had a big article in the journal that says "You've Got Mail". And in parenthesis, you don't want. So I think it's a very creative article, probably laying out the problems and the challenges that we face on spamming. Spammers—ISP's who incorporate more sophisticated filtering to catch such alterations find that spammers will include 1–800 numbers as graphic files imbedded in an ordinary text message. Such telephone numbers would display normally in ordinary e-mail, but because they were encoded in the graphics format instead of in ordinary text, Internet filters would miss them entirely.

I find the analysis of the anti-spamming activist quoted in the article quite instructive. They felt that "the technical methods that have just given rise to an arms race situation, where each improvement of the technical means for blocking spam, just drives the creation of new spam means of getting spam past the block. It will only be stopped by legislative solutions. When it becomes too much of a financial risk for not enough benefit, the spammers will go away, and not before."

And I couldn't agree more. The CAN-spam bill will provide spammers with the only kind of incentives to get out of the busi-

ness, and they understand stopping it and stop invading on the privacy of consumers.

I look forward to hearing from the witnesses today, and I call them to the table at this time. We have Ms. Eileen Harrington, Associate Director of Marketing Practices, Bureau of Consumer Protection, Federal Trade Commission here in Washington, DC. Ms. Harrington, thank you for taking time out of your busy schedule and coming to testify before this Committee today. We look forward to your remarks.

STATEMENT OF EILEEN HARRINGTON, ASSOCIATE DIRECTOR OF MARKETING PRACTICES, BUREAU OF CONSUMER PROTECTION, FEDERAL TRADE COMMISSION

Ms. HARRINGTON. Thank you very much, Mr. Chairman. As you said, I am Eileen Harrington of the Federal Trade Commission's Bureau of Consumer Protection. The Commission is very pleased to be asked to present its views today and has submitted its testimony to the staff for the record. I will be, of course, happy to answer any questions that you may have, and the answers will be my own views and not necessarily those of the Commission.

The low cost of sending UCE or spam differentiates it from other forms of unsolicited marketing such as direct mail or outbound telemarketing.

Those marketing techniques, unlike spam, impose costs on senders that may serve to limit their use. There are no comparable limits on spam, however. Nevertheless, well-known manufacturers and sellers of consumer good and services, generally do not send spam. Rather, these merchants use requested about available products, services and sales.

For example, consumers may agree in advance to receive information about newly published books on subjects that interest them, or weekly e-mails from airlines advising them of discounted air fares, giving consumers the ability to choose the information they receive over the Internet. Known in the industry now as permission-based marketing, it is likely to create more confidence in its content and in the sender.

This permission-based approach is the model mandated by S. 630. Not all UCE is fraudulent. Fraud operators, however, are always among the first to exploit any technological innovation, and it is no surprise therefore, that they have seized on the Internet's capacity to reach literally millions of consumers quickly and at a low cost through spam.

Not only are fraud operators able to reach millions of individuals with one message, but they can misuse the technology to conceal their identity.

Many spam messages contain false information about the sender and where the message was routed from. This makes it nearly impossible to trace the spam back to the actual sender. In the same vein, spam often contains misleading subject lines and extravagant earnings or performance claims about goods and services. These types of claims are the stock in trade of fraudulent schemes.

The Commission has conducted a vigorous law enforcement program against fraudulent or deceptive spam. At least thirty of the 173 cases the Commission has brought to date against fraud on the

Internet, have targeted fraudulent operations that used spam as an essential integral part of their scheme.

The Commission has also conducted an educational program to alert consumers and businesses about the dangers of spam. It has published nine consumer publications that relate to spam and more than 1.6 million of those documents have been distributed to consumers either through paper copies or via access to the FTC's website.

I would add the Commission is also probably the only organization in the country that has invited consumers to send us their spam. We operate a special spam mailbox, UCE@FTC.gov and to date we've received over 8 million pieces of unwanted spam from consumers. The Commission supports the goals of S. 630 which are to help control the additional costs and other potential negative effects that spam can impose, both on Internet service providers and Internet users and to strengthen consumer choice in the matter of whether to receive spam.

S. 630 addresses two basic problems that together pose a real threat to consumers' confidence in the Internet as a medium for personal electronic commerce. First, there is the problem of fraudulent or deceptive spam. This is addressed by the prohibitions in S. 630 against false or misleading header information or subject headers. The Commission welcomes these proposals as potential enhancements to its existing authority under the Federal Trade Commission Act.

The second serious problem addressed by S. 630 is the stress on the Internet infrastructure resulting from the sheer volume of spam. Spam, even if not deceptive, may lead to disruptions and inefficiencies in Internet services and constitutes a great nuisance to consumers and businesses using the Internet. This aspect of the problem is addressed by the bill's opt-out provisions. S. 630 would require commercial e-mail messages to contain an opt-out notice and a functioning return e-mail address for sending an opt-out request.

Further, S. 630 would prohibit sending any spam after a recipient has opted out. These provisions are a big step in the right direction to stem the tide of spam by giving consumers more control over which commercial e-mail messages they receive.

Now there are several issues raised by S. 630 that I want to mention for your consideration. First, a key term used throughout S. 630 is commercial electronic mail message. This term is defined in section 3 of the bill. The relevant portion of the definition provides that an electronic mail message shall not be considered to be a commercial electronic mail message solely because such message includes a reference or link to an Internet website operated for a commercial purpose.

However, in our experience much spam, particularly spam related to pornographic websites consists of nothing more than such a reference or link. The definition as currently drafted could potentially be exploited by senders of such spam to evade the requirements of this bill.

A second concern, the language in section 5 of the bill that prohibits header information that is not legitimately obtained, is ambiguous. To ensure that this language does not create enforcement

problems or engender unintended lawsuits, clarification is essential.

The third concern that we want to raise concerns the provision in S. 630 prohibiting deceptive subject lines. This provision raises an issue about the Federal Trade Commission's authority to challenge deception under the Federal Trade Commission Act. Currently, under the FTC Act, the Commission could challenge a materially false or misleading subject line in a commercial e-mail message by using section 5 of the FTC Act.

And the Commission could use that section of the FTC Act to challenge this type of false or misleading representation or any other false or misleading representation.

The applicable legal standard that the FTC must meet under this provision of the FTC Act to demonstrate a deceptive practice is that it is likely to mislead consumers acting reasonably under the circumstances about a material fact. S. 630 would establish a higher standard applicable to subject lines in commercial e-mail messeges. It would require a showing that the person who sent the e-mail had knowledge that the subject line was likely to mislead the recipient about a material fact regarding the contents or subject matter of the message.

This knowledge requirement, not an element of deception under well-established law under the FTC Act, would make it more difficult for the FTC to take action under S. 630 against materially false and misleading subject lines.

As a matter of policy and fairness in enforcement, deceptive spam should not be treated differently from other deceptive marketing material. Moreover, the requirement of a showing that the subject line was likely to mislead the recipient and not reasonable consumer could increase the burden on the Commission to enforce this part of S. 630.

This may require a showing that each individual recipient was likely to be misled, which is a very difficult burden to meet especially where millions and millions of consumers have received one particular message. Imagine proving that each one of them was likely to be misled.

Because violators of section 5 of S. 630 would be exposed to liability for civil penalties of up to $11,000 per violation, it may be appropriate to adopt stringent standards for liability in S. 630 as a safeguard against penalties for what could be mere technical violations of the bill. However, the Commission recommends clarifying that S. 630 does not affect the FTC's current ability to bring enforcement actions targeting materially false or deceptive representations in commercial e-mail messages under the FTC Act, pursuant to the criteria of and seeking the remedies currently available under that Act. This could be accomplished by broadening the savings clause in section 7a of the bill.

Additionally, section 7 of S. 630 appears to preclude enforcement of most existing federal civil laws that apply to commercial electronic mail such as the FTC Act's broad prohibition of deceptive advertising, except to the extent specifically provided in S. 630. We believe that S. 630 should not supplant other relevant federal law and we recommend expanding the savings clause to make this point clear.

Before concluding, I do want to note that the enforcement scheme laid out by S. 630 and which you describe, Mr. Chairman, in your opening statement is modeled on similar schemes Congress established for enforcement for the Commission's 900 number rule and the telemarketing sales rule in the statutes that mandated promulgation of those rules.

The Commission's efforts would be supplemented with those of the state attorneys general and possibly by other federal agencies with jurisdiction in areas where the FTC has none.

This type of dual federal/state enforcement scheme has proved extremely successful in the past, particularly in challenging deceptive and abusive telemarketing practices and the Commission would expect it to work equally well in this context.

[The prepared statement of Ms. Harrington follows:]

PREPARED STATEMENT OF EILEEN HARRINGTON, ASSOCIATE DIRECTOR OF MARKETING PRACTICES, BUREAU OF CONSUMER PROTECTION, FEDERAL TRADE COMMISSION

Mr. Chairman, I am Eileen Harrington of the Federal Trade Commission's Bureau of Consumer Protection. The Federal Trade Commission is pleased to provide testimony today on the subject of unsolicited commercial e-mail, the consumer protection issues raised by its widespread use, the FTC's program to combat deceptive and fraudulent unsolicited commercial e-mail, and the FTC's views on the "Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2001" (S. 630), which Chairman Burns has proposed.[1]

I. Introduction and Background

A. FTC Law Enforcement Authority

As the Federal Government's principal consumer protection agency, the FTC's mission is to promote the efficient functioning of the marketplace by taking action against unfair or deceptive acts or practices, and increasing consumer choice by promoting vigorous competition. To fulfill this mission, the Commission enforces the Federal Trade Commission Act, which prohibits unfair methods of competition and unfair or deceptive acts or practices in or affecting commerce.[2] The Commission's responsibilities are far-reaching. With certain exceptions, this statute provides the Commission with broad law enforcement authority over virtually every sector of our economy.[3] Commerce on the Internet, including unsolicited commercial electronic mail, falls within the scope of this statutory mandate.

B. Concerns About Unsolicited Commercial E-mail

Unsolicited commercial e-mail—"UCE," or "spam," in the online vernacular—is any commercial electronic mail message sent, often in bulk, to a consumer without the consumer's prior request or consent. The very low cost of sending UCE differentiates it from other forms of unsolicited marketing, such as direct mail or out-bound telemarketing. Those marketing techniques, unlike UCE, impose costs on senders that may serve to limit their use.

Generally, well-known manufacturers and sellers of consumer goods and services do not send UCE. Rather, such merchants use **solicited** e-mail to give consumers information that they have requested about available products, services, and sales. For example, consumers may agree in advance to receive information about newly-published books on subjects of interest, online catalogues for products or services frequently purchased, or weekly e-mails about discounted airfares.

These examples of bulk commercial e-mail sent at the consumer's request demonstrate the value of consumer sovereignty to the growth of Internet commerce. Giving consumers the ability to *choose* the information they receive over the Internet—known in the industry now as "permission-based" marketing—seems likely to create more confidence in its content and in the sender.

By no means is all UCE fraudulent, but fraud operators, who are often among the first to exploit any technological innovation, have seized on the Internet's capacity to reach literally millions of consumers quickly and at a low cost through UCE. Not only are fraud operators able to reach millions of individuals with one message, but they can misuse the technology to conceal their identity. Many spam messages contain false information about the sender and where the message was routed from, making it nearly impossible to trace the UCE back to the actual sender. In the same

vein, UCE messages also often contain misleading subject lines and extravagant earnings or performance claims about goods and services. These types of claims are the stock in trade of fraudulent schemes.

Bulk UCE burdens (indeed, sometimes cripples) Internet service providers and frustrates their customers. The FTC's main concern with UCE, however, is its widespread use to disseminate false and misleading claims about products and services. The Commission believes the proliferation of deceptive bulk UCE on the Internet poses a threat to consumer confidence in online commerce and thus views the problem of deception as a significant issue in the debate over UCE.

II. The Federal Trade Commission's Approach to Fraud on the Internet

In 1994, the Commission filed its first enforcement action against deception on the Internet, making it the first federal enforcement agency to take such an action.[4] Since that time, the Commission has brought 173 law enforcement actions against more than 575 defendants to halt online deception and fraud. The pace of our Internet law enforcement has been increasing, in step with the growth of commerce—and fraud—on the Internet; over two-thirds of the FTC's Internet-related actions have been filed since the beginning of 1999.

The Commission brings to the Internet a long history of promoting competition and protecting consumers in other once-new marketing media. Recent innovations have included 900-number technology and telemarketing. The development of each of these advances in the marketplace was characterized by early attempts of fraud artists who sought to capitalize on the new way of doing business. In each instance, the Commission used its statutory authority under Section 5 of the FTC Act to bring tough law enforcement actions to halt specific deceptive or unfair practices, and establish principles for non-deceptive marketing.[5] In some instances, most notably national advertising, industry took an aggressive and strong self-regulatory stance that resulted in dramatic improvements in advertising and marketing practices.[6]

In other instances, at the direction of Congress or on its own initiative, the Commission has issued trade regulation rules to establish a bright line between legitimate and deceptive conduct.[7]

III. The Commission's Approach to Unsolicited Commercial E-mail

A. Monitoring the Problem

The Federal Trade Commission closely monitors the development of commerce on the Internet. Since the inception of the Internet as a commercial medium, the Commission has conducted a series of hearings and public workshops so that it could have the benefit of views from a wide range of stakeholders.[8] In June 1997, at a workshop devoted to issues of privacy on the Internet, the Commission heard discussion of three distinct UCE problems: (1) deception in UCE content; (2) economic and technological burdens on the Internet and delivery networks caused by the large volume of UCE being sent; and (3) costs and frustrations imposed on consumers by their receipt of large amounts of UCE.

While the Commission has maintained a focus on deception perpetuated through UCE, industry and advocacy groups that participated in the privacy workshop directed their attention to the economic and technological burdens caused by UCE. Under the leadership of the Center for Democracy in Technology, these groups spent a year studying the problem and identifying possible solutions, and in July 1998 issued their "Report to the Federal Trade Commission of the Ad-Hoc Working Group on Unsolicited Commercial E-Mail."[9] This report recommended the pursuit of technologies and public policies that would provide consumers with more control over the UCE they receive. Specifically, the report:

- urged marketers to give consumers a choice to "opt-in" or "opt-out" of receiving a UCE solicitation; and
- urged law enforcement to continue to attack fraudulent UCE solicitations, including those with deceptive "header" information.[10]

On another front, in 1998 the FTC set up a special electronic mailbox reserved for UCE in order to assess, first hand, emerging trends and developments. With the assistance of Internet service providers, privacy advocates, and other law enforcers, staff publicized the Commission's UCE mailbox, "uce@ftc.gov," and invited consumers and Internet service providers to forward their UCE to it. The Commission also created a database in which all of the forwarded UCE messages are stored. Over 8,300,000 pieces of UCE have been forwarded to the Commission since January 1998, and the UCE mailbox receives an average of 10,000 new pieces of UCE every day, 7 days a week. UCE received and entered in the database within the preceding 6 months is searchable. Periodically, staff has used the data to supplement

law enforcement and consumer and business education efforts. Commission staff has recently made arrangements to purchase new indexing software that will allow staff to conduct much more sophisticated searches as well as manipulate the data to determine trends and patterns in the UCE received.

B. Aggressive Law Enforcement

The Commission has responded to fraudulent UCE with a vigorous law enforcement program. To date, about 30 of the Commission's Internet cases have targeted scams in which spam was an essential, integral element. Most of these cases have been Section 13(b) actions in federal district court. For example, in May 1999, the Commission filed *FTC* v. *Benoit*.[11] This scheme used the ruse of a spam notification about charges purportedly to be billed to consumers' credit card accounts to lure the consumers into calling an expensive international telephone number.[12] The initial spam message purported to inform consumers that their "orders had been received and processed" and that their credit card accounts would be billed for charges ranging from $250 to $899. In fact, the consumers had not ordered anything. The spam advised recipients to call a specified telephone number in area code 767 with any questions about the "order" or to speak to a "representative." Many consumers were unaware that area code 767 is in a foreign country—Dominica, West Indies. But because Dominica is included within the North American Numbering Plan,[13] it was not necessary to dial 011 or any country code to make the calls.

Consumers who called to prevent charges to their credit cards, expecting to speak to a "representative" about the erroneous "order," were connected to an adult entertainment "audiotext" service.[14] Later, these consumers received charges on their monthly telephone bills for the international long-distance call to Dominica, West Indies. The defendants shared in the revenue received by a foreign telephone company for the costly international calls. The defendants hid their tracks by using forged headers in the spam they used to make initial contact with consumers.

The final stipulated order that resolved this case includes a provision specifically prohibiting the defendants from sending or causing to be sent any e-mail (including unsolicited commercial e-mail) that misrepresents the identity of the sender of the e-mail or the subject of the e-mail. The Order thus bans the defendants from falsifying information in the "from" and "subject" lines of e-mails, as well as in the text of the message.

Another recent case, *FTC* v. *Martinelli,*[15] targeted an alleged pyramid scheme that centered on spam. The defendants in that case ran an operation called DP Marketing, which was a Connecticut-based pyramid scheme, elaborately disguised as a work-at-home opportunity. DP Marketing solicited new recruits through "spam" and through newspaper classified ads across the country. The spam contained messages such as: "National Marketing Company seeks individuals to handle office duties from home. This is a full or part-time position with a salary of $13.50/hr. The position consists of processing applications for credit, loans or employment, as well as online consumer service."

Consumers who responded by visiting DP Marketing's Web site or by calling the company received a pitch stating that they could receive $13.50 per hour by just processing orders for the company from the comfort of their own homes. The defendants also represented that no experience was necessary, and that for a "registration fee" ranging from $9.95 to $28.72 purchasers would be sent everything needed to get started, including telephone scripts, product sheets, time sheets and ID numbers. What consumers actually got was a kit instructing them first to place advertisements identical to the ones to which they had responded, and then to read the same script to people who responded to their ads. Instead of $13.50 per hour, consumers' earnings depended on the number of new victims they recruited.

The FTC complaint alleged that the defendants misrepresented to consumers that DP Marketing offers jobs at a specified salary; failed to disclose the material fact that they were offering a pyramid work-at-home scheme; and provided to others the "means and instrumentalities" to commit unlawful and deceptive acts. On November 14, 2000, the court entered a stipulated final order banning the defendants from future pyramiding, barring them from misrepresenting the availability and profitability of jobs, and requiring the defendants to pay $72,000 in consumer redress.

The Commission has also brought a number of cases against credit repair scams that used spam as an integral aspect of their deception.[16] In a particularly pernicious variation on this scheme, consumers are urged to create a new credit identity in order to fix their credit. Using spam messages such as "BRAND NEW CREDIT FILE IN 30 DAYS," these scammers induce consumers to purchase instructions about how one can obtain a federally-issued, employee or taxpayer identification number, and use these numbers illegally in place of social security numbers to build a new credit profile that will purportedly allow one to get credit that would be de-

nied based on one's true credit history. In fact, using a false identification number to apply for credit is a felony—a point these scammers omit from their solicitations. The Commission, either on its own or through the Department of Justice, filed cases against seven operations that used this type of deceptive spam.[17]

More recently, in *FTC* v. *Para-Link International,*[18] the FTC sued several Florida-based companies that were using spam to market a work-at-home paralegal business opportunity. The Commission's complaint charged that the defendants use spam to induce consumers to purchase the business opportunity for $395–495. The spam contained representations such as: "Make Over $200 An Hour," and "You Can Process Simple Divorces and Bankruptcies From Home and Make Over $200 An Hour in as little as 30 Days!!!"; and urged prospective purchasers to call a toll-free number for more information. Defendants promised that the business opportunity would include training so purchasers could become at-home paralegals; defendants also promised to refer a steady stream of clients to purchasers of the business opportunity for a fee of $25 each.

According to the FTC's complaint, few consumers who purchased the business opportunity from the defendants ever realized these earnings. The court entered a temporary restraining order ("TRO") against the defendants on October 17, 2000, ordering them to cease operations, freezing their assets, and appointing a receiver to take charge of the companies. Subsequently, the court issued an order that extended the relief granted in the TRO pending issuance of a preliminary injunction.

Other types of deceptive schemes that use UCE have also been targets of FTC enforcement action, such as deceptive business opportunities[19] and deceptive weight loss schemes.[20] As these cases illustrate, the Commission's focus has been on the deceptive content of UCE messages.

C. Comprehensive Consumer and Business Education

The Commission has published nine consumer publications related to UCE, available in paper format and downloadable from the FTC's Web site. More than 1.6 million of these documents have been distributed to consumers, either through paper copies or via access to the Commission's Web site.[21]

The first, **Phone, E-mail and Pager Messages May Signal Costly Scams,** was published in 1996. It has been distributed in paper form over 16,000 times and has been accessed at the FTC's Web site more than 18,000 times. Two versions of the related **Trouble @ the In-Box** help consumers identify some of the scams showing up in electronic in-boxes and offer tips and suggestions for assessing whether an opportunity is legitimate or fraudulent. These publications also advise consumers about how to handle UCE and offer ideas for consumers to control the flow of UCE. The publications steer consumers to additional resource materials that can help them determine the validity of a promotion or money making venture. To date, over 87,000 paper copies of the brochures have been distributed, and they have been accessed on the FTC's Web site nearly 53,000 times.

How To Be Web Ready is a reader's bookmark that offers consumers tips for safe Internet browsing. It provides guidance for consumers on how to safeguard personal information, question unsolicited product or performance claims, exercise caution when giving their e-mail address, guard the security of financial transactions, and protect themselves from programs and files that could destroy their hard drives. A number of corporations and organizations have provided a link from their Web sites to the tips on the FTC's Web site, including Circuit City, Borders Group Inc., Netcom, Micron, and Compaq. More than 94,000 paper copies of the bookmark have been distributed, and it has been accessed more than 31,000 times on the FTC's Web site. A related publication, **Site-Seeing on the Internet: A Consumer's Guide to Travel in Cyberspace,** with similar helpful hints, has been accessed nearly a million times on the FTC's Web site, and over 165,000 papers copies have been distributed.

In July 1998, the FTC launched a public education campaign called **Spam's Dirty Dozen: 12 Scams Most Likely to Arrive Via Bulk E-mail** to publicize the most prevalent UCE scams. The list of scams was culled from a sampling of more than 250,000 spam messages that consumers had forwarded to the FTC's spam mailbox at *uce@ftc.gov.* The consumer alert identified the following twelve types of deceptive solicitations and described how each operates: business opportunity schemes; bulk e-mail programs[22]; chain letters; work-at-home schemes; health and diet scams; effortless income; free goods; investment opportunities; cable descrambler kits; guaranteed loans or credit on easy terms; credit repair; and vacation prize promotions. More than 24,000 paper copies of this consumer alert have been distributed, and it has been accessed more than 100,000 times on the FTC's Web site.

In March 2000, the Commission published an alert titled **Unsolicited Mail, Telemarketing and E-mail: Where to Go to "Just Say No"** which provided in-

formation to consumers on how to control junk mail and e-mail. Over 21,000 copies of this alert have been distributed in paper form, and it has been accessed over 20,000 times on the FTC's Web site. In September 2000, the Commission published a consumer alert entitled **The Lowdown on Chain Letters** in an effort to warn consumers about the risks of chain letters that arrive via e-mail. Over 10,000 paper copies of this brochure have been distributed, and it has been accessed over 8,200 times on the FTC's Web site.

In January of this year, the FTC published **Cracking Down on Mail, E-mail and Fax Scams: Project Mailbox** that offers tips to consumers about avoiding being scammed by mail or e-mail offers. The publication is only available on the FTC's Web site, and has been accessed online nearly 1,300 times to date.

IV. The Commission's Views on S. 630, the "Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2001" (the "CAN Spam Act of 2001").

The Commission generally favors the underlying goals of S. 630, which are to help control the additional costs and other potential negative effects that UCE can impose on Internet access service providers and other businesses and consumers that use the Internet, and to support consumer choice in the matter of whether to receive UCE. There are two basic problems that S. 630 addresses. First, there is the problem of fraudulent or deceptive UCE, and second, but also important, is the infrastructure problem that flows from the sheer volume of UCE. UCE, even if not deceptive, may lead to significant disruptions and inefficiencies in Internet services, and may constitute a great nuisance to consumers and businesses using the Internet. Both of these problems together pose a threat to consumers' confidence in the Internet as a medium for personal electronic commerce.[23]

S. 630 mandates the "permission-based" marketing model already adopted by many well-known manufacturers and sellers of consumer goods and services, and advocated by the Center for Democracy in Technology and other groups in their 1998 "Report to the Federal Trade Commission of the Ad-Hoc Working Group on Unsolicited Commercial E-Mail."

Section 5 of S. 630 would make it unlawful to initiate transmission of a commercial e-mail message that does not contain specified items of information designed to enable consumers to identify UCE and to prevent future receipt of it from that sender. These disclosures, required to be clear and conspicuous, are: an identification that the e-mail is an advertisement or solicitation; a notice of the opportunity (mandated by the bill) to decline to receive further UCE from the sender to the recipient; a functioning return e-mail address to which a recipient may send a reply to the sender to indicate a desire not to receive further e-mails from that sender; and a valid physical postal address of the sender. Section 5 of S. 630 would also make it unlawful:

- for a sender, or any person acting on behalf of the sender, to initiate the transmission of UCE to any recipient after that recipient has sent to the e-mail address provided by the sender a request not to receive further e-mail from that sender;
- for any person to initiate the transmission of a commercial e-mail message that "contains, or is accompanied by, header information that is materially or intentionally false or misleading, or not legitimately obtained;" or
- for any person to initiate the transmission of a commercial e-mail message "with a subject heading that such person knows is likely to mislead the recipient about a material fact regarding the contents or subject matter of the message."

S. 630 includes a multi-faceted enforcement scheme. First, Section 5 of the bill, described above, would be enforceable by the FTC, and any violation of it would be treated as if it were a violation of an FTC Trade Regulation Rule adopted pursuant to Section 18 of the FTC Act, 45 U.S.C.§57a. This means that each such violation would subject the violator to a maximum civil penalty of $11,000 in an enforcement action by the FTC.[24]

Second, the bill would allow other federal agencies that have jurisdiction over industries whose activities are wholly or partially exempt from the FTC's jurisdiction, such as banking and common carriers, to enforce the bill. Third, both providers of Internet access service and the Attorneys General of the various states would have enforcement authority to obtain injunctions against violations of Section 5 of the bill, and to recover damages.[25]

In addition to civil enforcement of Section 5 of S. 630, Section 4 of the bill would establish liability for criminal fines or up to one year imprisonment for anyone who

"intentionally initiates the transmission of any unsolicited commercial electronic mail message . . . with knowledge that such message contains or is accompanied by header information that is materially or intentionally false or misleading."

S. 630 specifically provides that it would have no effect on the ability of providers of Internet access service to enforce their anti-UCE policies. Finally, the bill would mandate a study by the Commission within 18 months that would provide a detailed analysis of the effectiveness and enforcement of the bill's provisions.

The Commission's views, set forth below, on the provisions of S. 630, are informed by workshops and other discussions the Commission has had with interested members of the Internet and marketing industry, as well as the Commission's law enforcement experience in the area of UCE, and in related areas, such as the "Do Not Call" provision of the Telemarketing and Consumer Fraud and Abuse Prevention Act.[26] Where useful, the Commission also sets forth its views on H.R. 718, another legislative proposal dealing with UCE that is similar to S. 630.[27]

A. The Definition of the Term "Commercial Electronic Mail Message" [§ 3(2) of S. 630].

A key term used throughout S. 630 is "commercial electronic mail message"; this term is defined in Section 3 of the bill. The relevant portion of the definition provides that "an electronic mail message shall not be considered to be a commercial electronic mail message solely because such message includes . . . a reference or link to an Internet web site operated for a commercial purpose." Commission staff has observed that much UCE—particularly UCE related to pornographic web sites—consists of nothing more than such a reference or link. The definition as currently drafted could potentially be exploited by senders of such UCE to evade the requirements of the bill. As a practical matter, it may be difficult to demonstrate to a court that an e-mail consisting of nothing more than a URL and perhaps a statement such as "check this web site!" falls within the bill's definition of "commercial electronic mail message"—*i.e,*. that its "primary purpose . . . is to advertise or promote, for a commercial purpose, a commercial product or service"—when the definition apparently demands more than a reference or link to an Internet web site operated for a commercial purpose to bring an e-mail message within the scope of the bill's coverage. The House Bill currently under consideration, H.R. 718, avoids this problem by employing a definition of the term that tracks the definition in S. 630 but excludes the final problematic clause.

B. The Prohibition Against Header Information That Is Materially or Intentionally False or Misleading, or Not Legitimately Obtained [§ 5(a)(1) of S. 630)].

This provision would likely benefit consumers. Chief among consumer complaints about UCE is that consumers do not know who sent the UCE, and therefore do not know to whom they can send a request not to receive more UCE. In addition, false routing information can cause UCE messages to clog the e-mail systems of providers of Internet access service, thereby slowing service to consumers trying to dial into the Internet through those providers of Internet access service or even completely shutting down the providers' systems. Indeed, some providers have had to devote significant resources and staff to dealing with the sometimes overwhelming tide of UCE. These costs likely are passed on to consumers. The Commission is aware of no legitimate reason for using false header information.

The provision prohibiting falsification of routing information would allow a consumer to know who sent him or her the UCE. It could also help providers of Internet access service better handle the flow of both solicited and unsolicited commercial e-mail, because valid routing information is more easily handled by the Internet access service providers' e-mail servers. This could result in fewer impairments to consumers' Internet service, and possibly fewer costs passed on to consumers.

The provision strikes an appropriate balance by specifying that header information that is "materially . . . false or misleading" violates Section 5 of S. 630, while technically false header information not meeting the standard of "materiality" would be actionable only if it could be shown that the falsehood was intentional. This appropriately ensures that inadvertent and relatively minor mistakes in header information will not trigger enforcement action or private lawsuits.

The language in the provision specifying that header information "not legitimately obtained" violates Section 5 of the bill appears ambiguous. To ensure that this language does not create enforcement problems or engender unintended lawsuits, clarification would be helpful.

This provision would impose few if any additional costs on senders of commercial e-mail. Further, the benefits to providers of Internet access service, recipients of e-mail, and Internet users generally who desire and expect optimum convenience, likely outweigh any additional costs. Also, these provisions could make the use of

commercial e-mail a more effective marketing tool, because consumers likely would be more willing to trust the contents of a piece of UCE if they know the source of the e-mail.

C. The Prohibition Against a Subject Heading That Such Person Knows Is Likely To Mislead the Recipient About a Material Fact Regarding the Contents or Subject Matter of the Message [§ 5(a)(2) of S. 630].

Consumers also complain about being misled by false subject lines of UCE. These misrepresentations lead them into believing that the contents are about one thing, but when they open the e-mail, they discover that it is about something else entirely. For example, many senders of UCE that advertises pornography will use benign subject lines such as "Thanks for lunch" or "An old friend" that the average e-mail recipient might believe are messages from someone he or she knows. In fact, to the consumer's surprise, such UCE advertises pornographic Web sites. A subject line that non-deceptively described the contents of the UCE would allow a recipient to make an informed decision about whether to open the message.

The Commission is aware of no legitimate reason for using false subject heading information and supports this provision. Prohibiting deceptive subject lines would impose few, if any, additional costs on legitimate companies that use commercial e-mail to promote their goods and services. Benefits to individual consumer recipients of e-mail and to Internet users generally would outweigh any costs. As with the provisions discussed above, this provision could make the use of commercial e-mail a more effective marketing tool, because consumers likely would be more willing to trust the contents of a piece of UCE if they could rely on representations made in the subject to accurately and truthfully reflect the message's contents.

This provision of S. 630, however, raises an issue about the Commission's authority to challenge deception under Section 5 of the FTC Act. Currently, the Commission could challenge a materially false or misleading subject line in a commercial e-mail message under Section 5 of the FTC Act, as it could any other deceptive representation. The applicable legal standard that must be met to demonstrate a deceptive practice is that it is "likely to mislead consumers acting reasonably under the circumstances about a material fact."[28] S. 630 would establish a higher standard applicable to subject lines in commercial e-mail messages by requiring a showing that the person who sent the e-mail had knowledge that the subject line was likely to mislead the recipient about a material fact regarding the contents or subject matter of the message. The scienter requirement—not an element of deception under Section 5 of the FTC Act—would make it more difficult for the Commission to take action under S. 630 against materially false and misleading subject lines. As a matter of law enforcement, deceptive UCE should not be treated differently from any other deceptive act or practice. Moreover, the requirement of a showing that the subject line was likely to mislead the *recipient*, and not a reasonable consumer, could increase the burden on the Commission in any action targeting materially false or deceptive representations made in subject lines of commercial e-mail messages. This may require a showing that each individual recipient was likely to be misled, a very difficult burden to meet.

Because violating Section 5 of S. 630 would expose a person to liability for civil penalties of up to $11,000 per violation, the Subcommittee may believe it appropriate to adopt stringent standards for liability in S. 630 to protect against penalties for what could be mere technical violations of the Bill.[29] However, the Commission believes that it would be useful for S. 630 to make clear that it does not affect the FTC's current ability to bring enforcement actions targeting materially false or deceptive representations in commercial e-mail messages under Section 5 of the FTC Act, pursuant to the criteria of, and seeking the remedies available under, that Act.[30] This could be accomplished by broadening the savings clause in Section 7(a) of the bill.[31] Therefore, clarification of an intent to leave intact the Commission's powers under the FTC Act with respect to deceptive representations in subject lines of commercial e-mail messages would be helpful.

D. The Requirement of an E-mail Address to Which Consumers Can Request to No Longer Receive UCE, and the Requirement That Senders of UCE Honor Such Requests [§§ 3 & 4 of S. 630].

These provisions would also likely benefit consumers. A major frustration among recipients of commercial e-mail, and particularly with UCE, is that often any reply to the sender's e-mail address "bounces back" and is never received by the sender. In such a case there is nothing the consumer can do to avoid receipt of additional commercial e-mail from the same sender.

The provision requiring senders of commercial e-mail messages to include a valid reply e-mail address to which consumers may send requests to receive no more e-

mail, and requiring senders to honor such requests, would go a long way in helping consumers control the amount of commercial e-mail, both solicited and unsolicited, they receive. However, it would likely impose some burdens on senders of commercial e-mail. S. 630 would require every sender of commercial e-mail to set up and maintain an e-mail account to which consumers could send requests, and senders would have to monitor and update their mailing lists at least as often as every 10 days. Nevertheless, the benefits of such a requirement would likely outweigh the costs to the senders.

E. The Requirement of an Identifier, Opt-out Opportunity, and Physical Address of the Sender in Each UCE Message.

S. 630 would require that every UCE message contain an identifier indicating that the message is an advertisement or solicitation. This provision would benefit consumers by enabling them to immediately recognize UCE messages as advertisements. It also may allow consumers to employ software that would filter UCE into a separate folder, or block UCE messages entirely. This provision would thus help empower consumers to control the amount of UCE they receive. Notice that a message is an advertisement or solicitation would impose few, if any, additional costs on senders of UCE; they would merely have to add a few words (or even a few letters) to each message sent. Unlike print or broadcast communications, additional words in e-mail messages do not add to their cost.

S. 630 would also require each UCE message to contain a clear and conspicuous notification of an opportunity for the recipient to decline to receive further UCE from the sender. This requirement would benefit consumers by helping them realize that they have a choice about whether they wish to receive additional UCE from a particular sender. Again, this requirement would impose few, if any, additional costs on senders of UCE; as with the identifier requirement, they would only have to add a few words to each message sent. It might also lower the overall volume of unwanted UCE on the Internet, thereby lowering certain cost burdens imposed on providers of Internet access service and potentially passed on to consumers.

Finally, S. 630 would require that each UCE message include the physical location of the sender. This provision might produce benefits in the form of enhanced consumer confidence in the legitimacy of senders. In cases where the UCE eventually leads to a transaction, the consumer would have an additional means of contacting the seller if the goods or services are not provided in accordance with the consumer's understanding, or, where applicable, if the consumer wishes to go to a seller's store. It is noteworthy that this provision of S. 630 is consistent with the guidelines of the Organization for Economic Co-operation and Development, which recommend that online businesses disclose their physical address. The Commission has endorsed those guidelines.[32]

F. The Enforcement Scheme.

The enforcement scheme laid out by S. 630 likely would work well. It is modeled on similar schemes Congress established for enforcement for the Commission's 900-Number Rule and the Telemarketing Sales Rule in the statutes that mandated promulgation of those Rules.[33] The enforcement provisions would allow the Commission to treat violations of S. 630 as violations of a rule under Section 18 (15 U.S.C. § 57a) of the FTC Act regarding unfair or deceptive acts or practices. Moreover the Commission's efforts would be supplemented with those of the state Attorneys General, and possibly by other federal agencies with jurisdiction in areas where the FTC has none. This type of dual federal-state enforcement scheme has proved extremely successful in the past, particularly in challenging deceptive and abusive telemarketing practices, and the Commission would expect it to work equally well in this context.

G. The Effect on Other Laws [§ 7 of H.R. 630].

S. 630 provides an express savings clause for specific enforcement provisions of the Communications Act of 1934 and for federal criminal statutes. This express clause appears to preclude enforcement of most existing federal civil laws that apply to commercial electronic mail, such as the FTC Act's broad prohibition of deceptive advertising, except to the extent specifically provided in S. 630. The Commission believes that S. 630 should not supplant other relevant federal law, and recommends expanding the savings clause to make this clear.

H. The Provision That Within 18 Months the Commission Conduct A Study of the Effectiveness and Enforcement of S. 630's Provisions.[34]

A study of the effectiveness and enforcement of S. 630, if enacted with a requirement for such a study, would be based largely on the consumer complaint data from the Commission's UCE database. This database holds more than eight million UCE messages forwarded by consumers and providers of Internet access service. The

Commission uses this database to assess the current state of UCE, spot emerging trends, and target its law enforcement efforts on the most serious problems. The Commission would be able to conduct a study on the effectiveness and enforcement of S. 630's provisions. However, 18 months may be too short a time frame for the Commission to effectively research and develop such a study. To meaningfully measure the effect of S. 630, it may be necessary to assess the situation before it goes into effect, and then gather data and information after it goes into effect and businesses have had time to come into compliance. The Commission therefore urges that the time frame for the study be extended to 24 months, in order to enhance the value of the study.

The Commission appreciates the opportunity to provide its views on S. 630 and on its efforts against deceptive UCE. I would be happy to answer any questions.

END NOTES

[1] The views expressed in this statement represent the views of the Commission. My responses to any questions you may have are my own.

[2] 15 U.S.C. § 45(a). The Commission also has responsibilities under more than 45 additional statutes, *e.g.,* the Fair Credit Reporting Act, 15 U.S.C. §§ 1681 *et seq.*, which establishes important privacy protections for consumers' sensitive financial information; the Truth in Lending Act, 15 U.S.C. §§ 1601 *et seq.,* which mandates disclosures of credit terms; and the Fair Credit Billing Act, 15 U.S.C. §§ 1666 *et seq*., which provides for the correction of billing errors on credit accounts. The Commission also enforces over 35 rules governing specific industries and practices, *e.g.*, the Used Car Rule, 16 CFR Part 455, which requires used car dealers to disclose warranty terms via a window sticker; the Franchise Rule, 16 CFR Part 436, which requires the provision of information to prospective franchisees; and the Telemarketing Sales Rule, 16 CFR Part 310, which defines and prohibits deceptive telemarketing practices and other abusive telemarketing practices.

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

[4] *FTC* v. *Corzine,* CIV–S–94–1446 (E.D. Cal. filed Sept. 12, 1994).

[5] Section 5 of the FTC Act, 15 U.S.C. § 45, authorizes the Commission to prohibit unfair or deceptive acts or practices in commerce. The Commission may initiate administrative litigation, which may culminate in the issuance of a cease and desist order. It can also enforce Section 5 and other laws within its mandate by filing actions in United States District Courts under Section 13(b) of the FTC Act, 15 U.S.C. § 53(b), seeking injunctions, consumer redress, disgorgement, and other equitable relief. Section 18 of the FTC Act, 15 U.S.C. § 57a, authorizes the Commission to promulgate trade regulation rules to prohibit deceptive or unfair practices that are prevalent in specific industries. Courts may impose civil penalties of up to $11,000 per violation of Commission trade regulation rules.

[6] For example, the National Advertising Division of the Council of Better Business Bureaus, Inc., operates the advertising industry's self-regulatory mechanism.

[7] For example, the Rule Concerning Cooling-Off Period for Sales Made at Homes or at Certain Other Locations (the "Cooling-Off Rule"), 16 CFR Part 429; the Mail or Telephone Order Merchandise Rule, 16 CFR Part 435; the Trade Regulation Rule Pursuant to the Telephone Disclosure and Dispute Resolution Act of 1992 ("The 900-Number Rule"), 16 CFR Part 308; and the Telemarketing Sales Rule Pursuant to the Telemarketing and Consumer Fraud and Abuse Prevention Act, 16 CFR Part 310.

[8] The first of these was held in the fall of 1995, when the Commission held four days of hearings to explore the effect of new technologies on consumers in the global marketplace. Those hearings produced a staff report, *Anticipating the 21st Century: Consumer Protection Policy in the New High-Tech, Global Marketplace* (May 1996).

[9] This report is available at *www.cdt.org/spam.*

[10] "Header" information, at minimum, includes the names, addresses, or descriptions found in the "TO:", "FROM:", and "SUBJECT:" lines of an e-mail. It also includes the technical description of the route an e-mail has traveled over the Internet between the sender and recipient.

[11] *FTC* v. *Benoit,* No. 3:99 CV 181 (W.D.N.C. filed May 11, 1999). This case was originally filed under the caption *FTC* v. *One or More Unknown Parties Deceiving Consumers into Calling an International Audiotext Service Accessed Though Telephone Number (767) 445–1775.* Through expedited discovery, the FTC learned the

identities of the perpetrators of the alleged scam by following the money trail connected to the telephone number. Accordingly, the FTC amended its complaint to specify the defendants' names.

[12] A similar scheme that used spam was targeted in *FTC* v. *Lubell,* No. 3–96–CV–80200 (S.D. Ia. 1996). In that case, the spam urged consumers to call an expensive international number to hear a message that purportedly would inform them about discount airline tickets and how to enter a sweepstakes.

[13] *See http://www.nanpa.com/home.*

[14] The term "audiotext services" describes audio information and entertainment services offered over the telephone through any dialing pattern, including services accessed via 900-number, as well as international and other non-900-number, dialing patterns.

[15] *FTC* v. *Martinelli,* No. 399 CV 1272 (CFD) (D. Conn. filed July 7, 1999). Other alleged pyramid schemes that utilized spam have been targets of FTC enforcement action. *See, e.g., FTC* v. *Nia Cano,* No. 97–7947–IH–(AJWx) (C.D. Cal. filed Oct. 29, 1997); *In re: Kalvin P. Schmidt,* Docket No. C–3834 (final consent Nov. 16, 1998).

[16] *FTC* v. *Consumer Credit Advocates,* No. 96 Civ. 1990 (S.D.N.Y. filed Mar. 19, 1996); *FTC* v. *Dixie Cooley, d/b/a DWC,* No. CIV–98–0373–PHX–RGS (D. Ariz. filed March 4, 1998).

[17] *FTC* v. *Cliff Cross and d/b/a Build-It-Fast,* Civ. No. M099CA018 (W.D. Tex. filed Feb. 1, 1999); *FTC* v. *Ralph Lewis Mitchell, Jr.,* No. CV 99–984 TJH (BQRx) (C.D. Cal. filed Jan. 29, 1999); *FTC* v. *Frank Muniz,* No. 4:99–CV–34–RD (N.D. Fla. filed Feb. 1, 1999); *U.S. v. A. James Black,* No. 99–113 (M.D. Fla. filed Feb. 2, 1999); *FTC* v. *James Fite, d/b/a Internet Publications,* No. CV 99–04706JSL (BQRx) (C.D. Cal. filed April 30, 1999); *U.S. v. David Story, d/b/a Network Publications,* 3–99CV0968–L (N.D. Tex. filed April 29, 1999); and *FTC* v. *West Coast Publications,* LLC., CV 99–04705GHK (RZx) (C.D. Cal. filed April 30, 1999).

[18] *FTC* v. *Para-Link International,* No. 8:00–CV–2114–T–27E (M.D. Fla. filed Oct. 16, 2000).

[19] *FTC* v. *Internet Business Broadcasting, Inc.,* No. WMN–98–495 (D. Md. filed Feb. 19, 1998); *United States v. PVI, Inc.,* No. 98–6935 (S.D. Fla. filed Sept. 1, 1998).

[20] *TrendMark International, Inc.,* Docket No. C–3829 (final consent Oct. 6, 1998)

[21] The distribution and access numbers for these consumer education materials are accurate as of March 31, 2001.

[22] These schemes claim that one can make money sending one's own solicitations via bulk e-mail. They offer to sell one lists of e-mail addresses or software to allow one to make the mailings. What they don't mention is that the lists are of poor quality and that sending bulk e-mail violates the terms of service of most providers of Internet access service.

[23] *See Unsolicited Commercial E-mail: Hearing Before the Subcomm. on Telecomm., Trade and Consumer Protection of the House Comm. on Commerce,* 106th Cong. (Nov. 1999) (statements of various providers of Internet access service detailing costs and loss of goodwill caused by UCE); Serge Gauthronet & Etienne Drouard, *Unsolicited Commercial Communications and Data Protection* (Jan. 2001), p. 9. (finding, in this study undertaken by the Commission of European Communities, that the global cost to Internet users may be conservatively estimated at 10 billion Euros ($8.943 billion) annually); *See generally* the 1998 *Report to the Federal Trade Commission of the Ad-Hoc Working Group on Unsolicited Commercial E-Mail* (citing several types of costs imposed on consumers and businesses by UCE—intrusion on consumers' privacy, lost opportunity costs, Internet infrastructure costs, access and storage fees, and reputational harms) (available at www.cdt.org/spam).

[24] An action seeking civil penalties for violation of a Trade Regulation Rule promulgated under Section 18 must be forwarded by the Commission to the Department of Justice for filing and litigating. If the Department of Justice declines to file the complaint within 45 days, the Commission, through its own attorneys, may file and litigate the matter. 45 U.S.C. § 56(a). Pursuant to Section 13(b) of the FTC Act, 45 U.S.C. § 53(b), however, the Commission may file and litigate, through its own attorneys, any action seeking injunctive relief, consumer restitution, disgorgement of ill-gotten gains or other equitable remedies without first forwarding the matter to the Department of Justice.

[25] Successful plaintiff states or providers of Internet access service could recover an amount equal to actual damages or statutory damages of up to $10 for each separately addressed unlawful message received by the states' residents, with a maximum of $500,000, and in cases of willful and knowing violations, three times this amount. Recovery of costs and reasonable attorneys' fees would be authorized. Section 6(e) of S. 630 would establish an affirmative defense in cases brought by providers of Internet access service or the states where a defendant can show that it

has established and implemented compliance policies and procedures, and that any violation occurred despite good faith efforts to follow those policies and procedures.

[26] 5 U.S.C. § 6102(a)(3)(A).

[27] This bill was introduced on January 3, 2001 by Rep. Heather Wilson, and is titled the "Unsolicited Commercial Electronic Mail Act of 2001."

[28] *Cliffdale Associates, Inc.,* 103 F.T.C. 110, 165, *appeal dismissed sub nom., Koven* v. *F.T.C.,* No. 84–5337 (11th Cir. 1984).

[29] It is noteworthy that Section 5(m)(1) of the FTC Act, 15 U.S.C. § 45(m)(1), requires the Commission, in actions to recover civil penalties for violations of trade regulation rules, to prove that the defendant violated the rule "with actual knowledge or knowledge fairly implied on the basis of objective circumstances that such act is unfair or deceptive and is prohibited by such rule." Moreover, this provision requires courts, in assessing civil penalties for rule violations, to "take into account the degree of [the defendant's] culpability, any history of prior such conduct, ability to pay, effect on ability to continue to do business, and such other matters as justice may require."

[30] In enforcement actions under Section 5 of the FTC Act the Commission can not seek civil penalties; instead it can seek administrative cease and desist orders, or, in the case of actions in district court under Sections 5 and 13(b) of the FTC Act, equitable remedies—injunctions, disgorgement, or restitution for consumer victims.

[31] In a related context, Congress ensured, in enacting the Telemarketing and Consumer Fraud and Abuse Prevention Act, that the Commission's ability to challenge deceptive telemarketing practices under the FTC Act would remain intact by including a broad savings clause: "Nothing contained in this chapter shall be construed to limit the authority of the Commission under any other provision of law." 15 U.S.C.§ 6105(c):

[32] *See, http://www.ftc.gov/opa/1999/9912/oecdguide.htm.*

[33] Telephone Disclosure and Dispute Resolution Act of 1992 (codified in relevant part at 15 U.S.C. §§ 5701 *et seq.*) and the Telemarketing and Consumer Fraud and Abuse Prevention Act (codified in relevant part at 15 U.S.C.§§ 6101–6108).

[34] The House bill, H.R. 718, contains a provision substantially similar to the mandatory study provision of S. 630.

Senator BURNS. Thank you very much. We've enjoyed your testimony and I have some questions for you. We've been joined on the Committee by Senator Rockefeller. Do you have a statement?

STATEMENT OF HON. JOHN D. ROCKEFELLER IV, U.S. SENATOR FROM WEST VIRGINIA

Senator ROCKEFELLER. I'm going to put it in the record.

[The prepared statement of Senator Rockefeller follows:]

PREPARED STATEMENT OF HON. JOHN D. ROCKEFELLER IV, U.S. SENATOR FROM WEST VIRGINIA

Thank you Mr. Chairman for holding this hearing. As we all know from our constituents, junk e-mail is a serious problem. It is costly to consumers; it is costly to Internet service providers; and it often puts pornography or fraudulent material into our in-boxes.

We should find a way to reduce the costs of junk e-mail, while respecting the First Amendment, and the rights of legitimate marketers.

I applaud your efforts to bring this matter before the Committee again this year, and to reintroduce legislation. However, I feel that for legislation to be successful it must include several things that are not yet in the bill we are considering.

First, we should give regular Americans and businesses the ability to protect themselves from junk e-mail. The bill includes a "private right of action" for Internet service providers, but leaves regular Americans and businesses without the ability to go to court if they are injured in violation of the bill.

I agree that we should give Internet service providers the right to sue, but why leave the everyday people who have to suffer through junk e-mail everyday with no way to seek redress? That doesn't make sense.

Second, we should listen hard to what Mr. Catlett on the second panel has to say about how effective the proposed bill would be in actually stopping illegitimate junk e-mail. This bill should be about consumers—Internet users—first and foremost. If we do not give consumers the tools to stop e-mails they don't want, then the bill will not work.

I think that we should start by requiring that every commercial e-mail contain the word "advertisement" in the subject line. That way consumers can use technology to filter for them if they wish. Mr. Catlett has several other ideas that we should pay close attention to.

I am sorry that I cannot spend more time at the hearing today and I look forward to working with all of you on moving this bill forward.

Senator BURNS. You're going to put your statement in the record and I'm—Ms. Harrington, do we need legislation to enable you to do the things that should be done with regard to spamming?

Ms. HARRINGTON. I think that this proposed bill greatly enhances the FTC's current statutory authority. We don't need legislation to give the FTC the authority to bring enforcement action against deception. However, this legislation makes very specific that certain practices are deceptive so that lightens our prosecutorial burden, if you will, by establishing that as a matter of law it is a deceptive practice to fail to do certain things. And in addition, there are provisions in S. 630, for example the requirement of opt-out, and the requirement that there be a valid return e-mail address and a physical address that probably—that certainly wouldn't be natural remedies that we could obtain in a lawsuit under the FTC Act, so yes, I think there is a need.

Senator BURNS. How close are you to being up to speed for enforcement of this Act?

Ms. HARRINGTON. We're ready.

Senator BURNS. You're ready. Any additional dollars you'll need?

Ms. HARRINGTON. I don't do dollars.

[Laughter.]

Ms. HARRINGTON. Let me tell you that the FTC has been the leading federal enforcement agency in the area of Internet fraud both in terms of the dollar volume of fraud stopped, the numbers of actions taken. We've done that on a lean budget. Our people are well-trained and ready to go. We have, as I mentioned, an existing database of over 8 million pieces of spam. That is a searchable database and we can search that database to find spam that is not in compliance with certain provisions of this statute if it becomes law, and we're ready to go.

Senator BURNS. I found the Wall Street Journal article the other day very interesting and pretty eye-opening too. It seems like as soon as the ISPs and the consumers come up with ways to filter out spam, it doesn't take spammers very long to circumvent that other technology. Can you comment right now, the cat and mouse game, and if there's anything the FTC can do and again, do you have the tools to do it?

Ms. HARRINGTON. We have decades of experience with fraudsters using new technologies and they are very good at innovating to get around laws and other blocks to their bad practices. I cannot tell you that we can stay a step ahead of them.

Senator BURNS. We're also running into a lot of spamming in the wireless situation.

Ms. HARRINGTON. Right.

Senator BURNS. Are you equipped there?

Ms. HARRINGTON. I think that——

Senator BURNS. Is the spamming in the wirless a little bit different than in the wire lines.

Ms. HARRINGTON. It is. It's interesting you ask. I just came back from a meeting of an organization called the International Marketing Supervision Network which is a group of consumer protection authorities from over 30 OECD and related countries. I was talking to our colleagues in Scandinavia where wireless is a far more pervasive form of communication technology and I was talking to them specifically about this issue, about wireless spam.

I think we have a steep learning curve to get up to speed. We're working on it. We had a workshop about 9 months ago on this issue at the FTC, where we invited industry and law enforcement and consumer groups to come in and talk with us about the technology, about business plans and business models that might use that technology for marketing. I would tell you that the legitimate businesses, both the communications companies and the innovators who are seeking to use the technology, have been very forthcoming and helpful in helping us understand this. But I think we've got a steep learning curve.

We can always use more resources. When I say I don't do dollars, I run an enforcement program. We have done everything that we can do to stretch every person's time and every dollar that the Congress has provided to us. I think wireless poses a whole new set of issues again and I think that if there are additional resources to be had, we would make good use of them. And I can also tell you that with the resources we currently have, we are working very hard to understand and stay on top of the technology.

Finally, I would say that one difference between our approach to the Internet and now wireless and to the fraudulent and deceptive applications of new technologies—one difference between our approach at the FTC and practically everyone else's approach, I think, is that our decision was to train the entire staff, all of the attorneys, all of the investigators, all of the paralegals on these technologies.

So rather than having a unit that is only devoted to the Internet, everybody knows about the Internet, has access to our lab and our tools. And that means we can shift our people really quickly from telemarketing to Internet to wireless back to telemarketing because everybody's trained up.

Senator BURNS. You mentioned the fact that you had over 8 million complaints on spamming and examples of spamming. Can you give me any kind of a figure on the number or the percentage of those complaints which were out and out fraudulent pieces of spam?

Ms. HARRINGTON. Whew, there are two ways of looking at it. Number one, what does the spam say. And I would say that the overwhelming majority of those 8 million pieces of spam make blatantly false statements about earnings, about product performance, something like that.

On the other hand, and much to my gratification and ours, we find that the people who forward this spam to us generally don't fall for it. There are certainly exceptions where consumers have lost significant money relying on these spams but we also find that lots and lots and lots of people don't believe it. But they send it to us because we've asked—you know: give us your tired, your poor and your spam. We want this. We want to see what's coming into

consumers' mailboxes. We want to organize it and search it, so that we can keep track of what's going on with this marketing medium.

Senator BURNS. Senator Rockefeller.

Senator ROCKEFELLER. Thank you Mr. Chairman.

Senator BURNS. You're welcome.

Senator ROCKEFELLER. We're very courteous to each other. We're good friends.

I get a lot of these complaints too from my folks in West Virginia and actually it would be interesting to know the percentage of your folks versus my folks that have home computers, et cetera. We'll compare that at a later date. You're not responsible for that, Ms. Harrington.

But one of the concepts which has been put forward is the idea of tagging, you know, labeling something in advertisements and I'm trying to think around in my mind what—you know, I turn on AOL and it sort of—do you have to say something's an advertisement or do people kind of inherently know it's an advertisement just by the way it looks?

For example, when I put on AOL I cannot put on AOL without, you know, I hear the you've got mail thing only after I've gotten rid of what is clearly an advertisement for one reason, it's not AOL, which one obviously recognizes. Then second, it looks like an advertisement. If it walks like a duck, et cetera.

So my question to you would be, and ISPs I would have to assume might be against that, either because they think it's inconvenient. They get revenue from it although, on the other hand, they also get swamped by it, or some people do, you know, trying to push all this stuff through.

Do you think that tagging or labeling something in advertisement, the argument being that while—what is your view on that?

Ms. HARRINGTON. With respect to unsolicited commercial e-mail, the proposed bill requires a label that would indicate that it is an advertisement or it is a commercial e-mail.

Senator ROCKEFELLER. It would say advertisement.

Ms. HARRINGTON. It doesn't specifically say that it has to say advertisement I don't believe.

Senator ROCKEFELLER. Well that's what I am trying to get from you. In other words, isn't—I mean there are all kinds of users. I mean it's like, one of the people that I work with and I were talking over here about people using cell phones, and we were trying to figure out how many unnecessary phone calls are made because there are things called cell phones in this world, and we came up with a mutual conclusion of about 50 percent of the phone calls that were made really don't have to be made, but they are there because everybody's got a phone. So, everybody's got an advertisement.

My assumption is that they would recognize that. That may be only because I use the Internet and therefore am in a position to recognize it and others might not and might be subject to it, particularly the ones that pop up, you know, in the corner of your screen. They tend to have a special kind of a nature. Then you read them, you don't look for the tag, you just—you look for the body of information to the extent that your eye stays over there, and you know it's an advertisement. So, I just want to get a sense of wheth-

er you think it's necessary to label it as such, where those who don't use it as much might be less—or it's fine without it.

Ms. HARRINGTON. Well you raise the issue of blurring. And that's an issue that has been central to all media as it becomes used more and more for advertising. We have issues with newspapers in blurring, and you now see in print media typically, that text that looks like it could be editorial text is labeled, advertisement when it is such. We saw that issue with television in blurring——

Senator ROCKEFELLER. It's the same principle there actually, because it's like—I obviously did mean to interrupt you or else I wouldn't have done it. But for example, sometimes countries whose kings or prime ministers are coming over here, do sections. And you're right. In the newspaper, advertisement will be written across the top. But you don't need to see that to know that. It looks like that, because it's got a picture of the king or the prime minister or whatever it is and some beautiful ocean. So, you know it's an advertisement without looking. So I, again, I just want to hone in on the tagging thing.

Ms. HARRINGTON. But—one of the beauties of the Federal Trade Commission Act is that it focuses on the reasonable consumer, and what a consumer reasonably understands is something that changes with time, with experience. You posed the question from the standpoint of the consumer who is less familiar with the Internet. And when a medium is new, I think that we need to assume that most consumers are less familiar. So at one point in time, it is deceptive to fail, or it may be deceptive to fail to indicate that something is, in fact, an advertisement, when consumers are very unfamiliar with that.

You raised the example, or point to the example of the pop up screen. And you know, I know that we've all seen pop up screens that are in the Microsoft Windows warning or error message format, that are actually advertisements. Are you familiar with that format? And so when you click on the red X to close it out, instead of closing it out, it may take you to an advertisement. Now my view is that, at this point in time, the reasonable consumer who sees a Microsoft Window warning message format in a pop up screen, the reasonable consumer thinks that that is an error or a warning message and doesn't think that it's an advertisement. Now 5 years from now, the reasonable consumer may know, ah-hah. You know, that could be anything. And so, the reasonable consumer is less likely to be misled or deceived.

So it really—that is really one of the great strengths of the Federal Trade Commission Act. It's flexible because it focuses in part on what the reasonable consumer understands a representation or a situation to mean, and that changes, as media change, as circumstances change, as times change.

Senator ROCKEFELLER. Do you think that this legislation would benefit from sort of a pop up part?

Ms. HARRINGTON. Well this legislation is about unsolicited commercial e-mail, and I think that that's a different matter than pop up screens and windows and other——

Senator ROCKEFELLER. No, I'm talking about pop ups that are advertisements.

Ms. HARRINGTON. Right.

Senator ROCKEFELLER. Not that are something else, you know, or a chat room or anything of that sort. I'm talking about a real advertisement. And you know the way they place those, you go to Netscape and all of a sudden you have something that you're looking at and then you have this great—this perpendicular rectangle hits you in the face and you've got to get rid of it before you can go on. And that's an enormous inconvenience.

Ms. HARRINGTON. I think the pop up screens raise a lot of the same issues of deception that false header and router information raises. I think that the method of delivery is different. Spam is delivered one way and pop up screens are programmed really differently and they're programmed to appear on a particular website rather than to be sent out as e-mail. So, I think that the method of delivery is different, and I'm not sure that there is a logical way to marry those two methods of delivery in one bill. That's my, like off the top of my head answer.

Senator ROCKEFELLER. As a matter of philosophy are you an opt-in or an opt-out person?

Ms. HARRINGTON. Well the Commission's position here is that it supports the opt-out provision in S. 630.

Senator ROCKEFELLER. No, but that's not what I asked. I'm trying to get underneath that. I mean, I'm an opt-in person. I think that you have to specifically say I am willing to do this. I want this, as opposed to you're getting it and then, oh, by the way, I think I'll decide to opt-out if I happen to understand what it is. I mean I'm just trying to get it at——

Ms. HARRINGTON. I think that the ISPs offer consumers the choice of—that is depending on which ISP I select, if I'm an opt-in person, I can select an opt-in ISP. If I'm an opt-out person, I can select an opt-out ISP. I personally have selected an opt-in ISP.

Senator ROCKEFELLER. OK. Thank you. Now one more question. And that is, the obvious one. Regarding ISPs—fundamentally, computers and the use of them is about consumers. And it's like saying is a car about General Motors or is a car about somebody who drives it. And I tend to think a car is about somebody who drives it, buys it, because it's their property. So the General Motors consideration is there, but it's secondary, to me at least. So that gets you to the so-called, the right to sue thing. And I know that can be an overblown question, and a stereotypical question, but nevertheless it's an interesting one because—and I think that Senator Burns and Senator Wyden and others, Senator Breaux, when they introduced this bill, they introduced it as a platform, not as a final product, because that's the way they usually do things, to get a discussion going and then to try and look at a bill that would be useful. But, isn't that right reserved to ISPs. That is, the right to sue. Shouldn't that be available to consumers and if—and I'm not asking, saying you have to agree with me, but I'd like to hear your kind of arguments on both sides. Some people say that you would be endlessly lost in litigation and all the rest of it, but I'd just be interested in your views.

Ms. HARRINGTON. Well on the one hand, I think that there is no group that has both a stronger interest and greater strength in protecting the interest against spam, unwanted spam, than the ISPs do. And so, unlike your General Motors analogy where there

may be a divergence of interest between General Motors' interest and the product owner and driver's interest, I think that the ISP and its customers may have a unified interest here in keeping unwanted e-mails out of consumers' mailboxes. The basis of the unified interest may be different. With the ISP, it goes to the economics and efficiency and reputation of their company. For the consumer, it's the time and nuisance factor of getting all this stuff. But I think the interest is the same.

And so on the pro side, you asked me to argue both sides. On the pro side, I would say that here, the ISPs have the same interest as consumers. It's rooted in something different, but the ISPs have more resources to take that interest to court and litigate it. I also think that there is greater efficiency in having the ISP bring the action, because then we have one lawsuit, not 10,000.

Senator ROCKEFELLER. And I understand that. But if one of the things about this problem is that it is so incredibly cheap for advertisers. I mean it's just the cheapest thing in the world. You push a button and millions of things go out across the world. Nevertheless, if you've gotten 8 million—I mean the aggregation of that begins to add up to quite a lot, and that implies therefore, revenue. And that revenue, even though it may be much smaller than television or radio or newspapers, nevertheless accrues to the ISPs. So is there anything to be said there?

Ms. HARRINGTON. I'm not sure that there is revenue that accrues to the ISPs from the sending of bulk spam. I don't know that. I think, though, to argue the other side of it, that is that there ought to be a right of action on the part of the individual, I would look at a couple of things first. The Telephone Consumer Protection Act of 1991 and 1992, which is enforced by the Federal Communications Commission gives individual consumers a cause of action in State Small Claims Court against telemarketers who call them after they have indicated to the telemarketer that they don't wish to receive calls.

So I would take a look at what the experience has been with that statute. I think that that is one of the first or few federal statutes that provides individuals with a right of action to vindicate their rights as consumers in state court, and my belief is that there has not been a glut of lawsuits brought in small claims courts on the part of individual consumers to enforce their rights under that statute.

You know, one concern is well, gee, we are opening the floodgates. The FTC does all of its law enforcement work in federal courts and so I have a selfish interest because we are all trying to get speedy resolution of our lawsuits to benefit consumers and get money back. I have a selfish interest in arguing against opening the federal courts to private rights of action by individual consumers because I think that that slows, that that would not be workable.

But you know, in this instance, Senator, I think that, that the ISPs and the customers who don't want spam really have an identical interest, and for myself personally, Star Power is my ISP at home, and I'd rather have them go to court to keep spam out of my mailbox than me spending time going to court on my own.

Senator ROCKEFELLER. If they would do that, and you indicate you think they would? Yes. It doesn't—it still—if there is a precedent to do so, if there is a precedent by saying consumers can't.

Ms. HARRINGTON. Can or cannot? I am sorry.

Senator ROCKEFELLER. Cannot, in this bill, and one has to deal with that at some point. But I understand what you are saying, and I appreciate your answers. Thank you, Mr. Chairman.

Senator BURNS. Senator, the state's attorney generals can do it. And each of the states can do it. On behalf of the consumers—we have been joined by Senator Allen of Virginia. And it is nice to have you here today. Ms. Harrington—and Senator Wyden, where have you guys been all day?

Senator ALLEN. I was at the Foreign Relations Committee meeting.

Senator BURNS. Good heavens. And we have been joined by Representative Goodlatte of Virginia, and who is working this legislation through the House side and if you would come forward and want to make a statement, why, we would sure entertain that.

Senator Wyden, do you have questions for Ms. Harrington?

Senator WYDEN. Mr. Chairman, since I just walked in, we were negotiating on a variety of the other tech questions, let me catch up a little bit so I am not repetitive, and I'll have some in a moment.

Senator BURNS. OK. Thank you very much. Ms. Harrington, we look forward to working with you and thank you for bringing some specifics that you think are necessary to make the legislation a little bit better and as far as you are concerned and the FTC. We appreciate those suggestions and we look forward in working with you as we get the final, the final bill out of Committee and move it on. So thank you for coming today, and we look forward to working with you. Thank you.

We are joined now by Representative Goodlatte of Virginia, who is working his will or the will of this legislation through the House of Representatives. We welcome you here today, Congressman, and we look forward to your comments.

STATEMENT OF HON. BOB GOODLATTE,
U.S. REPRESENTATIVE FROM VIRGINIA

Mr. GOODLATTE. Thank you, Mr. Chairman. Would that that were so, directing my will. I do appreciate the opportunity to testify before the Committee. It is good to be back. You have been generous in inviting me to testify before, and I do have a statement to make a part of the record, and I would offer part of it.

Senator BURNS. Without objection, so ordered.

Mr. GOODLATTE. Unsolicited e-mail, especially commercial e-mail such as advertisements, solicitations, or chain letters has become the junk mail of the information age. Jupiter Communications reported that in 1999 the average consumer received 40 pieces of spam. By 2005, that organization estimates that the total is likely to soar beyond 1,600 pieces to the average consumer. These numbers are astounding and while it costs the spammer almost nothing to send, it results in damage to a protected computer and would be punishable by a fine under Title 18 or by imprisonment for up to 1 year.

I want to commend you, Mr. Chairman, on the introduction of your own spam legislation that takes a balanced approach to combatting spam by including strong monetary penalties, but does not include a private right of action, an area in which we should proceed with caution in that it could have the effect of discouraging the use of electronic commerce.

Because of the complexity surrounding all e-commerce issues like spam, legislation must be carefully balanced to ensure that enforcement mechanisms address real harms without causing damage to the unique advantages provided by the Internet.

S. 630 provides law enforcement with the tools they need to combat spam without opening the floodgates to frivolous litigation. Legislation addressing the problem of unsolicited commercial e-mail is greatly needed during this legislative session to protect consumers and Internet service providers from victimization by spam.

I look forward to continuing to work with representative Heather Wilson, who has another important bill dealing with this issue in the House, as well as with you, Chairman Burns, and Senator Allen and Senator Wyden, who I know have a great interest in this legislation as well to achieve our common goal of reducing the burden of unwanted e-mail on consumers and Internet service providers, and I thank you for allowing me the opportunity to testify today.

Senator BURNS. Just, you know, not only I think are we interested in protecting the ability of legitimate commercial entities. I guess financial institutions come to mind that sometimes they use e-mail to inform their clients and customers of changes and updates in company policies. These are actually mandated by law. Would your bill affect their ability to do that in any way?

Mr. GOODLATTE. Absolutely not. This is designed to facilitate the ease with which businesses do that. Now, there are some concerns raised about other legislation and while I am very supportive of the efforts to push forward in that area with that legislation, I do think there is some fine tuning that needs to be done so that companies can effectively communicate with their customers, policyholders and so on without fear of violating the law.

Senator BURNS. Well, we thank you for your statement today. We appreciate that very much. I understand you have been spammed, and I think we all have or whatever. I was back in 1955 in the United States Marine Corps, but—those, that is water under the bridge.

Mr. GOODLATTE. It is great.

[The prepared statement of Mr. Goodlatte follows:]

PREPARED STATEMENT OF HON. BOB GOODLATTE,
U.S. REPRESENTATIVE FROM VIRGINIA

Thank you, Mr. Chairman, for holding this very important hearing. I appreciate the opportunity to appear before the Subcommittee to testify about the need for legislation to address the growing problem of mass unsolicited e-mail, also known as "spam."

The Internet is a revolutionary tool that dramatically affects the way we communicate, conduct business, and access information. Electronic-mail has become a powerful medium for commerce and communication by offering an affordable way for people to reach one another with rapid speed and reliable delivery.

Marketers have learned to take advantage of this new capability to reach consumers. Many consumers choose to communicate via e-mail with their financial in-

stitutions, favorite retailers and other companies with which they form relationships. Millions of individuals and businesses opt to receive communications and notices by e-mail. In order for the Internet to continue to thrive and grow as a medium for commerce, legitimate businesses must be able to responsibly communicate with their customers or consumers who wish to do so.

However, unsolicited e-mail, especially commercial e-mail such as advertisements, solicitations or chain letters, has become the 'junk mail' of the information age. Jupiter Communications reported that in 1999 the average consumer received 40 pieces of spam. By 2005, Jupiter estimates that the total is likely to soar to 1,600 pieces of spam. These numbers are truly astounding. While it costs the spammer almost nothing to send, unsolicited e-mail messages burden consumers by slowing down their e-mail connections, and cause big problems for the small business owner who is trying to compete with larger companies and larger servers.

Even more disturbing are the numerous examples that I receive from my own constituents of the increasing amount of spam that is pornographic in nature. This pornographic spam, opened innocently by the recipient, often disguises the subject of the e-mail and includes a link that takes the recipient to a pornographic web site. E-commerce will never reach its full potential if consumers and their children cannot utilize e-mail without the fear of being unwillingly transported into the seamier side of the Internet.

Consumers are not the only ones victimized by spam. In recent instances, unsolicited e-mail transmissions have paralyzed small Internet Service Providers (ISPs) by flooding their servers with unwanted e-mail. Excessive e-mail tie up network bandwidth and monopolize staff resources. This has the potential to do great damage to small ISP companies and the communities they serve.

Currently, ISPs are developing programs that require the individual sending the unsolicited message to include a valid e-mail address, which can then be replied to in order to request that no further transmissions be sent. Under these programs, once the individual sending the original e-mail receives a request to remove an address from their distribution list, they are required to do so. However, offending spammers get around this requirement by using the e-mail address of an unsuspecting user to spam others.

To address the problem of fraudulent unsolicited e-mail, I have introduced legislation in the House to give law enforcement the tools they need to prosecute individuals who send unsolicited e-mail that clog up consumers' in-boxes: H.R. 1017, the Anti-Spamming Act of 2001.

The Anti-Spamming Act would amend the criminal code to address fraudulent unsolicited electronic mail. It would add to the substantive conduct already prohibited under the law, by prohibiting both the intentional and unauthorized sending of unsolicited e-mail that is known by the sender to contain information that falsely identifies the source or routing information of the e-mail.

This legislation would subject those who commit such prohibited conduct to a criminal fine equal to $15,000 per violation or $10 per message per violation, whichever is greater, plus the actual monetary loss suffered by victims of the conduct. In addition, prohibited conduct that results in damage to a "protected computer" would be punishable by a fine under Title 18 or by imprisonment for up to one year.

I commend you, Chairman Burns, on the introduction of your own spam legislation which takes a balanced approach to combating spam by including strong monetary penalties, but does not include a private right of action, an area in which we should proceed with caution in that it could have the effect of discouraging the use of electronic commerce.

Because of the complexity surrounding all e-commerce issues like spam, legislation must be carefully balanced to ensure that enforcement mechanisms address real harms without causing damage to the unique advantages provided by the Internet. S. 630 provides law enforcement with the tools they need to combat spam without opening the floodgates to frivolous litigation.

Legislation addressing the problem of unsolicited commercial e-mail is greatly needed during this legislative session to protect consumers and Internet Service Providers from victimization by spam. I look forward to continuing to work with Representative Heather Wilson and others in the House as well as with you, Chairman Burns, here in the Senate to achieve our common goal of reducing the burden of unwanted e-mail on consumers and Internet Service Providers.

Again, I thank you Mr. Chairman for allowing me the opportunity to testify today and for your continuing efforts to curb spam.

Senator BURNS. Senator Wyden.

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

Senator WYDEN. Thank you, Mr. Chairman. It is good to have our friend Bob Goodlatte, who I have had a chance to work with often over the years and I think you know Senator Burns and I have been prosecuting this cause, like you have, for a number of years, and that our bill really tracks your thinking, I think, very closely. I thought we were going to get it passed last session. We didn't quite get it there.

I am curious in terms of the House, what is taking place in terms of trying to reconcile the approach that Senator Burns and I have, which you are also very interested in with the Wilson bill and what is the progress of discussions in the House to get that done?

Mr. GOODLATTE. Well, I think there is a lot of open-mindedness on the part of Congresswoman Wilson, and myself and others on the two Committees, the Commerce Committee and the Judiciary Committee, which have jurisdiction over this issue. The Commerce Committee has passed her bill out of the Committee. The Judiciary Committee is on a 60-day secondary referral of her bill, and it also has my bill before it because my bill is primarily focused on Title 18, which is the jurisdiction of the Judiciary Committee.

So it is my hope that in the very near future, we are going to come up with a bill that is agreeable to all sides because I think the differences that divide us are not that great. The private right of action is certainly the biggest thing that we have got to work out.

Senator WYDEN. We will be working closely with you. It just seems to me what CAN-Spam has been trying to get done, what you have been trying to do is to set out some rules that if you want to send unsolicited marketing e-mail, you have got to play by a set of principles, rules that allow consumers to see where the messages are coming from and to tell the sender to stop.

So this is ultimately about consumer empowerment and Senator Burns and I have made that point again and again. We are not interested in interfering with the legitimate e-commerce, the core business activities that are so important in the digital economy, so we will be working with you.

Good luck with negotiations because those are essentially the same sort of talks we are having here, and hopefully, we can all hit pay dirt quickly and get this bill on the way to the President.

Mr. GOODLATTE. Well, I appreciate that, Senator. We look forward to working with you as well, and you are right, commercial e-mails have great potential value to people who want to receive them and we don't want to interfere with that but we do want to have the abusers live by the rules of the road, and that is basically what this is about and giving law enforcement some more tools and Internet service providers some more tools to combat that I think are important.

Senator BURNS. Senator Allen.

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

Senator ALLEN. Thank you, Mr. Chairman, and let me commend you, Mr. Chairman, for your leadership on this matter. I am very

pleased to be a co-sponsor of S. 630 and I associate myself with the bill and the comments from the Senator from Oregon, Mr. Wyden, and it is good to see my good friend from Virginia, Congressman Bob Goodlatte, who is a leader on technology in matters on the House side, and it is important that we all work together on this, and I think this House Resolution 1017 is the closest House companion to your measure in my brief review of the key provisions in the various measures in the House versus your measure.

Now, unsolicited commercial e-mail or spam has been a consumer issue for a long time. I thought it only was around since the 1980's, but since you were getting spammed you said in 1950's, I guess you might have——

Mr. GOODLATTE. I think his had pineapple on it, though.

Senator ALLEN. Pineapple with some bread around it, or maybe he invented the Internet.

Senator BURNS. The first CAN-Spam.

Senator ALLEN. They probably didn't bother to take it out of the can if they were throwing it at you because otherwise it wouldn't have any great effect, but nevertheless, the modern term of spamming is an aggravation. I think anybody who has the Internet has been spammed to one extent or another, and it is so aggravating. You log on to your e-mail account and it says you have got mail and of course what you have gotten mail from is some person or entity you have no idea who they are trying to sell you something that you don't want.

And then you, of course, have done that after wasting time opening up this irrelevant attachment and also usually, not usually, but a great number of times they say you have Hot Mail, they are saying your account size is too large, and if you do not delete things, they are going, do they give you a list of all the things that you are going to delete? Usually things that you would actually want to have kept in there. Some of them you would almost wish they would delete some of these others.

There is always e-mail from your brother or a friend that you would like to keep just for your archives but at any rate, apart from the annoyance of having to delete the piles of unwanted solicitation, Spamming can and does create a lot of problems, cause problems for servers and networks throughout the country. It is also a waste of time. It is a waste of our time at home and it is a waste of time in our offices.

The nation—in our nation, our capacity for electronic mail is not unlimited. It is not limitless. That is why you say your account sizes are too large and why it does slow down certain networks.

The best example or the worst example from my experience is right here in the U.S. Senate, where e-mail is often delivered late or maybe not at all due to heavy e-mail traffic and its impact on the Senate server, so right here that is the situation. Now, I know the Senate is not unique. And maybe not quite as up to date as some law firms and folks in the private sector, but that happens in the private sector as well where because of these unsolicited, unwanted commercial e-mails it is slowing down productivity in the office, in the businesses, especially a pain for small businesses, and obviously what you have is people wasting time which is wasting

lost productivity and you are wasting the capacity, the capacity with these unsolicited junk mails.

Now, for these reasons, these are the reasons and I think it is a very balanced approach that the Chairman has taken here on this measure. I chose to co-sponsor what you call the CAN-Spam Act and our esteemed Chairman is obviously fighting a good battle, and here are the key things that that Act will do if we pass it in the Senate and in the House.

It will force spammers to act honestly. Now, who could be against that? If you send an unsolicited commercial e-mail you must include true and accurate contact information so consumers can opt-out and stay out. One of the frustrating aspects of this as I said, well, if you don't want any more e-mails or any more solicitations, please click such and such and fill out your information and we won't send it to you any longer. Well, in researching this, that is exactly what they want you to do so then they know hey, this is a live e-mail address so now we can continue pestering that person so it is very aggravating to even have to fill all that stuff out in the first place, and it is particularly annoying if it is actually counterproductive.

Second, this CAN-Spam Act will stop the practice of collecting e-mails for the sole purpose of spamming or so-called spotter programs. It will also add enforcement to these provisions to help ensure that an effective deterrent includes severe penalties under the law and I think the legal approaches you are taking is the right approach and very balanced and really, that is the point.

This CAN-Spam Bill seeks to balance the interest of Internet consumers with the interests of legitimate e-commerce businesses seeking to utilize online opportunities. I am one who very much likes people to be completely without a lot of regulations, a lot of limits. I very much dislike limits. Nevertheless, you should have honesty. You do need to have consumers informed and people in their own homes ought to be able to control to the best they can what is coming in and clogging up and pestering them on their Internet.

And indeed by way of analogy in 1991, the Telephone Consumer Protection Act by law stopped unsolicited junk fax advertising, so in my view by analogy if we can protect fax machines, why not computers as well?

So again, Mr. Chairman, I am very happy that you are having this, this hearing. I think you will have a lot of support from people all across America, and I look forward to working with you, Mr. Chairman and other Members, Senator Wyden and others to effectuate a good common sense approach with good balances on privacy, on commerce, but also make sure there is honesty and recourse for people who don't care to be pestered, annoyed or have their e-mail mailbox clogged up. Thank you.

Senator BURNS. Thank you, Senator. Any more statements? We are going to have our next panel come forward if we could.

Mr. Jerry Cerasale, Senior Vice President of Government Affairs, Direct Marketing Association. Mr. Jeremiah S. Buckley, General Counsel, Electronic Financial Services Council here in town. David Moore, President and CEO of 24/7 Media. And Jason Catlett, President and founder, Junkbusters and Harris Pogust of Sherman, Sil-

verstein, Kohl, Rose and Podolsky from New Jersey and David McClure. All make their way to the table and we'll start this discussion.

It should be a lively one, and if you could keep your statements to 5 minutes or so or less, if you possibly can, I know you can't limit these Senators. I'll guarantee you that. They get started and then we'll have a few questions. Mr. Cerasale. Thank you for coming today.

STATEMENT OF JERRY CERASALE, SENIOR VICE PRESIDENT, GOVERNMENT AFFAIRS, THE DIRECT MARKETING ASSOCIATION INC.

Mr. CERASALE. Thank you very much, Senator Burns, and I appreciate the opportunity to be here. I am Jerry Cerasale from the Direct Marketing Association and I ask that my written statement be included in the record.

Senator BURNS. All of your full statements will be made part of the record today.

Mr. CERASALE. Thank you very much. I want to first start out by thanking you and Senator Wyden and your staffs for putting together this bill, S. 630. We think you put a lot of thought into it, and we think that it is an excellent starting point.

Let me start with what the DMA is. It has been around since 1917. How we look at the Internet. The Internet is basically another medium, another way to try and reach customers and reach potential customers, so as we look at it, let's, I want to raise where the DMA guidelines have been for all marketing that our members must use.

The first thing that you have to do is you don't lie. You tell people who you are. And I think your bill does that.

You tell people that you are trying to sell them something, and that is also in your bill. If consumers tell you I don't want to hear any more from you, you have to honor that. That is also in S. 630.

And we have gone a little farther at the DMA way back starting in 1972. We had a mail preference service for people who didn't want to receive mail. In 1985, we began a telephone preference service for people who don't want to receive telephone calls and in 2000, we began an e-mail preference service for people who do not want to receive unsolicited e-mail. Our members must use those three services if they happen to use those medium or those media to reach consumers.

And so we have a situation where the Direct Marketing Association members believe and use an opportunity for individuals to say I don't want to receive further solicitation. So we think that the basic premises, we think. We know the basic premise in S. 630 is right along the lines of where the DMA has been for a long, long time and we applaud you for that.

We specifically also believe in a strong federal standard. This is a borderless communications medium, and we think that a strong federal standard is what makes sense and having the FTC enforce that is an excellent idea, along with allowing the state's attorneys general a role to support in either federal or state court to enforce this bill as well. We think that the strong penalties for fraud are very important.

One of the things that happens, especially in an emerging medium, as Eileen Harrington said, is that get rich quick schemes are probably the first to try and reach and use the medium, and we think that anti-fraud devices are very, very important to try and protect confidence in the medium, so we support that.

We think that in looking at enforcement, the idea of an opt-out in every commercial e-mail message makes sense. The idea of saying who you are, the idea of not lying in the headers or in the subject line is very, very important.

We believe that your bill also protects permission-based marketing, which we think is an emerging response to consumer needs and desires on the Internet. We do have some areas where we think we can tweak that a little bit and we'll gladly be working with your staffs on that to keep permission-based marketing open and free to consumers. The Internet is important. It is a new medium. It is not the answer. It is not going to eliminate other forms of marketing. It has to be integrated within the American economy and system. It can help strengthen the economy. We think marketers have to learn to use it and keep their practices and the principles the same regardless of medium. We think this bill goes along in that way, and we appreciate all your efforts in this endeavor, and I am happy to answer any questions you may have.

[The prepared statement of Mr. Cerasale follows:]

PREPARED STATEMENT OF JERRY CERASALE, SENIOR VICE PRESIDENT, GOVERNMENT AFFAIRS, THE DIRECT MARKETING ASSOCIATION INC.

I. Introduction

Good afternoon, Mr. Chairman, and thank you for the opportunity to appear before your Subcommittee as it examines unsolicited commercial electronic mail. I am Jerry Cerasale, Senior Vice President of Government Affairs for The Direct Marketing Association, Inc. ("The DMA").

The DMA is the largest trade association for businesses interested in direct, database, and interactive marketing and electronic commerce. The DMA represents more than 4,500 companies in the United States and 54 foreign nations. Founded in 1917, its members include direct marketers from 50 different industry segments, as well as the non-profit sector. Included are catalogers, financial services, book and magazine publishers, retail stores, industrial manufacturers, Internet-based businesses, and a host of other segments, as well as the service industries that support them. The DMA's leadership also extends into the Internet and electronic commerce areas through the companies that are members of The DMA's Internet Alliance and the Association for Interactive Media.

The DMA member companies, given their track record in delivering high quality goods and services to consumers, have a major stake in the success of electronic commerce, and are among those most likely to benefit immediately from its growth. The healthy development of electronic commerce depends on consumer trust. It is imperative that the e-mail communications medium earns that trust.

The DMA commends the drafters for this legislation. While it is not clear that legislation is imperative at this juncture, we support the efforts of Senators Burns and Wyden. We think that S. 630 takes the appropriate approach for legislation regarding UCE. S. 630 contains many of the elements of what successful legislation in this area should look like. We believe that the requirement that senders of unsolicited commercial electronic mail identify themselves truthfully and provide individuals the ability to opt-out of unsolicited commercial electronic mail messages is essential. Likewise, The DMA is very supportive of maintaining the ability for businesses to send messages to those individuals who have provided affirmative consent and those individuals with which a business has a pre-existing business relationship without such messages being treated as unsolicited commercial electronic mail. We also believe that providing criminal penalties for sending unsolicited commercial electronic mail that contains fraudulent routing information should prove very useful in limiting egregious unsolicited messages. We continue to have some concerns

with the definitions of "initiator" and "affirmative consent" and look forward to working with the members and staff on these issues.

There are several topics I wish to focus on in more detail in my testimony today. These are:

- The DMA's self-regulatory program the e-Mail Preference Service;
- The need for strong penalties against entities that send fraudulent messages;
- Federal Trade Commission enforcement of a uniform federal standard; and
- Permission-based communications.

The DMA welcomes this congressional inquiry into these important matters.

II. The DMA's e-Mail Preference Service Empowers Consumers With Choice Concerning Receipt Of Unsolicited Commercial E-Mail

Mr. Chairman, The DMA is a long time leader in self-regulation and peer regulation. We believe that in the borderless world of electronic commerce self-regulation with effective choice to consumers is the best means of empowering consumers regarding receipt of unsolicited commercial electronic mail, creating and maintaining opportunity for the many exciting new benefits of legitimate marketing in the interactive economy.

For this reason, since publishing our electronic commerce guidelines almost 5 years ago, we have supported an industry standard of notice and opt-out for electronic mail marketing communications. More recently, last year we created and launched the e-Mail Preference Service ("e-MPS"). The e-MPS allows individuals to remove their e-mail addresses from Internet marketing lists. This ambitious undertaking is aimed at empowering consumers to exercise choice regarding receipt of UCE, while creating opportunity for the many exciting new benefits of legitimate marketing in the interactive economy.

The e-MPS is based on The DMA's very successful Mail Preference Service ("MPS") and Telephone Preference Service ("TPS") self-regulatory initiatives. Both of these initiatives represent The DMA's response to consumers' request for choice in the amount of mail and telephone solicitations that they receive. In developing responsible marketing practices for the Internet age, we have adapted this important concept of consumer choice to the Internet medium through the development of e-MPS.

As of January 2000, consumers have been able to register for the e-MPS at a special DMA web site. Consumers can use this service, at no cost, to place their e-mail addresses on a list indicating that they do not wish to receive UCE. This service affords consumers with flexibility to determine the types of solicitations they receive. Through this service, individuals can opt-out of business-to-consumer UCE, business-to-business UCE, or all UCE.

The e-MPS is part of The DMA's "Privacy Promise to American Consumers," which became effective July 1, 1999. The Privacy Promise requires as a condition of membership in The DMA, that companies, including online businesses, follow a set of privacy protection practices. As part of this promise, all DMA members who wish to send UCE to consumers are required to remove the e-mail addresses of those consumers who have registered with the e-MPS from their lists of consumers to whom they send e-mail solicitations. Those consumers on the e-MPS list will receive no e-mail from DMA members unless they have an established online business relationship with that company. This service also is available to companies that are not members of The DMA so that they too may take advantage of this innovative service and respect the choice of those consumers who choose not to receive UCE.

III. Strong Penalties Should Exist To Combat Fraudulent Messages

The DMA is particularly sensitive to the practice of sending fraudulent electronic mail messages in which some individuals are engaged, and fully supports a prohibition on this practice. This practice includes the sending of messages with false or fictitious header information. The use of such fraudulent e-mail has no place in a healthy and robust Internet. The sending of bulk fraudulent messages has crashed the networks of Internet service providers.

In addition to deceiving consumers, fraudulent e-mail diminishes the reputation of the entire medium, particularly messages sent from the responsible marketers that make up our membership. Ultimately, we believe the sending of fraudulent messages is an area in which legislation is critical, as it is more difficult to prevent fraudulent messages.

IV. Sending Of Commercial Messages When Consumer Permission From The Consumer Exists Should Be Outside The Scope Of Any Legislation

Consumers often give permission to a company, or request that it pass along their e-mail address to receive information and offers from other service providers in a given category, such as financial services. These consumers have requested information and granted permission, but it may not be specific to a particular initiator. For example, I might indicate that I would like to receive mailings on sales of men's clothing. A variety of different businesses could then send me messages when they have sales at their stores. Such marketing is very beneficial to consumers and to the free flow of commerce. Any legislation should allow such communications. It would burden the free flow of information to such consumers to require that they give specific permission to each "initiator."

V. Any Legislation Should Provide Enforcement Of A Uniform Federal Standard

The DMA supports the approach taken in the legislation that preempts state law by providing a uniform federal standard. Strong preemption is the appropriate approach in the electronic environment. Differing state regulatory standards for communicating via electronic mail could have the effect of eliminating the inherently global characteristics of the communications, which are in large part responsible for its extraordinary success. It would be impossible for businesses to comply simultaneously with different and potentially inconsistent laws in multiple jurisdictions where individuals to whom they send messages may be located. Often, the business is unaware of the location of the recipient of the message. If businesses were required to comply with the different laws of the 50 states, it would be a tremendous burden on the Internet and could have the result of limiting business offerings. Moreover, a patchwork of state laws, particularly as they affect interstate communications, may ultimately be found unconstitutional.

Likewise, we are heartened by the decision not to create a private right of action. Creating a private cause of action would impose substantial burdens on ISPs, resulting in the expenditure of resources both in terms of time and money to defend litigation. Such an approach is unnecessary in light of the fact that the FTC would be empowered to protect consumer rights. Inclusion of a consumer cause of action would create a very substantial bounty for class action lawyers that would produce very substantial damage awards wholly unrelated to the costs imposed by UCE. The legislation must foreclose the possibility of class actions.

VI. Conclusion

We thank the Members of Congress who have introduced legislation in this area for their thoughtful consideration of such an important issue. We also thank the Chairman and the Subcommittee for the opportunity to express the views of The DMA. We know that Congress and this Subcommittee will continue to monitor this issue closely and we look forward to working with you.

Senator BURNS. Thank you very much. Jeremiah Buckley, General Counsel, Electronic Financial Services Council. Thank you for coming today.

STATEMENT OF JEREMIAH S. BUCKLEY, JR., GENERAL COUNSEL, ELECTRONIC FINANCIAL SERVICES COUNCIL

Mr. BUCKLEY. Thank you very much, Mr. Chairman. My name is Jeremiah Buckley, and I am a partner in the Washington office of Goodwin, Procter. I serve as general counsel of the Electronic Financial Services Council, which is an association of technology companies and financial services firms interested in promoting the electronic delivery of financial services. We are pleased to be here and have an opportunity to comment on S. 630.

Thinking back to the passage of the E-Sign Act last year, we know this Committee and its staff appreciates the importance of federal legislation in promoting e-commerce.

We have enjoyed working with you, Senator Burns, and with you, Senator Wyden, in the past, and we look forward to working with you to make this an excellent piece of legislation. We support

the fundamental premise of S. 630, that is that offensive, fraudulent or otherwise harmful UCEs should be prohibited and that consumers should have the ability to control the flow of their e-mail traffic. Achieving these goals is an important step toward assuring that consumers feel comfortable doing business in the electronic medium, a goal that we all share.

We believe that the UCE legislation should fit into the framework created by previous e-commerce legislation. Congress has repeatedly endorsed the vision of e-commerce as a national resource. The E-Sign Act recognizes that the Internet is a borderless medium for which it is desirable to have uniform federal rules. S. 630 recognizes that legal uniformity is an important part of e-commerce. It includes a provision in Section 7(b) preempting inconsistent state law.

This preemption provision, however, does contain a number of exceptions. In particular, it does not apply to any state trespass, contract or tort law. These types of exceptions, we would caution the Committee, do run the risk of swallowing up the preemption itself. If S. 630 is to fashion a uniform national standard for dealing with spam, it should occupy the field. It should not leave room for the development of a patchwork of legislative and judicial pronouncements at the state level creating a compliance jigsaw puzzle which only the most sophisticated players can solve.

Having established that uniform standard, we believe it is appropriate that federal agencies be the ones assigned the responsibility for enforcement policy, and it seems to us this is best because in the course of enforcement, the policies that Congress has articulated will be fleshed out, and we think it is best that agencies which are under the jurisdiction and direction of the Congress have the responsibility for establishing that enforcement policy. States would, of course, continue to have the authority to adopt uniform unfair deceptive acts and practices legislation, as they do now, and under those statutes, they could declare that violations of the provisions of S. 630 constitute violations of state law. If they do, they could also assign to their state attorney general, to private parties, or to other agencies within the state the responsibility for enforcement of their state law.

But we think it is wise to keep a demarcation between federal law and state law, between federal enforcement and state enforcement, and we think it is respectful of the legislatures in the states to allow them to establish who will enforce the law within their states.

Now let me turn to an issue that legislation does not address, but which we think is vital, preserving the reliability of e-mail communications. Last year's E-Sign Act was a vote of confidence by the Congress in the predictability and reliability of electronic communications. E-Sign would envision that individuals and businesses would be able to contract and conduct their ongoing business electronically.

In the nonelectronic world, a third party cannot arbitrarily disrupt contractual arrangements between parties, and E-Sign envisions that this would not happen in the e-commerce world either. However, we are concerned about reports that ISPs in their eagerness to help their subscribers avoid receiving unwanted UCEs may

block, in fact, there is evidence that they are blocking, e-mails that subscribers not only want but have specifically contracted to receive as a part of the electronic business relationship created pursuant to E-Sign or prior legislation.

This will have a significant negative impact on the potential growth of electronic delivery of financial services and other relationships with e-commerce. S. 630 currently does nothing to prevent this from happening. It is in the interest of all who seek to promote e-commerce to preserve the sanctity of electronic contracts. If the electronic message, which is not a UCE, and is not going to be delivered, at a minimum both the sender and the recipient should be notified by the ISP. We hope to work with the ISPs and with your Committee as appropriate to develop standards to assure reliable delivery of permission-based electronic communications, and we believe this is a goal that is complementary to and as important as getting rid of spam.

Certain provisions of your legislation could, as we say in our written testimony, benefit from clarification. If time permitted, I would go into those, and I would be happy to answer questions. We are very pleased to have had the opportunity to comment on this legislation and look forward to working as we have in the past with the Committee staff and with you Senators to perfect this bill.

Senator BURNS. We are looking forward to working with you also. And we like the idea of bringing specifics to the table, because that is the way we solve some of the problems as this legislation moves along.

[The prepared statement of Mr. Buckley follows:]

PREPARED STATEMENT OF JEREMIAH S. BUCKLEY, JR., GENERAL COUNSEL, ELECTRONIC FINANCIAL SERVICES COUNCIL

My name is Jeremiah S. Buckley. I am a partner in the Washington office of the law firm of Goodwin Procter, and I serve as general counsel to the Electronic Financial Services Council. The EFSC is an association of technology companies and financial service providers dedicated to promoting the availability and delivery of financial services through electronic commerce. Given this mission, the EFSC is intensely interested in federal legislative developments that could have an effect on e-commerce. For this reason, we are pleased to have the opportunity to comment this afternoon on S. 630, the CAN-spam Act of 2001.

The EFSC recognizes that federal legislation is not merely helpful, but sometimes necessary to resolve legal uncertainties and unleash the economic potential inherent in our new e-commerce environment. Thinking back to the passage last year of the Electronic Signatures in Global and National Commerce Act ("E-Sign"), we know that this Committee shares our belief in the benefits of appropriate legislation. We have enjoyed working with Senators Burns and Wyden in the past, and we look forward to working with the Committee and its staff once again in dealing with the very significant issue of unsolicited commercial electronic mail ("UCE").

We agree with the fundamental premise underlying S. 630—that consumers should be protected from misleading, offensive, fraudulent or otherwise harmful UCEs, and that the ability of consumers to control the flow of their e-mail traffic should be respected. Achieving these goals is an important step in assuring that consumers feel comfortable using the electronic medium as a preferred way of doing business, a goal we all share.

UCE Legislation Should Fit Into the Framework Created by Previous E-Commerce Legislation

Congress has repeatedly endorsed a vision of e-commerce as a national resource. Last year's passage of E-Sign legislation established the parity of electronic and non-electronic communications under federal law. E-Sign recognized that the Internet is a borderless medium, for which federal regulation and uniform federal standards are appropriate. Our specific comments reflect our strong support for this vi-

sion of e-commerce as a national resource appropriately subject to a set of uniform national rules designed to encourage the development of e-commerce to its fullest potential.

S. 630 recognizes that legal uniformity is important to e-commerce, and for that reason it includes a provision—Section 7(b)—preempting inconsistent state laws. The preemption provision, however, has a number of exceptions: in particular, it does not apply to any state trespass, contract or tort law. This type of exception, we would caution the Committee, runs the risk of swallowing the preemption provision itself. If S. 630 is to fashion a uniform national standard for dealing with spam, it should occupy the field. S. 630 should not leave room for the development of a patchwork of state legislative or judicial pronouncements using tort or trespass theories to create a compliance jigsaw puzzle which only the most sophisticated players can solve.

Having established a uniform federal standard, we believe that the appropriate course is to assign to federal agencies the responsibility for enforcing that standard. To the extent that enforcement policy shapes or clarifies the meaning of the provisions of S. 630, it seems to us best to leave that power with agencies which are subject to the jurisdiction and direction of Congress. State attorneys general and private parties should not be assigned enforcement responsibilities in this area as a matter of federal law.

While the authority of a state to enact legislation inconsistent with S. 630 would be preempted, states would, of course, continue to have the power to enact unfair and deceptive acts and practices ("UDAP") statutes, or interpret their current UDAP statutes, so as to define violations of S. 630 as unfair and deceptive practices under state law. In this context, the states would be free to assign enforcement responsibilities for their UDAP statutes to their state attorneys general or such other agencies or private parties as they deem appropriate. It seems to us that this course of action has the advantage of providing a clear line of demarcation between state and federal law and is more respectful of the right of state legislatures to determine how state law will be enforced within a state's boundaries.

Need for Clear Definitions

Section 5(a)(5)(A) of S. 630 requires that a UCE contain a "clear and conspicuous . . . identification that the message is an advertisement or solicitation." Because of the centrality of this requirement to the purposes of S. 630, we believe that the Committee should consider a more precise definition of what constitutes clear and conspicuous identification. It might be worthwhile for the Committee to consider creating a standard indentifier to appear in the e-mail subject line, to serve as a universal signal that the e-mail is an advertisement. This requirement could then be included in the legislation itself, or provided as an example in the Committee's report. In the absence of such clear guidance, senders of UCEs will be left uncertain as to the efficacy of their compliance efforts.

Likewise, we would counsel against the use of undefined terms, such as "primarily" to determine the amount of advertising content that defines a "commercial electronic mail message." If, in a communication relating to a transaction with its customers, a firm includes an electronic "statement stuffer" alerting the customer to other products or features available to the customer, S. 630 does not establish how much such material will render the communication "primarily" advertising. We would recommend that, to avoid this problem, any communication related to a transaction or relationship with an existing customer be excluded from the definition of a "commercial electronic mail message."

Preserving the Reliability of E-Mail Communications

Last year's E-Sign Act was a vote of confidence by the Congress in the predictability and reliability of electronic communications. E-Sign envisions that individuals and businesses will be able to contract freely through electronic media, without having to worry about the enforceability of contracts that they enter into electronically. It also envisions that business will continue to be conducted electronically after the initial contracts have been signed, with records being freely transmitted in fully electronic relationships if the parties so desire. In the non-electronic world a third party cannot arbitrarily disrupt a contractual arrangement between two parties, and E-Sign envisions that this should not be able to happen in e-commerce either. However, we are concerned about reports that ISPs, in their eagerness to help their subscribers avoid receiving unwanted UCEs, may block e-mails that the subscribers not only want, but have specifically contracted to receive as part of an electronic business relationship. This result would have a significant negative impact on the potential growth of electronic delivery of financial services. S. 630 does nothing to prevent this from happening, and does not even require ISPs to give notice

to consumers they intend to block, or that they have blocked, the transmission of e-mail either in general or from particular senders.

It is in the interest of all who seek to promote e-commerce to preserve the sanctity of electronic contracts. If an electronic message which is not a UCE is not going to be delivered, at a minimum both the sender and the recipient should be notified by the ISP. We hope to work with ISPs and with your Committee, as appropriate, to develop standards that assure reliable delivery of permission-based electronic communications.

We appreciate the opportunity to share our views on S. 630 and the willingness of the sponsors of this legislation and their staffs to work with us and others to assure that the CAN-spam legislation will create clear and workable standards to regulate the transmission of UCEs.

Senator BURNS. Mr. David Moore, President and CEO of 24/7 Media. New York.

STATEMENT OF DAVID MOORE, PRESIDENT/CEO, 24/7 MEDIA

Mr. MOORE. Good afternoon. I am David Moore. I am the CEO of 24/7 Media, and I'd like to thank Chairman Burns, the Ranking Member, Senator Hollings, Senator Wyden, and Members of the Committee for inviting 24/7 Media to participate today.

I would like to begin by commending Senators Burns and Wyden for their leadership in crafting the Unsolicited Commercial E-mail Act of 2001. This bill represents a responsible, common-sense approach to establishing standards for commercial e-mail practices and is an important first step in helping to protect consumers and legitimate marketers from the abuses of spammers.

As a leading provider of online marketing and advertising solutions and services, 24/7 Media's clients have included such notable businesses as Reuters, The Economist, USA Today, American Express, Law.com, MSNBC, General Motors, Verizon, AT&T, and The Financial Times, to name a view. We provide a valuable service to consumers by delivering content that they have requested, such as news, newsletters, real-time stock quotes, and other information.

The success of the interactive industry lies in the confidence of the relationship among content publishers, service providers, marketers, advertisers, and consumers. We support permission-based communications that empower consumers with notice and choice.

The interactive marketing industry has been tainted by the actions of disreputable marketers who use deceptive practices in sending unsolicited commercial electronic e-mail. These marketers, or spammers, should not be allowed to infringe upon or negatively influence the need for legitimate commerce to prosper in the online world. The Committee and Congress should focus on legislation this year that specifically addresses the problem of fraudulent, misleading, forged, and inaccurate e-mail communications. These practices are an encroachment on the rights and privacy of consumers.

24/7 Media, along with other companies, has worked diligently over the past year to establish and to put into effect guidelines and practices that will enable the Internet to prosper as the world's leading communication, educational, and information tool.

24/7 Media has an interest in minimizing spam. We maintain one of the largest, permission-based e-mail databases and generate a significant portion of our revenue from list management and brokerage, as well as from our e-mail service bureau, 24/7 Exactis. We

recognize that respecting the privacy rights of consumers will help us sustain our long-term business model.

Let me tell you more specifically how we conduct our business. We don't spam. We don't allow our clients to spam. We include a functioning return e-mail address in all e-mail deliveries. We don't use deceptive subject headings. We always provide clear and conspicuous notice for consumers to opt-out. We don't do business with any business that distributes pornography.

I am proud to say that 24/7 Media's level of accuracy in delivering the appropriate content to the consumer is exceptional. During a 6-month period last year, 24/7 Exactis received 1 complaint for every 16,000 e-mails delivered. That is .000625 percent. Most client lists in fact generated no complaints at all. We also found that in most instances, if there was a complaint, the complaint was resolved soon after the subscriber was reminded of how the marketer obtained their e-mail address.

From 24/7 Media's point of view, the Burns-Wyden bill appropriately focuses on e-mail abuse. These spammers devalue our own efforts and weaken the consumer confidence that is so important for all online businesses to succeed and flourish. We also believe that enforcement mechanisms should deter spammers from encroaching on the privacy of consumers and not penalize legitimate markets who are adhering to the standards.

In announcing the introduction of this bill on March 27th, Chairman Burns said, for many people, spam is ruining their online experience and their ability to use e-mail. It is high time for Congress to act to protect consumers from overzealous marketers. I agree with that sentiment, and I invite the rest of our industry to stand behind this effort to support responsible practices and continue to provide value to the consumer. Mr. Chairman and the Committee, I thank you again for the opportunity to participate in today's hearing. This is a complex policy challenge that must accommodate evolving technologies and business models. We look forward to working with you to fine tune this legislation. 24/7 Media remains committed to engaging lawmakers on key policy issues and recognizes that regulation of commercial e-mail practices is only one of many key decisions this Committee will have to sort through in the future.

We look forward to continuing to work with you and to be a resource to you as you consider Internet-related policy and work toward our common objective of protecting the rights and privacy of all consumers while at the same time ensuring the long-term viability of the Internet and legitimate web-related businesses. Again, thank you for your time and I look forward to your questions.

Senator BURNS. Thank you very much. We appreciate your testimony here today, Mr. Moore. What is it 24/7 Media covers 24 hours a day, 7 days a week?

Mr. MOORE. We are always in business.

Senator BURNS. Always in business. You know, up in Montana, you know, on the shield of the state patrol is 3–7–77, 3-day, 7-day, 77. We don't know what that stands for. But I will tell you this. It is not a bad idea. That was the number the vigilantes used years ago before we were a state. We were a territory, vigilantes made the law and if you came home and that number was written on

your door, you had 24 hours to shuffle along. You know. And they weren't kidding either. They were pretty serious about it. Thank you for coming today.

[The prepared statement of Mr. Moore follows:]

PREPARED STATEMENT OF DAVID MOORE, PRESIDENT/CEO, 24/7 MEDIA

Good Afternoon, I am David Moore, CEO of 24/7 Media.

I'd like to thank Chairman Burns and the Ranking Member, Senator Hollings and Members of the Committee for inviting 24/7 Media to participate today and would like to begin by commending Senators Burns and Wyden for their leadership in crafting the "Unsolicited Commercial E-mail Act of 2001". This bill represents a responsible, common-sense approach to establishing standards for commercial e-mail practices and is an important first step in helping to protect consumers and legitimate marketers from the abuses of spammers.

As a leading provider of online marketing and advertising solutions and services, 24/7 Media's clients have included such notable businesses as Reuters, The Economist, USA Today, American Express, Law.com, MSNBC, General Motors, Verizon, AT&T, The Financial Times, and Disney to name a few. We provide a valuable service to consumers by delivering content they have requested such as news, real-time stock quotes, and other information.

The success of the interactive industry lies in the confidence of the relationship among content publishers, service providers, marketers, advertisers, and consumers. We support "permission-based" communications that empower consumers with notice and choice.

The interactive marketing industry has been tainted by the actions of disreputable marketers who use deceptive practices in sending unsolicited commercial electronic mail. These marketers, or spammers, should not be allowed to infringe upon or negatively influence the need for legitimate commerce to prosper in the online world. The Committee and Congress should focus on legislation this year that especially addresses the problem of fraudulent, misleading, forged and inaccurate e-mail communications. These practices are an encroachment on the rights and privacy of consumers.

24/7 Media, along with other companies, has worked diligently over the past year to establish and put into effect guidelines and practices that will enable the Internet to prosper as the world's leading communication, educational and information tool.

24/7 Media has an interest in minimizing spam. We maintain one of the largest, permission-based e-mail databases and generate a significant portion of our revenue from list management and brokerage as well as from our e-mail service bureau, 24/7 Exactis. We recognize that respecting the privacy rights of consumers will help sustain our long-term business model.

Let me tell you more specifically how we conduct our business:

We don't spam.
We don't allow our clients to spam.
We include a functioning return e-mail address in all e-mail deliveries.
We don't use deceptive subject headings.
We always provide clear and conspicuous notice for consumers to opt-out.
We don't do business with any business that distributes pornography.

I am proud to say that 24/7 Media's level of accuracy in delivering the appropriate content to the consumer is exceptional. During a 6 month period last year, 24/7 Exactis received 1 complaint for every 16,000 e-mails delivered. Most client lists, in fact, generated no complaints at all. We also found that in most instances, if there was a complaint, the complaint was resolved soon after the subscriber was reminded of how the marketer obtained their e-mail address.

From 24/7 Media's point-of-view, the Burns-Wyden bill appropriately focuses on e-mail abuse. These spammers devalue our own efforts and weaken the consumer confidence that is so important for all online businesses to succeed and flourish. We also believe that enforcement mechanisms should deter spammers from encroaching on the privacy of consumers and not penalize legitimate marketers who are adhering to the standards.

In announcing the introduction of this bill on March 27, Senator Wyden said: ". . . Spam could have a significant negative impact on how consumers use Internet Services and e-commerce. This legislation strikes at unscrupulous individuals who use e-mail to annoy and mislead". I agree with that sentiment and I invite the rest of our industry to stand behind this effort to "strike out at the unscrupulous", support best industry practices and continue to provide value to the consumer.

Mr. Chairman and the Committee, I thank you again for the opportunity to participate in today's hearing. This is a complex policy challenge that must accommodate evolving technologies and business models. We look forward to working with you to fine-tune this legislation.

24/7 Media remains committed to engaging lawmakers on key policy issues and recognizes that regulation of commercial e-mail practices is only one of many key decisions this Committee will have to sort through in the future. We look forward to continuing to work with you and to be a resource to you as you consider Internet-related policy and work toward our common objective of protecting the rights and privacy of all consumers while at the same time ensuring the long-term viability of the Internet and legitimate web-related businesses.

Again, thank you for the time and I look forward to your questions.

Thank you.

Senator BURNS. Mr. Jason Catlett, President and CEO of Junkbusters. Yes, Junkbusters. There you go. Thank you for coming today.

STATEMENT OF JASON CATLETT,
PRESIDENT/CEO, JUNKBUSTERS CORP.

Mr. CATLETT. Thank you, Senator. And it is a pleasure to be back before you and Senator Wyden again. I'd like to begin with two issues that you raised.

First, the technology arms race that is going on between spammers and largely ISPs who are using technological means to try to abate the amount of spam from their networks before it reaches the spammer's intended recipients. That is a silent battle that goes on continuously and if it were stopped as we have heard earlier testimony suggesting a measure that might do it, this would cause an enormously greater amount of spam to reach the end consumers, so technological means for automatically spam filtering are tremendously important and do a lot of good.

However, you are absolutely correct that this is not a solution to the problem. And that ultimately it is essential to have laws to stop the attempts of the spam to be inserted into the network.

We heard from Senator Rockefeller about the question of labeling. Is it sufficient to label the material? Well, I can tell you as someone who has written scientific papers on automatic text classification that those methods are always imperfect and even if the spammers were perfectly honest in their labeling of the material, it would still impose an unacceptable burden on the network to try and reject each article after checking the appropriate label.

The second point I would like to raise is the issue of wireless spam which indeed has been a problem, particularly in Europe where the technology is at a later stage of adoption, but also in states such as Arizona, where a class action suit on that is underway.

I would like to note that trade associations with the wireless industry have come out strongly in favor of an opt-in criteria that you should never receive commercial solicitations to your cell phone unless you have deliberately requested them, and I think that is an admirable position for them to take.

I'd like to commend you on the hard work that you have done on spam over a long period of time, and I am sorry to say that in its present form, I don't think that the bill will achieve the goals that it sets out to do. I don't think it will significantly reduce the amount of junk e-mail that is sent, and that two modifications

would be necessary in order to have a spam bill that really deserves the name of CAN-spam, and those two were issues raised by Senator Rockefeller.

The first is opt-in. The appropriate criterion for e-mail solicitation is opt-in. You should only get e-mail, commercial e-mail if you ask for it, and that is what the majority of people online believe are appropriate. It is also what a large number of consumer groups believe to be appropriate, and it is also the practice as we have heard from David Moore from 24/7 Media is the common industry practice only to send e-mail to people who have asked for it.

Almost no legitimate established marketer sends unsolicited commercial e-mail because it is despised by consumers and it is actually against the terms of services of most ISPs. So the first suggestion I would have to you is to make the criterion opt-in. This has worked very well with the Telephone Consumer Protection Act as we have heard discussed for junk faxes and I think that the success of that bill should be an example to us, particularly the provision to do with my second point, which is a private right of action for consumers. The idea of a waterfall of frivolous litigation simply isn't borne out in practice under the Telephone Consumer Protection Act. There is very little litigation on junk faxes. But it is a sufficient amount to discourage businesses systematically violating the law.

The idea of not allowing consumers the opportunity to protect their interests and hoping that the ISPs, some of whom are going bankrupt, will spend additional money to go to court for their individual consumers, I think it is very naive.

The appropriate thing to do is to give individuals the means to protect their own interests, and that is being done with the junk faxes because of the same situation. This is postage due marketing.

Senator BURNS. You believe in the vigilantes, too, huh?

Mr. CATLETT. The consumers should be able to act with the authority of law in an appropriate manner. Some spams do make me want to go to the vigilante state. In fact, I would like to read you a particular spam that I picked out almost at random under a specific criterion. It is a little bit like at a hearing on locust plagues to bring along a single grasshopper and hold it up for the Committee and say this is the problem, but imagine multiplied a million times the problem. It is in the, my prepared statement, but I'll read you briefly this spam. Sex sells really works. "Why pay to belong to an adult website? When you can own your own for less than the cost of a membership. Anyone with an Internet connection can own an adult website for less than the cost of the next dinner. No experience required. Anyone can sell sex on-line in just minutes."

I'll spare you the details of how to sign up for this offer, but I'd like to draw your attention to the footer of this e-mail, which is very common. This message is sent in compliance of the new e-mail bill, section 301 paragraph (a)(2)(C) of Senate 1618. It again gives a URL for the website of your colleague, Senator Mikulski.

I would like you to imagine perhaps with your folks back at home in Montana when a mother discovers that her teenage son has received this solicitation to establish a pornographic website from the comfort of his own bedroom and then they, this person clicks through to Senator Mikulski's site and sees, this is the legis-

lation, this is in fact Mikulski's bill. It did not pass but spammers still use it and if you pass a junk e-mail bill along the lines of an opt-out, you will get exactly the same situation.

You will get the mother saying is it the policy of the United States that spammers may spam? They are going to click through to your website, then click on contact us, and you are going to get questions and letters from your constituents and I wonder how you are going to answer them.

With the current form of the Senate bill, would you have to, when the mother asks you, is it true, is what this spammer says true, that it is Okay for him to send this e-mail, would you have to answer something like yes, the spammer can send you as much e-mail as he wants until you tell him to stop, and if they don't stop, if they keep on doing it, then you can't do anything about it yourself. You have to either get your ISP to do something or you have to get the Federal Government department to do something.

Now, I don't think that is an answer that your constituents would want to hear. The answer that I think you would want to be able to give to them is something like this. The spammer is lying. My bill made spamming illegal. And it gives you the right to sue people who spam you if they break the law.

So the correct policy, I think, and I have made the two key points, is to have an opt-in policy and to have a private right of action for consumers. So the question of opt-in versus opt-out and the private right of action really comes down to if your name goes on this bill and it becomes law, do you want it associated in the spams that are sent out in this case with so much spamming?

Senator BURNS. Thank you very much. And your full statement will be made part of the record.

Mr. CATLETT. Thank you, sir.

[The prepared statement of Mr. Catlett follows:]

PREPARED STATEMENT OF JASON CATLETT, PRESIDENT/CEO, JUNKBUSTERS CORP.

My name is Jason Catlett, and I am President and CEO of Junkbusters Corp. I'm grateful for this opportunity to speak with you again.

Junkbusters is a for-profit company whose mission is to free people from unwanted commercial solicitations through media such as e-mail, physical mail, telephone, and faxes. Since our web site launched in 1996, millions of people have turned to us for information, services and software for stopping junk messages, particularly e-mail. I have worked advising government departments and legislators on e-mail and other privacy issues since 1997.

As a technologist—my Ph.D. was in Computer Science—my initial inclination years ago was towards solutions based on technology and administrative processes. But years of practical experience with large numbers of consumers have led me to believe that the essential requirement for the collective protection of privacy is strong rights for the individual. Thanks to the private right of action in the Telephone Consumer Protection Act of 1991, junk faxes are today rare compared to junk e-mail, a result achieved without any vast government bureaucracy, and with little frivolous litigation. In contrast, billions of unwanted e-mail solicitations are sent each day, vexing hundreds of millions of people who feel unable to stop it. This reduces participation in online commerce and erodes the considerable benefits that responsible e-mail marketing offers to consumers and businesses. What is needed to reverse this harm to consumer confidence in the medium is a law establishing an opt-in standard for commercial e-mail, and a private right of action for recipients and network operators. S. 630 would establish an opt-out standard and lacks a private right of action, and in my opinion would not improve the situation it addresses.

Before focusing on the specifics of spam, I would like to briefly review the unhappy recent history of online privacy more generally. In the 11 months since I appeared before you in May, the prevailing level of privacy on the Internet appears

to have lowered. (Space allows only a few brief examples, for greater detail see *http://www.junkbusters.com/testimony.html* on the Web.)

- Ever more intrusive collection technologies are being rolled out. Profiling companies are continuing development of their Consumer Profile Exchange technology without any committment to observe fair information practices in their use of it.
- Most "privacy policies" offered by companies still offer little privacy, and appear to be getting even worse, according to one longitudinal study by Enonymous.
- In September Amazon.com substantially weakened its privacy policy.
- The standards proposed by DoubleClick and a few other online advertising companies and sanctioned by the FTC in July are deplorably low.
- P3P, which has been billed by some as the pot of privacy gold at the end of the technological rainbow, is now being used by Microsoft as an excuse not to fix the default settings on its next browser that allows tens of millions of web bugs to gather click streams in volumes of billions of clicks per day.
- At a public workshop run by the Federal Trade Commission in March, the major profiling companies refused to allow people access to their own profiles, or even to provide example profiles.

With this background, and with spam as a regular reminder to consumers of the ease with which personal information can be misused and the difficulty of individual redress, few would be surprised by the conclusion that privacy concerns have severely dampened the growth of e-commerce (certainly not any Member of this Committee). Over the past year, its spectacular triple digit growth has dropped to such disappointing levels that many online merchants are struggling to break even, finding difficulty attracting investment, or filing for bankruptcy. Yesterday's Wall Street Journal reported that most U.S. households have never made a purchase online. Of consumers who place items in online shopping carts, the majority are still abandoning the transaction before checkout. Online merchants have known for years that the number one concern here is fear for privacy. Furthermore, Forrester Research has found in extensive polling that concerns about privacy are not being assuaged as people gain more years of experience online. In my own discussions with online marketers whom I know from consulting engagements or from industry conferences, spam is despised as the major cause of damage to consumer confidence and participation.

The failure to control spam is the greatest economic tragedy of the Internet age. E-mail marketing conducted in a fair, consensual manner offers enormous benefits to consumers and businesses alike, particularly to small businesses who could not afford the expense of traditional media. As e-mail marketing becomes synonymous with spam—a tragedy because this is unnecessary and avoidable—many consumers are deciding simply not to participate. The right public policy for spam, as with all privacy law, is to give people who participate rights to ensure their personal information is not used unfairly. This promotes both greater participation and better business practices.

Almost no reputable marketer routinely sends e-mail on an opt-out basis. (A few have occasionally done so in error; this is perhaps the reason some companies oppose a private right of action, which would hold them accountable for such mistakes.) It is deplorable that certain trade associations such as the Direct Marketing Association are trying to hold the door open for spamming. H. Robert Wientzen, President and CEO of the DMA addressed members at the organization's 1998 conference with the following words: "Let me begin by recognizing that bulk unsolicited commercial e-mail is not real popular with consumers. And to date, very few of you are employing it. However, we also feel that most of those who push for an opt-in-only regime have very little understanding of the incredibly negative impact it would have on the future use of e-mail as a marketing tool." The DMA continues to indulge in its fantasy of cyberspace as a world of free paper, free printing and postage-due delivery of solicitations, failing to realize that if it had its way, consumers would rebel or flee.

Opt-in is the right policy for marketing by e-mail, and is consistent with successful legislation on marketing by fax. As in the TCPA, the definition of a commercial message should of course be carefully limited to avoid any impact on non-commercial speech, such as speech about religion or politics. The opt-in approach taken in the TCPA for faxes, cellphones and 800 numbers has as its basis the fact that the recipient may incur costs for receiving the unsolicited message. This is also the case for spam, so the opt-in criterion is therefore equally appropriate. The fact that in

some situations recipients appear to incur negligible incremental costs from a specific spam does not change the fundamental fact that spam is postage-due marketing.

The TCPA's prohibition against telemarketing calls to cellular telephones is not qualified any exemption for situations such as when the carrier offers the first incoming minute free or where the subscriber has excess minutes available for the particular month. That would be as silly as a spam law that said that people whose Internet service plans include unlimited hours are disqualified from monetary damages. Nor is there any exemption in the TCPA for fax-modems where no paper is consumed, a situation closely resembling junk e-mail. Despite the fact that a spam recipient often cannot produce a specific line item from a bill relating to the spam, costs are being incurred by individuals, as well as being diffused among consumers. Of course in many situations the cost can be quantified, such as on certain usage-based tariffs, or when dialing up from a hotel room. In some cases these direct costs exceed the cost of paper for a junk fax or 15 seconds on an 800 number.

Furthermore, spam imposes a hidden tax on all Internet users by increasing network capacity requirements and requiring additional administrative costs at ISPs. I estimate this cost at around one dollar per month for the average subscriber, and billions of dollars per year including institutional buyers of network services. Because ISPs absorb this as a cost of doing business, this expense is not visible to individual consumers, but it is certainly passed on to them. An opt-in policy would reduce this spam-subsidizing tax, lower the cost of Internet access, and stimulate demand for Internet services and e-commerce.

A opt-out policy that allows each spammers one free spam is like permitting shoplifters to steal items until each store requests that they cease thieving. It imposes unfair burdens: in both cases, even people who are not directly victimized incur costs through higher prices. More than a million businesses have Internet access; if even 10 percent of them sent a single message to half of online U.S. households over a period of 5 years, the American homes would receive an average of 27 spams per day. The opt-out model is simply inappropriate and unsustainable for the Internet. If opt-out spam were to prevail, e-mail, the killer application of the Internet, would become the application that killed the Internet.

Consider an excerpt from an actual spam and imagine the reaction of a constituent in Alaska reading after downloading it via a toll call. (Of course, it's also important to remember that billions like it may have been sent to millions of people, so focusing on a single specimen is rather like examining a single dead grasshopper at a Senate hearing on locust plagues, but imagine your reaction multiplied to an appropriate scale.) Here is the spam:

SEX SELLS!!! REALLY WORKS!!!

"Why Pay To Belong To An Adult Web Site When You Can Own Your Own For Less Than The Cost Of The Membership?"

"Anyone With An Internet Connection Can Own An Adult Web Site For Less Than The Cost Of Their Next Dinner!"

"No Experience Required! Anyone Can Sell Sex Online In Just Minutes!"

[extraneous detail deleted]

This message is sent in compliance of the new e-mail bill: Section 301. Per Section 301, Paragraph (a)(2)(C) of S. 1618, *http://www.senate.gov/*~murkowski/commercialemail/

Claims of compliance such as the one at the end of this spam have become all to familiar to Internet users, and have been examined in the Wall Street Journal. A key goal of spammers is to gain an appearance of legitimacy, and many have turned to boasting their compliance even with bills that never became law. Some bills from the current congress may already have been used in this manner. The sponsors of these bills may want to consider how they will respond to irate voters who click through to their congressional web sites. When you receive a letter from a constituent angered by the solicitation sent to her teenage son to become a pornographer from the comfort of his own bedroom, how will you answer her question "Is this junk e-mail really obeying your law?" The answer will depend on the kind of bill you pass. As S. 630 stands, you would have to answer something like this: "Yes. Every spammer can send you at least one spam, and it's up to you to tell each separate spammer to stop. If they don't, you can't do anything about it yourself, you have to hope that a government agency will do something for you." Is that answer likely to please your constituents? A better answer, which you could give if you pass an amended or different bill, would be "The spammer is lying. My bill made spamming illegal, and it gives you the right to sue the spammer if they break the law."

Of course spammers are less likely to draw the attention of their victims to such a law. But if you pass a weak spam bill, the bill number and your name will surely be cited in vast numbers of junk e-mails for years to come. So when you consider the key questions of opt-in vs opt-out and whether to include a private right of action, think of these two alternatives: Do you want your name to be remembered as the lawmaker who said "spamming is wrong"? Or do you want it to become the name that launched a trillion spams?

I appreciate the opportunity to speak before you today. Now I would be pleased to answer your questions.

Senator BURNS. Mr. Harris Pogust. Looks like a law firm to me.

Mr. POGUST. That's correct, Mr. Chairman.

Senator BURNS. From New Jersey. Thank you for coming today. Thank you for joining us.

STATEMENT OF HARRIS L. POGUST, ESQ., PARTNER, SHERMAN, SILVERSTEIN, KOHL, ROSE AND PODOLSKY

Mr. POGUST. I am an attorney from Pennsauken, New Jersey. I work in a small firm which represents over 2000 small businesses in the Philadelphia and southern New Jersey area. Over the last several years, my practice has focused on technology-related issues. It is only because of the disturbing rise in spamming which has begun to cost my clients valuable time and expense that I have become involved with this issue.

I am here today, Senators, representing those small business men and women who had suffered commercial loss and other economic damages as a result of the conduct of entities that transmit thousands upon thousands of junk e-mails on a daily basis. This junk mail clogs the Internet and takes up valuable space on my clients' computer systems. Takes up valuable employee time and costs my clients hundreds and in some instances thousands of dollars a year in unnecessary and unwanted expenses.

As the Internet has grown, the problem of unsolicited e-mail has increased to the point of where it has become an intolerable burden on my clients, as well as myself. I commend you for identifying this issue as an important concern for the Subcommittee's oversight agenda, yet this is not the first time that Congress has had to address the problem associated with the introduction of new technologies in the workplace. Ten years ago when fax machines first became increasingly prevalent in the offices across the country and on Capitol Hill, Congress enacted the Telephone Consumer Protection Act in response to the overwhelming volume of unsolicited faxes being sent. The TCPA prohibits any person from using any telephone, fax machine, computer or other device to send an unsolicited advertisement to a telephone fax machine.

Among other provisions, the law provides a private right of action and there is a broad consensus that the TCPA has certainly curtailed the volume of junk faxes received in this country.

In spite of some predictions to the contrary, when this piece of legislation became law, it did not result in a proliferation of litigation. What did occur was that millions of unwanted junk faxes were no longer being sent as the deterrent effect of a private right of action took hold. The concerns addressed in the TCPA are the identical concerns that S. 630 is seeking to address. The TCPA has saved businesses millions of dollars in unwanted overhead expenses and has been a valuable tool in fighting unwanted faxes by

allowing a private right of action for damages, as well as injunctive relief.

The threat of possible litigation in and of itself has clearly been a deterrent to those whom have thought about violating the junk fax law. While I applaud this Subcommittee's effort to attempt to curb this latest abuse of technology, spam, there is one aspect of the bill that I, along with others, would like to see changed.

I am concerned that this bill does not provide a private right of action for many small businesses and individuals who have faced lost time or money due to these unsolicited e-mails filling their in boxes.

While I believe Congress must approach this issue in a balanced fashion and I support the comprehensive enforcement measures already proposed in S. 630, I also believe that there will be some cases in which an individual or business must directly seek recovery to address the economic harm they have suffered.

The largest Internet service provider, AOL, has estimated that 30 percent of its e-mail is spam. What is the effect of this abuse on the Internet? One result is the system-wide drag on the entire information highway costing the users the most valuable asset they have, their time. Another result is the millions of dollars citizens are collectively paying to their Internet service provider for the increased usage time that is required to read and delete these unwanted e-mails.

Unfortunately, under the proposed legislation, there is no way for these businesses and individuals to recoup the money that they have lost and continue to lose related to spam. It is my hope that with further consideration the Subcommittee will provide such a remedy as was done in the case of the TCPA.

It may be that on first impression one might surmise that the ISPs are the ones that are most damaged by junk e-mails. They suffer the increased expense in trying to filter out these unwanted e-mails and are required to spend money to provide additional bandwidth to provide optimal service to their end users.

But these ISPs already have a way to recoup these additional expenses. They charge their end users. This is exactly what many of the ISPs have done. Netcom Online communications services, a mid-sized Internet service provider, has stated that a conservative estimate of the cost to our customers to support spam is approximately 10 percent of their monthly bill.

Customers also pay fees to the ISPs for the additional connect time, as Senator Burns stated in his statement. It is a long distance phone call and the additional time costs the consumer money.

Pursuant to S. 630, the ISPs are not only permitted to recoup their additional expenses from the end users, but they are also entitled to sue the entity which sent the unwanted e-mails. Yet what incentive would the ISP have to spend potentially hundreds of thousands of dollars in legal expenses to go after the spammer when they can just charge the end users for this additional cost of doing business?

Who is left holding the bag and paying for the millions of dollars in damages which spamming causes? My business clients and the millions of other citizens throughout the country who use the Internet. What recourse did they have for footing this bill? I think the

answer is none. The question I have is why? If the concern is that every Internet user will race to the courthouse and file suit against a spammer, such a concern is misplaced. As noted above, the TCPA resulted in a significant reduction in the number of junk e-mails sent without a rush to the courts. Moreover, the Act only provides for recovery of actual damages suffered unless egregious conduct is involved.

In May of last year, Senator Lieberman stated spam undermines the viability of the Internet by burdening service providers who are forced to pass on the cost of funding spam to consumers. Our objective is not to strangle the Internet with government regulation or ban spam outright. Rather, we simply set out to give individuals control of their own e-mail accounts and to address the cost shifting problem brought by the proliferation of spam.

In this situation, it is critical that consumers be allowed to recover their full actual damages, whether that is the cost to replace a computer, a computer program that has been damaged as a result of excessive spamming or lost earnings resulting from clogged e-mail systems. These are concrete improvable damages. They are not speculative in the least.

Since it is impossible for Congress to predict the full range of possible damages suffered by consumers and small businesses, these damages should not be limited and just as in the TCPA to deter egregious behavior, the bill should also include some type of financial penalty for violations of this anti-spam bill. Without such a penalty, the entity sending these unsolicited e-mails might determine that it is financially worthwhile it continue to violate the law so long as they do not reach a volume likely to damage most computers or software.

Mr. Chairman, Senator Wyden, thank you again for allowing me to testify here today. I salute your consideration of this important issue and hope it will be possible to ensure that businesses and individual users of the Internet are not made to suffer economic harm without fair and balanced redress. I would be happy to answer any questions you may have.

Senator BURNS. Thank you and we appreciate your testimony today.

[The prepared statement of Mr. Pogust follows:]

PREPARED STATEMENT OF HARRIS L. POGUST, ESQ., PARTNER, SHERMAN, SILVERSTEIN, KOHL, ROSE AND PODOLSKY

Chairman Burns, Senator Hollings and distinguished Senators, it is an honor to appear before you here today.

My name is Harris Pogust, and I am an attorney from Pennsauken, New Jersey. I work at a small firm which represents over 2,000 small businesses in the Philadelphia and Southern New Jersey areas. Over the last several years my practice has focused on technology-related issues. It is only because of the disturbing rise in spamming, which has begun to cost my clients valuable time and expense, that I have become involved with this issue.

I am here today, Senators, representing those small businessmen and women who have suffered commercial loss and other economic damages as a result of the conduct of entities that transmit thousands upon thousands of junk e-mails on a daily basis. This junk mail clogs the Internet and takes up valuable space on my clients' computer systems, takes up valuable employee time, and costs my clients hundreds, and in some instances thousands of dollars a year in unnecessary and unwanted expenses. As the Internet has grown, the problem of unsolicited e-mails has increased to the point of where it has become an intolerable burden on my clients as well as

myself. I commend you for identifying this issue as an important concern for this Subcommittee's oversight agenda.

This is not the first time Congress has had to address the problems associated with the introduction of new technologies in the workplace. Ten years ago, when fax machines first became increasingly prevalent in offices across the country, and on Capitol Hill, Congress enacted the Telephone Consumer Protection Act ("TCPA") (47 U.S.C. §227) in response to the overwhelming volume of unsolicited faxes being sent. At that time, Congress decided to draw the line and let the senders of these unwanted faxes (in the form of solicitations and other questionable promotions) know that they could not continue their intrusive practices, which were clogging fax lines and wasting costly paper and employee time at small and large businesses alike.

The TCPA prohibits any person from using any telephone fax machine, computer or other device to send an unsolicited advertisement to a telephone fax machine. Among other provisions, the law provides a private right of action and there is broad consensus that the TCPA has certainly curtailed the volume of junk faxes received in this country. In spite of some predictions to the contrary, when this piece of legislation became law, it did not result in a proliferation of litigation. What did occur was that millions of unwanted junk faxes were no longer being sent as the deterrence effect of a private right of action took hold. The concerns addressed in the TCPA are the identical concerns that this legislation is seeking to address. The TCPA has saved businesses millions of dollars in unwanted overhead expenses and has been a valuable tool in fighting unwanted faxes by allowing a private right of action for damages and injunctive relief. The threat of possible litigation in and of itself has clearly been a deterrent to those who may have thought about violating the junk fax law.

The TCPA allows any person to bring suit in state court to enjoin a violation of the Act and to recover their actual monetary losses from such violations or they may seek a $500.00 penalty for each violation, whichever is greater. Additionally, the courts are authorized to award treble damages for egregious conduct—that is, where there are willful or knowing violations. Unfortunately, the pending legislation provides no such remedy to small businesses and individuals that suffer actual commercial consequences from junk e-mails filling their online mailboxes.

While I applaud this Subcommittee's efforts to attempt to curb this latest abuse of technology—spam—there is one aspect of this bill that I, along with others, would like to see changed. I am concerned that this bill does not provide a private right of action for the many small businesses and individuals who have faced lost time or money due to these unsolicited e-mails filling their inboxes. While I believe Congress must approach this issue in a balanced fashion—and I support the comprehensive enforcement measures already proposed in S. 630—I also believe that there will be some cases in which an individual or business must directly seek recovery to address the economic harm they have suffered.

The largest Internet service provider, America Online, has estimated that 30 percent of its e-mail is spam. America Online has stated that it was receiving 1.8 million spams per day from one company called Cyber Promotions. This continued until AOL obtained an injunction to stop this practice. Assuming that it takes the normal user 10 seconds to identify and discard a message, the end user was required to pay for 5,000 hours per day of connect time. What is the effect of this abuse of the Internet? One result is the system-wide drag on the entire information highway costing users the most valuable asset they have—their time. Another result is the millions of dollars citizens are collectively paying to their Internet service providers for the increased usage time that is required to read and delete these unwanted e-mails.

Unfortunately, under the proposed legislation, there is no way for these businesses and individuals to recoup the money they have lost and continue to lose related to spam. My hope is that, with further consideration, the Subcommittee will provide such a remedy, as was done in the case of the TCPA.

It may be that, on first impression, one might surmise that the JSPs are the ones that are most damaged by junk e-mails. They suffer the increased expense in trying to filter out these unwanted e-mails, and are required to spend money to provide additional bandwidth to ensure optimal service to their end users. But, these ISPs already have a way to recoup these additional expenses: charge their end users. This is exactly what many of the ISPs have done. Netcom On-Line Communication Services, a mid-sized Internet service provider, has stated that: "A conservative estimate of the cost to our customers to support spam is approximately 10 percent of their monthly bill."

Pursuant to 8.630, the ISPs are not only permitted to recoup their additional expenses from the end user, but they will also be able to sue the entity which sent

the unwanted e-mails. Yet, what incentive will the ISPs have to spend potentially hundreds of thousands of dollars in legal expenses to go after the spammer when they can just charge their end users for this additional cost of doing business? Who is left holding the bag and paying for the millions of dollars in damages which spamming causes? My business clients and the millions of other citizens throughout the country who use the Internet. What recourse do *they* have for footing this bill? None. The one question I have is: "Why"? If the concern is that every Internet user will race to the courthouse and file suit against spammers, such a concern is misplaced. As noted above, the TCPA resulted in a significant reduction in the number of junk e-mails sent, without a rush to the courts. Moreover, that Act only provides for recovery of actual damages suffered unless egregious conduct is involved.

In May of last year, Senator Lieberman stated that: "Spam undermines the viability of the Internet by burdening service providers who are forced to pass on the costs of fighting spam to consumers. Our objective is not to strangle the Internet with government regulation or to ban spam outright. Rather, we simply set out to give individuals control of their own e-mail accounts and to address the cost-shifting problems wrought by the proliferation of spam."

In this situation, as well, it is critical that consumers be allowed to recover their full actual damages—whether that is the costs to replace a computer or computer program that has been damaged as a result of excessive spamming, or lost earnings resulting from a clogged e-mail system. These are "concrete" and "provable" damages—and not speculative in the least. Since it is impossible for Congress to predict the full range of possible damages suffered by consumers and small businesses, these damages should not be limited. And just as in the TCPA, to deter this egregious behavior, this bill should also continue to include some type of financial penalty for violations of this anti-spam bill. Without such a penalty, the entities sending these unsolicited e-mails might determine it is financially worthwhile to continue to violate the law, so long as they do not reach a volume likely to damage most computers or software.

Mr. Chairman and Senator Hollings, thank you again for allowing me to testify here today. I salute your consideration of this important issue and hope it will be possible to ensure that business and individual users of the Internet are not made to suffer economic harm without fair and balanced redress. I would be happy to answer any questions that you may have.

Senator BURNS. And now we will hear from Mr. David McClure, President and CEO of U.S. Internet Industry Association here in town.

STATEMENT OF DAVID P. MCCLURE, PRESIDENT/CEO, U.S. INTERNET INDUSTRY ASSOCIATION

Mr. MCCLURE. Chairman Burns, Senator Wyden, it is a pleasure to be here to discuss with you the subject of unsolicited commercial e-mail and to express the support of our members for S. 630, the CAN-spam Act. I am especially pleased to note that this legislation is the product of two of the most respected technology legislators in the Senate today, yourself and Senator Wyden. We know from our work with you in previous issues that this has always resulted in the creation of well crafted and sensible Internet policy.

My name is David McClure. I am President of the U.S. Internet Industry Association, and we are the largest and oldest trade association representing Internet commerce, content and connectivity.

For the past 3 years, much of our effort has been taken up with the subject of UCE. In a white paper authored by Jim Butler and Andrew Flake, we outlined the problems that we encountered when we attempted to craft a legislative solution to spam and also the type of legislation that we believe is going to help bring relief to the situation.

I don't need to tell you how serious the problem of spam is. Congress already knows this. The Congressional Management Foundation this month released a report that said last year, Congress re-

ceived 80 million pieces of e-mail, most of it unsolicited bulk e-mail. That is double the previous year.

Nonetheless, while I don't need to tell you how serious the problem is, I think we do need to discuss the problems inherent in a legislative solution, and there are really two that we need to address up front. The first is that in terms of sending a single piece of unsolicited commerce e-mail, there is nothing really illegal in the Act, and we may well have some constitutional considerations in attempting to flatly ban it.

The second is more interesting in that we really can't define what it is that we are talking about when we say unsolicited commercial e-mail. We think we know what the term "e-mail" means, based on today's technology. It will change. I am not certain that we can satisfactorily define what "unsolicited" means or even what "commercial" means.

And a couple of quick examples. Does it mean that Girl Scouts who send out notices to their friends and neighbors of cookies for sale should be sent to jail? Does it mean perhaps that when the Red Cross sends an emergency notice of a need for O positive blood that they are in violation of the law? These are very difficult, difficult questions to answer, and we have struggled with them for 3 years.

Nonetheless, in the absence of a legislative solution, without the guidance of the law, we are left in a very difficult situation in which abuses do take place in which trade associations have their electronic newsletters to members routinely blocked, in which members who provide services—and this was referred to in the financial services industry—that they are required under contract and under law to provide, can find those communications blocked in the absence of any guidance.

More problematical from our standpoint are the actions of some black listers whose policies have in the past been somewhat arbitrary and have resulted in people being literally blocked from any kind of e-commerce. Good legislation is going to resolve that.

In our white paper, we identified what we considered to be four important things the legislation must do. First, it has to let the marketplace do its job. The greatest problem with UCE from our perspective is that it damages the network through its sheer bulk and its timing, but these are mechanical problems that can be resolved. And we believe that these are economic situations that can be resolved, and the market will eventually move to the kind of fee-based process that will resolve the damage to the networks. Once that happens, we expect to see—when e-mail is no longer free for bulk mailers—we will expect to see the volume decline.

Second, let's crack down on fraud. It is estimated that over 90 percent of spam is fraudulent. There is no excuse for this. We have laws and we'll have now a stronger national bill that requires people to identify who they are, where they come from, to use real header information and real subject information.

There are always going to be people who will not obey the law. Let's turn the cold light of daylight on every commercial message and woe be to the wicked. I believe that those people who do not obey this law should be punished without mercy. Third, support the acceptable use policies of ISPs. These are well crafted policies.

They are contracts that need to be supported, and when that happens, we believe that you'll see ISPs segregate themselves. Some will aggressively filter out all bulk e-mail and their terms of use, their acceptable use policies will notify consumers that that is what they wish to do. Consumers then will have the choice of whether they wish to use this or another ISP.

Finally, help marketers understand the word no. One of the problems with direct marketing is that in spite of the very best and well intentioned of legitimate marketers, there is always somebody who doesn't know the meaning of the word no. Opt-out should be simple, pervasive, and permanent.

Mr. Chairman, Senator Wyden, we are delighted to see that you have crafted legislation that meets all four of these points, and we believe that it is very important for the Committee now to pass this legislation on to the floor of the Senate to get it passed and move on to the House and put this legislation into effect. We don't believe that it needs extensive rewriting. It doesn't require good-faith exemptions or private rights of action or other major amendments. It needs only the support of this Committee and of the Senate. Thank you.

[The prepared statement of Mr. McClure follows:]

PREPARED STATEMENT OF DAVID P. MCCLURE, PRESIDENT/CEO, U.S. INTERNET INDUSTRY ASSOCIATION

Chairman Burns, and Members of the Communications Subcommittee,

It is my great honor to be invited to testify before you on the subject of Unsolicited Commercial Electronic Mail, and to express the support of our members for S. 630, the "CAN-spam Act." I am particularly pleased to note that this legislation is the product of two of the most respected technology legislators in the United States today, Senator Conrad Burns and Senator Ron Wyden. Our work with these distinguished Members of the Senate on other issues has always resulted in the creation of well crafted and effective Internet legislation.

My name is David McClure, and I am President of the U.S. Internet Industry Association, the oldest and largest trade association representing stakeholders in the Internet industry. USIIA was founded by leading companies in the online services industry to represent the interests of individuals and companies that do business on the Internet.

Our diversified membership includes Internet service providers from global and national ISPs to small providers serving remote areas nationwide; Internet backbone companies, telephone companies; hardware and software vendors involved in the technologies of the Internet; electronic commerce sites, and service providers to those sites. Our charter is to promote the growth of electronic commerce, content and connectivity through sound public policy and business support.

The issue of SPAM

For the past 3 years, much of our effort in public policy has focused on the issue of unsolicited commercial electronic mail. In a white paper authored by Jim Butler and Andrew Flake, we outlined the problems encountered in efforts to stop Spam with a legislative solution, and the scope of legislation that we believe will help bring relief.

I do not need to tell you how serious the problem of Spam is today. According to a report by the Congressional Management Foundation, the Congress itself suffered from more than 80 million pieces of electronic mail last year, the majority of those being unsolicited bulk mailings that interfered with the operations of Congressional offices and caused real damage to the communications capabilities of this body.

A Gartner survey released last week found that on average an employee spends 49 minutes of each work day simply managing e-mail. That is 10 percent of the workday for every employee in every office in America.

In spite of this, and in spite of our personal experiences, and the outcry from consumers and their advocates here today, efforts to legislation against unsolicited commercial e-mail suffer from two problems.

1. There is nothing illegal about sending UCE, and it may in fact be largely protected by the First Amendment; and
2. We don't know exactly what the term "unsolicited commercial e-mail" means. Certainly, we think we know what "e-mail" is—though advancing technology may render even our belief obsolete. I can assure you that we are unable to determine exactly what "commercial" should mean in this context, or "unsolicited," either.

Does it mean that girl scouts who send notices to their neighbors at cookie time should face jail time? Should the American Red Cross be punished for soliciting emergency donations of O-positive blood? We in this room would all agree that these are not the intent of the law. We, after all, only wish to stop the "bad spam."

But I can assure this Committee that even in the absence of such laws, anti-spam efforts are abused every day, causing irreparable damage to legitimate businesses. These include trade associations whose newsletters to their own members are routinely blocked by Spam filters. They include one of our member companies that gives more than one million consumers advance warning of viruses and security threats—but find themselves open to liability suits because those warnings are blocked in the name of preventing Spam.

Self-appointed spam blacklisters do not even wait until Spam is sent—they will blacklist your domain, and all of its customers, if they believe that at some future point your service might possibly be used to send Spam. It is vigilante law at its worst.

Solutions

What then, can this Committee do?

Must we abandon all efforts to stop unsolicited commercial e-mail in order to protect the First Amendment? Or must we accept the inefficiency and abuses inherent in efforts to stop any message that any person doesn't wish to read? In short, do we see efforts at a legislative solution fail, as they have for the past 3 years, because we cannot agree on a solution?

No.

In our white paper of 3 years ago, our association outlined the steps that would provide legislative relief without stumbling over the legitimate rights of communicators or corporations. There are four steps that I would re-state today:

- **Let the marketplace do its job.** The greatest problem with UCE from an infrastructure standpoint is that it damages the network through its sheer bulk and poor timing. These are both, though, economic issues. Marketers who want to send their messages through an ISP's servers should pay for the privilege. This is a contractual issue that the market is quite capable of managing. And frankly, once e-mail is no longer free and easy to send, its volume will decrease substantially.
- **Crack down on fraud.** It is estimated that over 90 percent of SPAM today is fraudulent. There is no excuse for this. We should have laws that force mailers to identify themselves, using real e-mail addresses, real header information and real contact information whenever they send a solicitation. Shine the daylight on every commercial message, and woe be to the wicked. Punish the lawbreakers without mercy.
- **Support the acceptable-use policies of ISPs.** Some ISPs will aggressively filter commercial messages as a service to their subscribers, and those subscribers who desire this service will flock to those ISPs. Others may choose not to block the information, and subscribers will receive what they wish. That is how an open, competitive market works, and the desires of all consumers can be met in this manner.
- **Help marketers understand the word, "No."** One of the problems with direct marketing is that in spite of the very best and well-intentioned efforts of legitimate marketers, there is always someone who can't understand the word. Opt-out should be simple, pervasive and permanent.

Conclusion

Mr. Chairman, and Members of the Subcommittee, I could ask you to craft the kind of legislation that would cover these four points. But that work is already done. In S. 630, we have a very good piece of legislation that will reduce unwanted commercial e-mail and resolve the outstanding legal issues, while still supporting consumer choice and the rights of service providers to run their businesses.

We are here today to ask that you give your support to S. 630 as it is today. It does not require re-writing—the industry has had ample time to give input to its

authors. It does not require "good faith" exemptions, or private rights of action, or any other major amendment. It needs only your support.

Mr. Chairman, on behalf of USIIA and its members, and of the Internet community at large, thank you for the opportunity to express our views on this issue. I would be honored to answer any questions you might have at this time.

The Effective Control of Unsolicited Commercial E-mail

An Internet Policy White Paper

By James W. Butler, III and Andrew Flake

Introduction

As commonly used, the pejorative "spam" refers to bulk electronic mailings of a commercial character, and the practice of "spamming" is positioned squarely at the center of contemporary debate over the Internet's commercial development, Internet etiquette and individual privacy.

For Internet service providers ("ISPs") especially, the bandwidth commandeered by spamming and the resultant slowdowns in service represent an infrastructure expense of increasing dimensions. At the same time, the law of the Internet remains in some disarray, although courts and even some states have taken initial stabs at regulating spam.

This White Paper presents a discussion of the problems inherent in direct electronic marketing from the perspective of both consumers and of the online community and concludes with modest recommendations for salient legislative initiatives.

Historical Overview

Spam is only one of a host of new legal issues that have arisen around electronic mail, and the term itself has had several incarnations in the online and Internet communities.

During the Internet's pre-commercial days, amid the perception of the need to minimize utilization of servers and message traffic to conserve acaUCEic and research resources, "spamming" referred to the act of posting an individual message to numerous UseNet Newsgroups. The exact path by which it did so is not known, but at some point the earlier, rather clean definition of "spam" evolved to encompass commercial or marketing messages as well.

One of the more critical events in the term's migration came with the infamous postings of an attorney who initiated a massive e-mailing in the hopes of soliciting green-card business among immigrants. His multi-posting efforts gained him the permanent enmity of Internet and UseNet users, as did his unwillingness to cease the effort once informed of his breach of Internet manners, or "Netiquette." That violation occurred simultaneously with explosive growth of Internet use among consumers: as they poured onto the Internet in 1994–1996, the sheer number of new users overwhelmed the online community and made the maintenance of the tightly-integrated Internet culture virtually impossible.

Despite very strong efforts by experienced Internet users to maintain their traditions and definitions, the communication became garbled, and two Internet conventions (one barring messages with commercial content, the other barring multi-posting of messages) were generally commingled into the general heading "spam."

The Terminology of Electronic Messaging

Whatever its traditional definitions and usage, the term "spam" may today be taken or mistakenly referred to as any one of the following sorts of messages: a message with commercial or marketing content; one that the recipient does not wish to receive, or which is unsolicited; one that the recipient has not specifically authorized in advance of its transmission; or, a message posted multiple times to a single or multiple newsgroups.

Accepting the Internet's transition into a commercial entity in which some forms of marketing and sales messages will be accepted and essential, imprecise definitions are counterproductive and serve to limit the development of electronic commerce. Although it is not the intent of this White Paper to alter Internet culture or common usage of terminology, the confusion and imprecision associated with the word "spam," suggest that a more precise labeling would be beneficial.

This White Paper will use the term Unsolicited Commercial Electronic mail ("UCE") to describe the process of directing a commercial message via electronic mail to a selected group of recipients.

Scope of the Problem

Measured by volume of use, electronic mail is fast approaching more traditional means of communication, including letter-writing and telephone communications. Though abuse of the UseNet messaging system on the Internet is both rampant and detrimental, the current controversy over electronic communication more frequently centers on unsolicited commercial e-mail. UCE is a problem for the Internet, for five reasons:

- **It is inefficient.** Presently, with no controls or costs attached to UCE, it is as cost-effective to drop one million pieces of UCE onto an ISP as it is to drop one—though the costs to the ISP are substantial. No production cost is involved in the creation of e-mail intended for UCE distribution—no brochures, artwork, printing or other mechanical costs. In effect, unchecked UCE is a "free ride" for marketers and provides them with a disincentive to research, focus or target the list of recipients to insure interest in the products or services presented.
- **It disrupts service.** A major mechanical drawback with UCE is that it arrives on the Internet without notice. It slows service for other users, often during peak use hours. In some cases, it has caused wholesale failures of Internet networks. This disruption is frequently aggravated by the fraudulent use of incorrect or non-existent return addresses, which causes the outraged responses of recipients to bounce across the network multiple times as the system attempts to deliver messages that cannot be delivered.
- **It is frequently fraudulent.** An Internet culture protective of user anonymity has the unfortunate side effect of creating an environment in which unscrupulous purveyors of UCE can operate. Messages are sent directly to an electronic mailbox, and marketers need not provide information, e.g., business name, physical address, telephone and fax numbers, that would enable consumers to assess the validity of companies. Without greater certainty about company legitimacy, Internet consumers quite rationally become wary of even legitimate marketers. These concerns have contributed to decisions by ISPs to seek judicial protection.
- **There is no effective "opt-out" procedure.** In the offline world, marketers operate a system that enables consumers to remove themselves from direct marketing lists. While the system is not completely effective, it does exist. In the online world, no such system exists, although numerous efforts to create one have been undertaken.
- **There is no compensation for service.** In the offline world, direct marketing subsidizes the U.S. Postal Service and/or telephone companies, effectively paying for itself. In the online world, UCE currently benefits only the originator of the message and does not pay for the burdens it places on the system. UCE provides very little value, e.g., convenient shopping, entertainment value, or consumer information, and Internet service providers bear the brunt of the resource outlay for the infrastructure that enables UCE. Realistically, a mechanism that shares the economic burdens of UCE will more closely mirror the offline world, and will produce stronger efficiencies in the way UCE is handled on the networks. A "pay as you go" system would compensate the ISP's who provide the on-and-off ramps for the UCE traffic.

Combating the Growth of UCE

In recent years, significant progress has been made toward understanding and dealing with the problems associated with UCE. Sanford Wallace, the self-proclaimed "king" of the UCE business, stepped down and joined the ranks of those opposing unchecked direct electronic marketing. Major Internet providers such as Earthlink and AOL successfully secured court orders against perpetrators of unwanted UCE. Nonetheless, the current legal situation remains far from clear, and debate rages on among those impacted by and involved with Internet service provision.

On one side are individual consumers who do not wish to have their time wasted by having to open and read the first few lines of countless messages in which they have no interest. ISP customers who fall into this group are supported by consumer advocacy groups, as well as by those whose loyalty to the old Internet culture of non-commercialism eschews marketing of any sort. On the other side are the marketers, who believe that they have a clear right to communicate with current and potential customers, regardless of legal trends to the contrary. These marketers are supported by customers who wish to have product and service information, as well

as by the Direct Marketing Association and its legion progeny, who fought for similar rights in the use of the mails and in direct telephone solicitation.

Individual ISPs straddle the line and await some clear resolution while attempting to cope with UCE's associated costs—these are the online and Internet services that suffer both the wear on their systems from dumping of UCE messages, along with the wrath of the subscribers incensed over wasted time and service slowdowns. These service providers seek additional sources of revenue to keep costs competitive as their business grows, but fear the network damage and other consequences of opening their systems to unwanted UCE.

Unsuccessful Initiatives

While the two camps (and the companies and individuals stuck in the middle) have generated significant public dialogue, attempts to deal with the very real and escalating problems of UCE have been only partially successful, and generally only in the event that the originator of the UCE can be identified. Initiatives that have proven *unsuccessful* include:

- Attempts to claim ownership of the electronic mailbox. Unlike the offline world, where the U.S. Postal Service rather than the consumer owns the mail box, the online industry assumes that each individual owns his or her e-mail box. Although such ownership has not been legally established, the constitutionality of so-called "receiver restrictions," in which consumers are given the right to refuse certain mailings, has been upheld.
- "Right to privacy" claims. There is a perceived "right" of consumers to not have to view anything they elect not to view, although no case law substantiates this position. By the same token, however, constitutional free speech does not mean that an individual is *obligated* to view particular subject matter.
- Extension of laws prohibiting marketing via facsimile. *See, e.g.,* "Netizens Protection Act of 1997," H.R. 1748, 105th Cong., 1st Sess. (1997). Although the laws that were used to prohibit direct marketing via fax automatically are sometimes believed to extend to electronic mail, this concept overlooks some very fundamental differences in the two systems. For one, fax machines use expensive resources, where electronic mail normally does not, and efforts to build a case based on the time wasted in reading unwanted e-mail have largely been countered by advances in message preview technology and by the move to flat-rate rather than per-minute pricing for Internet and online services.
- An "opt-in" solution, no matter how desirable, may be impractical. Much of the discussion of consumer rights to date has focused on whether UCE should be sent only to those who have specifically requested communications—an "opt-in only" solution. This approach, however, would severely limit communication with persons who have not given advance written consent.
- An "opt-out" solution needs strong enforcement mechanisms. The ability of consumers to quickly and easily "opt-out" of receiving UCE, will only work if there is a sufficient incentive to keep the opt-out list well-maintained, well-promoted and easily accessible by consumers.
- Efforts to delineate UCE based on the content of the messages has proven impractical. For example, even the most liberal definitions of "commercial" e-mail would prevent announcement to parents of what an elementary school is serving for lunch, since this would clearly be an advertisement of a product for sale.
- Use of mandatory "header" information is counter-productive. Many suggestions have been made regarding an identifying mark or phrase that could be placed in the subject line or at the head of any commercial message, thus allowing e-mail filters to more easily identify and eliminate UCE. While this idea is appealing, it suffers from the definitional problems because filtering systems, at their current level of sophistication, cannot differentiate between UCE and otherwise valid customer mailings. Attempting to have any body, organization or regulation define exceptions to the rule would be unwieldy, and use of extensive identifying information in the first lines of the message would render useless the preview screen technology used by many consumers to rapidly screen messages and their content.
- Use of a "pre-existing relationship" test may not be sufficient. It has been assumed by many in the online community that such a test may be implemented in the near future, under which electronic mailings would be permitted to those customers and other groups with whom the mailer has a "pre-existing relationship." This assumption, however, has led virtually every business that has a

web site or advertises via electronic mail to scramble to collect personal information about users as a hedge to show such a relationship. The rampant collection of data in order to prove the relationship has created another crisis in the area of privacy, as was noted by the Federal Trade Commission in its efforts to enforce Internet privacy guidelines.

Developing A Framework

To merely legislate or regulate UCE out of existence is neither Constitutional nor necessary. Though not yet tested, even unsolicited commercial messages would be subject to constitutional protections if Congress acted to prohibit their dissemination.

Such restrictions are better left to Internet service providers, which as private actors may ban distribution of UCE messages on their networks. Still, the industry's efforts with respect to UCE have so far proved only moderately successful. From these efforts, however, has emerged a sense of a viable framework to address its inherent problems.

- **Fraud Prevention Legislation.** The extension of regulations and legislation related to fraud to UCE. The trend at the state level is clearly toward regulating the practice of UCE. State legislation, however, must be carefully drafted to avoid constitutional challenge, as the experience of Georgia's UCE fraud statute indicates.
- **Measured Common Law Development.** Recognition by the courts that UCE as presently practiced creates a strong adverse impact on the Internet. Specifically, the channeling of hundreds of thousands of pieces of electronic mail through an Internet system at a single time significantly degrades the performance of the network and interferes with other forms of Internet access and communications.
- **Continued Industry Initiatives.** The growth of filtering technology for electronic mail. While still crude and relatively ineffective for the larger body of electronic messages, filtering technology has assisted ISPs in taking the first steps toward empowering consumers to automatically reject unwanted solicitations.

Any proposed framework will at best be preliminary, with additional time and consideration required for its full effectiveness, but reasoning from the current experience of the online industry, it is certain that the following will be factors in any consistent legislative approach to UCE:

- The first step is to **eliminate fraudulent mailings.** The most critical elements of a framework for control of UCE will be unsuccessful if unscrupulous operators are able to flaunt the rules with impunity. At a minimum, electronic mailers should be required to divulge their real identities and return addresses, as well as compliance with other consumer protections laws as appropriate. Although a number of ISPs have imposed guidelines prohibiting the use of their services for the sending of UCE messages, such efforts are far from universal, and the individual policies of an ISP provide no protection against external sources of UCE.
- The solution must include **relief for stress on the networks.** Consumer irritation aside, the damage done to the Internet by UCE is very real, and its elimination of this damage must be a central consideration in proposed legislation. At the minimum, a requirement for contractual notification of the Internet service or provider prior to transmission of UCE should be put in place; the market would be best served, however, by an industry-wide financial arrangement, similar to the postage system, to compensate all carriers of the message traffic. A compensation system would have the additional benefit of providing a barrier to entry for unscrupulous spammers.
- The **right of the states to impose more stringent consumer protections** should be preserved. State and local laws have provided some of the strongest protections against abusive UCE to date, in part because they have more extensive protections available against business interference and detrimental business practices. The framework for the future should include some assurance that state and local considerations on behalf of Internet services and consumers not be preempted, to the extent that they are more solicitous of consumer interests than any federal statutory cause of action. Federal initiatives should provide a base level of protection for consumers and ISPs, to circumvent the possibility of inconsistent regulation of an entity, the Internet, that is not bounded by geography.

Conclusion

The continuing popularity of electronic mail ("e-mail") as a medium of personal and business communication has brought in its wake a host of novel legal issues, among them the extent to which the practice of unsolicited commercial e-mail ("UCE") may be limited.

A compelling need to protect Internet users from unwanted, unnecessary and fraudulent commercial message traffic, as well to protect the infrastructure of the Internet from the problems created by massive postings of messages, either commercial or otherwise, has already seen some courts and state legislatures move to prohibit the practice in its various forms.

This White Paper has set forth in summary fashion the historical and legal underpinnings of the debate over UCE, and its conclusion is that federal legislation should be enacted that would (1) provide a minimum of protection for consumers against fraudulent electronic mailings by marketers; and (2) promote a more reasonable allocation of the costs of legitimate UCE toward the direct marketers that are its source.

Appendix A: USIIA Policies

The U.S. Internet Industry Association opposes any action, program, system or endeavor that corrupts the legitimate use or integrity of the channels of electronic communication. This policy is explicitly stated in paragraph 7 the USIIA Code of Standards, which reads as follows:

"*Members shall not knowingly create, acquire, distribute or allow intentional distribution of materials that violate the legitimate use or integrity of the channels of electronic communication, online services, computer systems or their contents.*"

Consistent with this policy, USIIA does not support the practices of Multiposting of Messages or Off-Topic Posting of Messages. It is the belief of the Association that persons who deliberately engage in these practices should have their access to the UseNet and other online lists, discussion groups or message bases terminated. This policy is not intended to affect the legitimate act of Cross-Posting of Messages. Similarly, USIIA does not support or condone the communication of information that is deliberately misleading or fraudulent. This is stated in the USIIA Code:

"*Members shall not knowingly disseminate false or misleading information and shall act promptly to correct erroneous communications for which he or she is responsible, or which originated from or resides on his or her system.*" USIIA Code of Professional Standards, #8.

This section of the Code is interpreted to include messages in which an attempt is made to disguise the commercial nature of the message, those which are fraudulent, those which misrepresent the origination of the sender, and those which are violations of the law at the point of origination. Nothing within the Code, the Bylaws of the Association, its Mission Statement or the will of its members specifically prohibits or discourages the legitimate commercial uses of electronic mail or messaging.

Senator BURNS. Thank you, Mr. McClure.

Senator WYDEN. Thank you.

Mr. Chairman, I think it is striking now. You and I have put an enormous amount of time into this issue now over the last Congress and this Congress and we thought we were going to get there at the end of the last session, and suffice it to say, I have got a number of questions I want to ask, but my biggest concern here is that we need to act, because people are tired of this. And to just go round and round the mulberry bush with everybody having their own difference just doesn't seem to me to be very constructive.

I mean, I would say to Mr. Pogust you know since my days as director of the Gray Panthers, my background has been consumer law and consumer rights.

I find it pretty hard to see a private right of action here for a handful of unsolicited e-mails, but to tell you the truth, I could see how you would differ. In other words, something reasonable people can differ on. The problem is that if we just go round and round on all of these, we are never going to get anything done in this

Congress so what I want to do is ask just a couple of questions in hopes that we can get a bill here and actually signed into law.

Do any of you think that the Burns-Wyden bill is not better than the status quo? Mr. Moore? Do you think that Burns-Wyden is better than the status quo?

Mr. MOORE. Absolutely. No question about it.

Senator WYDEN. Mr. Buckley?

Mr. BUCKLEY. Yes.

Senator WYDEN. Mr. Pogust?

Mr. POGUST. Yes, but I believe it needs a little work.

Senator WYDEN. I am going to still just take the yes.

Mr. CATLETT. I think there is a risk it will worsen the problem rather than improve it, so I am sorry to say.

Mr. CERASALE. Senator, yes.

Senator WYDEN. OK., so we got almost everybody saying that Burns-Wyden, even though we all have differences——

Senator BURNS. One-and-one. That is better than all in one.

Senator WYDEN. All right. That is encouraging. Anybody think that you ought to be able to falsify headers? I can't believe that anybody is in favor of that? I will take that as a United Nations opinion.

Everybody here, even though there are differences on the role of opt-out/opt-in thinks that opt-out is a useful pro-consumers principle? Mr. Catlett, you can take the floor. We recognize you are for opt-in and I understand that, but opt-out is better than nothing for the consumer, isn't it?

Mr. CATLETT. It is better than nothing in an individual case. However, if you apply broadly an opt-out policy, particularly if you preempt state law on this, you will actually increase the number of unwanted solicitations, most likely, so applied broadly, an opt-out policy with preemption may well make the problem worse.

Senator WYDEN. I am not going to belabor it. I think that is pretty far-fetched. To me, any way you slice it, when people are opting out, they are going to get fewer of those communications, but again, reasonable people can differ and let me just kind of keep going on this.

For the DMA folks and Mr. McClure, any sense on what the Burns-Wyden bill would cost to comply with? I mean, we think that these are pretty modest costs, and they would be consistent with free enterprise, you know, principles. Do you all disagree with that?

Mr. CERASALE. Not at all. As a matter of fact, our members, if someone says do not send me any more solicitations, they have to follow it already, so that I would say that this fits pretty tight within what our members already have to do.

Mr. MCCLURE. We are in agreement, sir. We don't see significant costs. We do, if I may quickly, address the issue that has been raised here repeatedly, and that is that somehow ISPs would not aggressively go after spammers because it costs too much money for them to sue. Certainly if it is going to cost them hundreds of thousands of dollars to sue, it would not cost much less for individual consumers to do so.

We believe that ISPs have a very strong record of suing spammers when they have the law on their side. And therefore, we

believe that this is a good bill for ISPs and it needs to be passed. We have gone 3 years, sir. It is time to get a bill passed.

Senator WYDEN. You are singing from my hymnal. Question for the financial services folks. I think you know, I think you all have raised legitimate concerns and to some extent they are not unlike what happened with the electronic signatures bill at the end because this is all new.

I mean, if you sat around the Senate Commerce Committee 20 years ago, you never debated this kind of stuff. You were talking about an economy where people in Montana and Oregon were doing the physical movement of goods and you got up in Missoula at 5 o'clock in the morning you ate about 20,000 calories at 5 o'clock in the morning and you did physical labor so this is all new stuff, so we are trying to be sensitive to your concerns.

You have indicated you have got some concerns about the enforcement issue, and we are going to try to address those, the role of the Federal Trade Commission and the states and I think we can, we can do that and as you know, some of those issues came up in the electronic signatures bill as well, the role of the Federal Government and the states, but the one that I would like to see if we can make progress on is on the definitions. I want to find out if we are talking about some technical stuff or are we talking about things where there is really a philosophical question.

You suggest, for example, that being clear may require, for example, a universal signal that the e-mail is an advertisement, a kind of universal signal. The reason we have taken the approach that we have, Senator Burns and I, Chairman Burns and I, is we are trying to give business a lot of flexibility because we thought that is what business folks were interested in is trying not to have this one-size-fits-all and everybody in Washington, DC running around saying we have got all of the wisdom.

Mr. BUCKLEY. I understand your frustration, Senator, as you say——

Senator WYDEN. We are trying to be responsive.

Mr. BUCKLEY. You say "let's try to give people flexibility" and that is something people often want, but in compliance statutes we find clear definition of responsibility is important. I practice law and defend lawsuits and try to advise clients on how to remain compliant. It is a good idea to try to give people a model. It doesn't necessarily eliminate flexibility—you could both retain flexibility and give a model saying "do it this way and you can be sure to have complied." You still have flexibility to comply otherwise, but in an area like this, using standards like "clear and conspicuous," without further definition of what you are talking about.

This notice is something that is going to be fairly universal and I hope fairly simple, but you know when you get into what is clear and conspicuous, what's the size of type, where does it have to be located, maybe we ought to have some discussion about that. You know, I don't want to pin people in other industries down where they feel that they need flexibility, but it is awfully helpful to know exactly what Congress has in mind. There is a class action bar lurking out there, and if we don't get some of the changes we have asked with respect to enforcement, we may have challenges to whether something is "clear and conspicuous" or not. Even the FTC

may conclude we don't agree with your understanding of what clear and conspicuous is.

So we think tightening down on the meaning of "clear and conspicious" would be helpful. I know precision is not what people are always asking for, but that seems best in this case in our judgment.

Senator WYDEN. Well, we will work with you and I know Senator Burns has some questions, but I think we ought to get this, get this bill to the White House for signing, for a signing ceremony. I think I have met with almost all of you individually, the financial services folks here recently, Senator Burns has done exactly the same thing, and you know, look, I think the American people say getting spam in their in box is like getting that unidentified stuff in your lunch box, and you didn't order it. You don't know where it comes from, and you are really ticked off.

So work with us here to try to resolve these remaining issues because even at this table there is a whole lot more common ground here than there are reasons to go off in your respective corners and come out swinging, which was why I asked that question about the status quo, and we will do our best to be responsive to your concerns and Senator Burns, like a pen from President Bush when this bill gets signed into law, and I would, too, and I thank you, Mr. Chairman.

Senator BURNS. All I need is one more pen. You bet. All I have is one more question, and I am going to throw it out on the table and let everybody take a shot at it. I referenced the article in the Wall Street Journal on Monday. And it had to do with mass harvesting.

Spammers can't survive without a plentiful supply of e-mail addresses, and as I understand it, businesses have sprung up to fulfill that need. They have technology that intrudes on popular websites and gathers thousands and thousands of e-mail addresses to spammers. And they sell and rent those addresses to spammers. The result is that someone who has posted a comment in a chat room or made a winning bid on an online auction, and I am an auctioneer, and I want to sell spurs so they don't send me much, they get on a spam list and they are flooded, absolutely flooded with unwanted messages. And I will tell you, I did sell a pair of spurs on eBay and boy, as soon as that happened, I'll tell you, I just threw my old computer away. I changed my name and everything.

That individual's privacy has been invaded and they don't know how it happened. It sours them on the entire business of e-commerce. Do we need to do something about this business of harvesting and do we, and is there a way to amend or how would you recommend that we deal with this situation of harvesting? Mr. Catlett?

Mr. CATLETT. Thank you, sir. Unfortunately, to ban harvesting would not be effective for the following reason. There is a technology employed now called dictionary spamming which is based on the age-old sales method of guessing so a spammer, for example, has an e-mail address John42@aol.com so they try sending a spam to John43@aol.com and the mail server tells them no such address or yes, that is a live one, then they go into John45 and so on and so forth. They also try John43@earthlink.com and because people

tend to use e-mail addresses which are easy to remember for their friends, they hit on a large number of deliverable addresses. So as deplorable as the practice of scavenging e-mail addresses is, to ban it, even if completely effective, would not solve the core problem.

Senator BURNS. Any other comments? How do we, how do we deal with these folks who break into commercial organizations and take their list?

Mr. CATLETT. Well, the Computer Fraud and Abuse Act would already make that illegal, I believe, sir. I am not a lawyer, but——

Senator BURNS. Is that correct? Well, that is about all the questions and Senator Wyden and the way you covered this thing, we will, we want to work with you and to move this thing out and find a way that we can find some similar ground on this thing.

Senator Allen had some questions, and I am going to allow him to submit those in writing and you can respond either to the Senator or to the Committee. We would appreciate that. And then I have a couple more, but it is getting close to 4:30 and I never work past 4 o'clock. And we have already gone overtime.

But I want to thank you for your testimony today. We invited AOL and Yahoo today and they declined to come and before we can, before we can solve some of these problems, we are going to, we have got to have a good, strong representation of the giants of the industry, and I am disappointed in that but nonetheless, we'll be meeting with those folks and continue our communications with you as we work it through the Senate. But I am like Senator Wyden. It is time to move this thing and we plan to do just that as soon as we can. Thank you for coming today. We appreciate it. These proceedings are closed.

[Whereupon, at 4:35 p.m., the hearing was adjourned.]

A P P E N D I X

PREPARED STATEMENT OF HON. ERNEST F. HOLLINGS,
U.S. SENATOR FROM SOUTH CAROLINA

Today's hearing examines a bothersome consumer issue—that of unsolicited commercial e-mail, also referred to as junk e-mail or spam. With the growth of commerce over the Internet, consumers are being bombarded with junk e-mail advertising various products and services, including get-rich-quick schemes, phone sex lines, and pornographic websites. In light of the bothersome and at times costly nature of junk e-mail, I believe it is appropriate for Congress to address this issue.

Since junk e-mail imposes real costs on recipients, it is important that we act to resolve this issue and not simply balance the concerns of competing business interests. For example, an ISP or a business has to expend money and resources when its network crashes because it cannot handle the volume of junk e-mail. Consumers have to expend time and money to delete junk e-mail from their accounts or inform the sender that they do not want to receive future junk e-mails.

An opt-out approach in which the recipient has to respond to every junk e-mail and ask the sender not to send any additional junk e-mail is riddled with loopholes. This approach is problematic because in the online world, spammers often do not provide correct addresses and header information. An opt-out system also requires electronic marketers to keep a well-maintained list for all consumers who have opted-out, provide clear information to consumers about what they need to do to opt-out, and ensure that consumers know that they can opt-out of receiving junk e-mail. An opt-out approach also presents difficult questions such as if a consumer opts-out of receiving information from the Gap does that mean that Old Navy, a store owned by the same parent company, can send the consumer junk mail? Also, where a consumer has multiple e-mail addresses, must the consumer opt-out for each e-mail address?

I also believe it is important that all consumers have some legal recourse when they are harmed. This means that when a business or consumer suffers damages from having their computer and Internet systems go down because of the volume of junk e-mail, they are able to recover damages. The threat of a lawsuit will help to ensure that senders of junk e-mail take the requisite care when they send junk e-mail.

This is an important issue and Congress should take the time to get it right. I welcome the witnesses and look forward to hearing their testimony.