S. HRG. 105–1028

SPAMMING

HEARING

BEFORE THE

SUBCOMMITTEE ON COMMUNICATIONS

OF THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION UNITED STATES SENATE

ONE HUNDRED FIFTH CONGRESS

SECOND SESSION

JUNE 17, 1998

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

U.S. GOVERNMENT PRINTING OFFICE

58–675 CC WASHINGTON : 1999

For sale by the U.S. Government Printing Office
Superintendent of Documents, Congressional Sales Office, Washington, DC 20402
ISBN 0-16-059690-4

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED FIFTH CONGRESS

SECOND SESSION

JOHN McCAIN, Arizona, *Chairman*

TED STEVENS, Alaska
CONRAD BURNS, Montana
SLADE GORTON, Washington
TRENT LOTT, Mississippi
KAY BAILEY HUTCHISON, Texas
OLYMPIA J. SNOWE, Maine
JOHN ASHCROFT, Missouri
BILL FRIST, Tennessee
SPENCER ABRAHAM, Michigan
SAM BROWNBACK, Kansas

ERNEST F. HOLLINGS, South Carolina
DANIEL K. INOUYE, Hawaii
WENDELL H. FORD, Kentucky
JOHN D. ROCKEFELLER IV, West Virginia
JOHN F. KERRY, Massachusetts
JOHN B. BREAUX, Louisiana
RICHARD H. BRYAN, Nevada
BYRON L. DORGAN, North Dakota
RON WYDEN, Oregon

JOHN RAIDT, *Staff Director*
MARK BUSE, *Policy Director*
IVAN A. SCHLAGER, *Democratic Chief Counsel and Staff Director*
JAMES S.W. DREWRY, *Democratic General Counsel*

SUBCOMMITTEE ON COMMUNICATIONS

CONRAD BURNS, Montana, *Chairman*

TED STEVENS, Alaska
KAY BAILEY HUTCHISON, Texas
SPENCER ABRAHAM, Michigan
SLADE GORTON, Washington
TRENT LOTT, Mississippi
JOHN ASHCROFT, Missouri
KAY BAILEY HUTCHISON, Texas
BILL FRIST, Tennessee
SAM BROWNBACK, Kansas

ERNEST F. HOLLINGS, South Carolina
DANIEL K. INOUYE, Hawaii
WENDELL H. FORD, Kentucky
JOHN F. KERRY, Massachusetts
JOHN B. BREAUX, Louisiana
JOHN D. ROCKEFELLER IV, West Virginia
RICHARD H. BRYAN, Nevada
BYRON L. DORGAN, North Dakota

CONTENTS

WITNESSES

SPAMMING

WEDNESDAY, JUNE 17, 1998

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

The committee met, pursuant to notice, at 9:29 a.m., in room SR–253, Russell Senate Office Building, Hon. Conrad Burns (chairman of the subcommittee) presiding.

Staff members assigned to this hearing: Kalpak Gude, counsel; Kevin M. Joseph, senior Democratic counsel; and Paula Ford, Democratic counsel.

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

Senator BURNS. We would like to call the hearing to order. It is a little before 9:30, about a minute. You know, it is terrible in Washington to be a minute ahead.

We have two Senators and a Congressman who wish to drop by this morning and offer their testimony on spamming. They come up with all of this stuff and I never know where they come up with it. But, nonetheless, we have a conference that starts at 10:30 a.m., and it involves all the Senators, on our side of the aisle anyway, and so we are going to try to make that conference, and limit the opening statements as much as we can.

I would like to welcome our witnesses that are here now, and our guests this morning, as we take a look at the explosion of junk E-mail, or spamming, on the Internet. From all that I can gather, this seems to be a growing problem on the Internet. And there has been some actions taken with regard to spamming. And we thought maybe we better have some folks up and visit with us about how big the problem is and all the ins and outs of it and how much it is hurting the Internet or it is helping the Internet.

I am going to submit my written statement this morning for the record—being that I am the unanimous consent myself. You know, it is kind of like playing golf by yourself, you get a lot more give-me's this way. [Laughter.]

I would like to welcome this morning—and we will start off with Sheila Anthony, who is Commissioner of the Federal Trade Commission. And if she would come forward and offer her testimony this morning. And as the Senators would show up, we will make room for them. In the meantime, the witnesses might get their statements together. And if you want to paraphrase, if you want

to make them smaller, your full statement will be made a part of the record.

[The prepared statement of Senator Burns follows:]

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

I would like to welcome our witnesses to today's hearing, which will address an unintended problem posed by the growth of the Internet: the explosion of junk e-mail, or "spamming." I would like to particularly thank Senator Murkowski, Senator Torricelli and Congressman Smith for taking time out of their busy schedules to testify before this Subcommittee on this critical issue.

The Internet has provided tremendous commercial and educational opportunities to people across the globe. Unfortunately, however, the revolution in communications technology has also allowed for unscrupulous actors to intrude on the privacy of Americans with the digital equivalent of junk mail. In the digital age, it is just as cheap and easy to send one million pieces of junk e-mail as it is to send one piece.

"Spamming" is truly the scourge of the Information Age. This problem has become so widespread that it has begun to burden our information infrastructure. Entire new networks have had to be constructed to deal with it, when resources would be far better spent on educational or commercial needs.

Spamming is especially troublesome to consumers in rural areas such as Montana. Often, rural residents must pay long distance charges to receive these unwanted solicitations, many of which contain fraudulent messages.

I congratulate Senators Murkowski and Torricelli for their hard work on dealing with the issue of spamming. I supported the Anti-Slamming Bill, S. 1618, which as amended included language that requires commercial e-mailers to identify themselves. The amendment also required that a junk e-mailer must honor requests from individuals to be deleted from mailing lists. As those of us with online accounts are discovering, millions of junk e-mails are sent out with fake e-mail addresses which prevent citizens from requesting that they not be sent any further messages from the same sources. This language was simply a "Truth in Advertising Amendment" and I welcomed it as a positive first step in dealing with this increasingly troublesome topic.

I will continue to work closely with my colleagues to make sure that Americans are freed from this invasion of their privacy in the digital world. I look forward to the testimony of our witnesses today on this important issue. Thank you.

Senator BURNS. I appreciate this, this morning. And, Commissioner Anthony, welcome, and we look forward to hearing from you at this time.

STATEMENT OF SHEILA FOSTER ANTHONY, COMMISSIONER, FEDERAL TRADE COMMISSION

Ms. ANTHONY. Thank you, Senator. It is nice to be back here.

I am here today to tell you about spam and junk E-mail, as you call it, also called unsolicited E-mail, or UCE. The Federal Trade Commission is the Nation's primary national consumer protection agency. Its principal consumer protection mandate is to take action, under section 5 of the Federal Trade Commission Act, against unfair or deceptive acts or practices in or affecting commerce.

Section 5 gives the Commission broad law enforcement authority over virtually every sector of the economy. Commerce on the Internet, including unsolicited commercial E-mail, falls within the scope of this statutory mandate.

The problem with unsolicited commercial E-mail, or spam in Internet lingo, is that it is often sent in bulk to a consumer without the consumer's prior request or consent. Although spam might be irritating to consumers, not all of it is fraudulent. The Internet's capacity to reach literally millions of customers quickly and at a low cost through UCE has been seized on, however, by fraud operators, who are often among the first and most effective at exploiting any technological innovation.

In fact, spam has become the fraud artists' calling card on the Internet. The staff of the Commission has reviewed a collection of over 100,000 pieces of spam. Much of it contains fictitious information about the sender, misleading subject lines, and extravagant earnings or performance claims about goods and services. These types of claims are the fraud operators' stock in trade.

Bulk UCE also burdens Internet service providers and frustrates their customers. But our concern as a Commission is its widespread use to disseminate false and misleading claims about products and services offered for sale on the Internet. The Commission believes the proliferation of deceptive bulk UCE on the Internet poses a threat to consumer confidence and online commerce. And we view this problem as significant.

Today, Congress, law enforcement and regulatory authorities, industry leaders, and consumers are faced with important decisions about roles of self-regulation, consumer education, law enforcement, and government regulation in dealing with unsolicited commercial E-mail, and its impact on the development of the Internet. Deceptive spam is a small part of a larger problem of deceptive sales and marketing practices on the Internet. The Commission has taken the lead in pursuing Internet fraud and deception under section 5 since commerce on the Internet began.

We have brought 36 law enforcement actions to halt online deception and consumer fraud. These cases targeted Internet scams ranging from pyramid schemes to credit repair schemes to fraudulent business opportunities. Last summer, we set up a special mailbox at the Commission to provide assistance to Internet service providers, privacy advocates and other law enforcers, and we invited consumers to forward their UCE to it.

This mailbox has received more than 100,000 forwarded messages, including about 1,500 new pieces of spam a day. Staff enters the message into a searchable data base and analyzes it and identifies trends. And then we use these findings to target law enforcement and education efforts.

The largest categories of spam in the FTC's database are chain letters and pyramid schemes. Both schemes make money for only a few participants. Our experience with pyramid marketing schemes supports the conclusion that 90 percent or more of investors are mathematically certain to lose money. Fees paid by new recruits, not profits from the sale of goods, generate most of their revenues. Both pyramid schemes and chain letters are illegal.

The Commission has responded to a large amount of chain letter and pyramid UCE with comprehensive consumer and business education programs and tough law enforcement. For example, in October 1997, the Commission sued Nia Cano, doing business as Credit Development International and Driver's Seat Network. In that suit, the Commission alleged that the defendants falsely promised that investors would receive an unsecured Visa and MasterCard, and they could earn $18,000 a month by recruiting others into the scheme.

The complaint alleged that the defendants urged participants to use bulk E-mail to solicit recruits. An estimated 27,000 participants flooded the Internet with UCE, repeating the defendants' offer. The Commission obtained a temporary restraining order and

preliminary injunction against these defendants, freezing more than $2 million for restitution to victims. The case is still in litigation.

The staff has taken aggressive steps to deter others who use spam to promote chain letter and pyramid schemes. Last February, with the assistance of the U.S. Postal Inspection Service, the Commission put more than 1,000 junk E-mailers sending UCE on notice that law enforcement agencies monitoring UCE for deception and fraud are keeping track of them.

The Commission sent letters, warning senders that their E-mail may violate Federal law, advising them of relevant laws, and inviting them to visit the FTC's Web site for further guidance. We continue to monitor the UCE data base to make sure that those who have been warned do not resume sending deceptive UCE.

If the Commission finds that senders of deceptive UCE who have been warned continue to send these messages, however, we will take appropriate action.

In addition to online pyramid schemes and chain letters, the Commission's UCE data base contains other categories of possibly deceptive UCE. These categories mirror schemes which have proliferated in other media: business opportunity offers, work at home schemes, guaranteed credit cards and loans, credit repair schemes, and diet and health products making false or unsubstantiated claims.

Analysis data base shows that well-known manufacturers and sellers of consumer goods and services do not send unsolicited E-mail. Rather, these merchants use solicited E-mail to give their consumers information they have requested about available products, services and sales.

For example, consumers may agree in advance to receive information about newly published books, online catalogs or weekly E-mails about discounted air fares. These examples demonstrate the value of consumer sovereignty to the growth of Internet commerce. When consumers are able to choose the information they receive over the Internet, they seem more likely to have confidence in its content and in the sender.

Conversely, when unsolicited information arrives in consumers' electronic mailboxes, the consumers who have contacted the Commission say they are far less likely to engage in commerce with the sender.

As government, industry and consumer interests examine legislative, self-regulatory and law enforcement options at this important turning point, it is useful to be mindful of lessons learned in the past. Earlier in this decade, the advent of the first and still most universal interactive technology, the 900 number, telephone-based, pay-per-call technology held great promise. Unfortunately, unscrupulous marketers quickly became the technology's most notorious users.

Although the FTC and State attorneys general brought dozens of enforcement actions to halt these schemes, and warned legitimate 900 number vendors that industry practices needed to improve, the industry did too little too late to halt the widespread deception. And Congress enacted the Telephone Disclosure and Dispute Reso-

lution Act of 1992, directing the FTC and the FCC to regulate 900 numbers by issuing rules under the Administrative Procedures Act.

The regulations have forced all 900 number vendors into a standard practice of full disclosure of cost and other material terms, and have virtually eliminated the problem of deceptive 900 numbers advertising. The Commission has steadfastly called for self-regulation as the most desirable approach to Internet governance. We still believe that economic issues related to the development and growth of economic commerce should be left to industry, consumers and the marketplace to resolve. But for problems involving deception and fraud, the Commission is committed to law enforcement as a necessary response.

Should the Congress enact legislation granting the Commission new authority to combat deceptive UCE, we will act carefully but swiftly.

Thank you, Mr. Chairman.

[The prepared statement of Ms. Anthony follows:]

PREPARED STATEMENT OF SHEILA FOSTER ANTHONY, COMMISSIONER, FEDERAL TRADE COMMISSION

Mr. Chairman, I am Sheila Foster Anthony, Commissioner of the Federal Trade Commission. 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, and the Federal Trade Commission's program to combat deceptive and fraudulent unsolicited commercial e-mail.[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. The Commission undertakes this mission by enforcing 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 the exception of certain industries, 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. Not all UCE is fraudulent, but the Internet's capacity to reach literally millions of consumers quickly and at a low cost through UCE has been seized on by fraud operators, who are often among the first and most effective at exploiting any technological innovation. In fact, UCE has be-

[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 approximately 40 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 approximately 30 rules governing specific industries and practices, e.g., the Used Car Rule, 16 C.F.R. Part 455, which requires used car dealers to disclose warranty terms via a window sticker; the Franchise Rule, 16 C.F.R. Part 436, which requires the provision of information to prospective franchisees; and the Telemarketing Sales Rule, 16 C.F.R. Part 310, which defines and prohibits deceptive telemarketing practices and other abusive telemarketing practices.

[3] Certain entities, such as banks, savings and loan associations, and common carriers, as well as the business of insurance are wholly or partially exempt from Commission jurisdiction. See Section 5(a)(2) of the FTC Act, 15 U.S.C. § 45(a)(2) and the McCarran-Ferguson Act, 15 U.S.C. § 1012(b).

come the fraud artist's calling card on the Internet. The staff of the Commission has reviewed a collection of over 100,000 pieces of UCE. Much of it contains false information about the sender, 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.

While bulk UCE burdens Internet service providers and frustrates their customers, the FTC's main concern with UCE is its widespread use to disseminate false and misleading claims about products and services offered for sale on the Internet. 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. Today, Congress, law enforcement and regulatory authorities, industry leaders and consumers are faced with important decisions about the roles of self-regulation, consumer education, law enforcement, and government regulation in dealing with UCE and its impact on the development of electronic commerce on the Internet.

II. THE FEDERAL TRADE COMMISSION'S APPROACH TO EMERGING MARKETPLACES

A. Law Enforcement

Deceptive UCE is a small part of the larger problem of deceptive sales and marketing practices 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 36 law enforcement actions to halt online deception and consumer fraud.

The Commission brings to this task a long history of promoting competition and protecting consumers in other once-new marketing media. These past innovations have included door-to-door sales, television and print advertising, direct mail marketing, 900 number sales, and telemarketing. The development of each of these media was marked by early struggles between legitimate merchants and fraud artists as each sought to capitalize on the efficiencies and potential profits of the new marketplace. 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]

B. Monitor and Study Industry Practices

The Federal Trade Commission closely monitors the development of commerce on the Internet. Through a series of hearings and public workshops, the Commission has heard the views of a wide range of witnesses and issued reports on the broad challenges posed by the rapid growth of the Internet and electronic commerce. In the fall of 1995, the Commission held four days of hearings to explore the effect of new technologies on consumers in the marketplace. Those hearings produced a staff report, Anticipating the 21st Century: Consumer Protection Policy in the New High-Tech, Global Marketplace.[8] The report warned of the potential for the Internet to become the newest haven for deception and fraud.

In 1995, the Commission also began its privacy initiative to explore online information practices used by Internet merchants. The Commission has held a series of public workshops to explore privacy issues and identify voluntary practices that could, if utilized, protect consumers' personally identifiable information when they

---

[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. Section 13(b) of the FTC Act authorizes the Commission to bring actions to enforce Section 5 and other laws the Commission enforces in United States District Courts to obtain injunctions 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 (§ 18).

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

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

[8] May 1996.

visit the Internet.[9] Two weeks ago, the Commission issued Privacy Online: A Report to Congress, which includes an evaluation of self-regulatory efforts to protect consumers' privacy online.[10]

III. THE COMMISSION'S APPROACH TO UNSOLICITED COMMERCIAL E-MAIL

A. Monitoring the Problem

The Commission's staff has similarly studied the widespread use of unsolicited commercial e-mail and whether it poses risks to consumers online. At its June 1997 Privacy Workshop, 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. The Commission's immediate concern has been with deceptive UCE, and in letters dated July, 31, 1997 to Senator John McCain, Chairman, Senate Committee on Commerce, Science and Transportation and Representative Thomas Bliley, Chairman, House Committee on Commerce, the Commission pledged to use its authority to investigate and bring law enforcement actions against deceptive spammers. The Commission also asked industry and advocacy groups to study the economic and technological burdens caused by UCE and to report back on their findings. Under the leadership of the Center for Democracy in Technology, these groups have spent a year analyzing economic and technological problems and identifying possible solutions. They will present their report to the Commission in July.

Since the June 1997 workshop, Commission staff has collected and analyzed a large amount of UCE received by consumers; sent warning letters to over 1,000 senders of apparently deceptive UCE; prepared and disseminated consumer education materials; and brought law enforcement actions to halt deceptive marketing campaigns that used UCE to cause significant economic harm to consumers. Last summer, the FTC set up a special electronic mailbox reserved for UCE. 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 to forward their UCE to it. The UCE mailbox has received more than 100,000 forwarded messages to date, including 1,000 to 1,500 new pieces of UCE every day. Staff enters each UCE message into a searchable database, analyzes the data, identifies trends, and uses its findings to target law enforcement and education efforts.

The largest category of UCE in the FTC's database is chain letters, followed closely by pyramid scheme solicitations. Both schemes make money for only the first few participants. Our experience with pyramid marketing schemes supports the conclusion that 90% or more of investors are mathematically certain to lose their investment. Some chain letters masquerade as legitimate businesses, in which participants receive "reports" or other worthless items in exchange for their payment. Pyramid schemes pose as legitimate multi-level marketing companies. Fees paid by new recruits, not profits from the sale of goods, generate most of their revenue. Both pyramid schemes and chain letters are illegal.

B. Aggressive Law Enforcement

The Commission has responded to the large amount of chain letter and pyramid UCE with comprehensive consumer and business education programs and tough law enforcement. For example, in October 1997, the Commission sued Nia Cano, doing business as Credit Development International and Drivers Seat Network.[11] In that lawsuit, the Commission alleged that the defendants falsely promised that investors would receive both an unsecured VISA or MasterCard, and could earn $18,000 a month by recruiting others into the scheme. The defendants urged participants to use bulk e-mail to solicit recruits, and an estimated 27,000 participants flooded the Internet with UCE repeating the defendants' allegedly false offer. The Commission obtained a Temporary Restraining Order and Preliminary Injunction against these defendants, freezing over $2 million for restitution to victims. This case is still in litigation.

---

[9] FTC Staff Report: Public Workshop on Consumer Privacy on the Global Information Infrastructure, Dec. 1996; FTC Report To Congress: Individual Reference Services, Dec. 1997.

[10] June 4, 1998. The report concluded that self-regulatory efforts, thus far, have fallen short of what is necessary to ensure adequate privacy protections on a widespread basis. The Commission recommended that Congress develop legislation to protect children's privacy online, and indicated that it would make further recommendations relating to online consumers generally later this summer.

[11] *FTC* v. *Nia Cano,* Civil No. 97–7947–IH–(AJWx) (C.D. Cal, filed Oct. 29, 1997).

The staff has taken aggressive steps to deter others who use UCE to promote chain letter and pyramid schemes. Last February, with the assistance of the United States Postal Inspection Service, the Commission put more than 1,000 junk e-mailers sending UCE on notice that law enforcement agencies are monitoring UCE for deception and fraud and keeping track of the senders. The Commission sent letters warning senders that their e-mail may violate federal law, advising them of relevant laws, and inviting them to visit the FTC's web site, www.fte.gov, for further guidance. Staff continues to monitor the UCE database to make sure that those who have been warned do not resume sending deceptive UCE. If the Commission finds that senders of deceptive UCE who have been warned continue to send deceptive messages, however, it will take appropriate action.[12]

In addition to online pyramid schemes and chain letters, the FTC's UCE database contains other categories of possibly deceptive UCE. These categories mirror schemes that have proliferated in other media: business opportunity offers and work-at-home schemes, guaranteed credit cards and loans, credit repair schemes, and diet or health products making false or unsubstantiated claims. As in the case of pyramids and chain letters, Commission staff is monitoring and has sent warnings to senders of these messages, and the Commission has brought enforcement actions against two of them.[13]

C. Comprehensive Consumer and Business Education

The Commission has published three consumer publications related to UCE in the last few months. *Trouble @ the In-Box* identifies some of the scams showing up in electronic in-boxes. It offers tips and suggestions for assessing whether an opportunity is legitimate or fraudulent, and steers consumers to additional resource materials that can help them determine the validity of a promotion or money making venture. To date, approximately 27,000 copies of the brochure have been distributed, and it has been accessed on the FTC's web site approximately 3,300 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 drive. A number of corporations and organizations have provided a link from their web site to the tips on the FTC's web site, including Circuit City, Borders Group Inc., Netcom, Micron, and Compaq. Approximately 22,000 copies of the bookmark have been distributed, and it has been accessed nearly 3,000 times on the FTC's web site.

The brochure *Net-Based Business Opportunities: Are Some Flop-portunities?* educates consumers about fraudulent Internet-related business opportunities. The brochure offers examples of the kinds of fraudulent solicitations that consumers may see in broadcast and print media, at seminars or trade shows and in UCE. The brochure also offers tips on how to avoid being scammed by fraudulent marketers making bogus offers. Nearly 18,000 brochures have been distributed, and it has been accessed approximately 1,200 times on the FTC's web site.

D. Considering the Future In Light of Past Experience

In the past year, Commission staff has investigated spamming and the extent to which consumers fall victim to misleading offers. Where staff's investigations revealed significant economic harm to recipients who responded to deceptive UCE, the Commission has taken enforcement action. While neither the Commission's UCE database nor staff's interviews with consumers constitute a representative sample of all UCE and UCE recipients, it is notable that in the Commission's experience to date, few consumers have actually lost money responding to deceptive UCE. However, a deceptive spammer can still make a profit even though very few recipients respond because the cost of sending bulk volume UCE is so low—far lower than traditional mail delivery. Whether consumers respond to deceptive UCE by either becoming victims or "flaming" senders (i.e., sending angry return e-mails), forwarding their UCE to the FTC, or automatically deleting all of their UCE, the Commission

[12] It should be noted, however, that because of the ease with which senders change screen names and e-mail addresses, and the widespread use of false routing information, it is difficult to keep track of many senders of UCE.

[13] *FTC* v. *Internet Business Broadcasting, Inc.*, Civil No. WMN–98–495 (D.Md. filed Feb. 19, 1998) (Defendants' UCE and home page contained allegedly false income claims for business opportunity); *FTC* v. *Dixie Cooley*, Civil No. CIV–98–0373–PHX–RGS (D.Ariz., filed Mar. 4, 1998) (Defendant used UCE to promote an allegedly fraudulent credit repair scheme).

As these cases illustrate, the Commission's focus has been on deceptive UCE. To the extent UCE is not deceptive, the Commission's ability to challenge it may be circumscribed.

is concerned that the proliferation of deceptive UCE poses a threat to consumers' confidence in the Internet as a medium for personal electronic commerce.

Analysis of the Commission's UCE database shows that well-known manufacturers and sellers of consumer goods and services do not send UCE. Rather, these 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. When consumers are able to choose the information they receive over the Internet, they seem likely to have more confidence in its content and in the sender. Conversely, when unsolicited information arrives in consumers' electronic mailboxes, the consumers who have contacted the Commission have been far less likely to engage in commerce with the sender.

As government, industry, and consumer interests examine legislative, self-regulatory, and law enforcement options at this important turning point, it is useful to be mindful of lessons learned in the past. Earlier in this decade, the advent of the first and still the most universal interactive technology, 900 number, telephone-based "pay-per-call" technology, held great promise. Unfortunately, unscrupulous marketers quickly became the technology's most notorious users. Scores of thousands of consumers wound up with charges on their telephone bills for calls to 900 numbers that they thought were free. Others were billed for expensive calls made by their children without parental knowledge or consent.

The FTC and State attorneys general brought dozens of enforcement actions to halt these schemes and warned legitimate 900 number vendors that industry practices needed to improve dramatically. Unfortunately, industry did too little to halt the widespread deception, and Congress enacted the Telephone Disclosure and Dispute Resolution Act of 1992, directing the FTC and FCC to regulate 900 number commerce by issuing rules under the Administrative Procedures Act. The regulations have forced all 900 number vendors into a standard practice of full disclosure of cost and other material terms, and have virtually eliminated the problem of deceptive 900 number advertising. All of this came at a considerable cost, however, because consumers lost confidence in pay-per-call commerce and stayed away from it in droves. Only now, some four years after federal regulations took effect, has there been growth in pay-per-call services as a means of electronic commerce.

The Commission has steadfastly called for self-regulation as the most desirable approach to Internet governance. The Commission still believes that economic issues related to the development and growth of electronic commerce should be left to industry, consumers, and the marketplace to resolve. For problems involving deception and fraud, however, the Commission is committed to law enforcement as a necessary response. Should the Congress enact legislation granting the Commission new authority to combat deceptive UCE, the Commission will act carefully but swiftly to use it.

Senator BURNS. Commissioner, thank you very much. And thank you for coming this morning.

We have been joined by two of our colleagues that have a very big interest in this issue. And they may have a question or two for you. And I would call upon my good friend from Alaska, who chairs the Energy and Natural Resources Committee. And, gentlemen, let me say thank you for your patience this morning. We got started right on time. We have a conference this morning at 10:30, and we only have an hour. And I want to get to as many of my witnesses as I possibly can.

So, I would call on Senator Murkowski. Thank you for coming this morning.

STATEMENT OF HON. FRANK MURKOWSKI, U.S. SENATOR FROM ALASKA

Senator MURKOWSKI. I have a brief statement. Mr. Chairman, I want to compliment you for holding this hearing—I think it is very timely—and also for your expertise in the area of communications,

which you have led as subcommittee chairman of the Commerce Committee.

I do not know if you recall the first time you ran into Spam. I do. I was a youngster during the second world war. It seemed to me the cartoons at that time showed in the soldiers' rations a can of Spam and a package of cigarettes. And they threw the Spam away and kept the cigarettes. But I do not know whether there is any timely message there or not. [Laughter.]

But, in any event, as you have said time and time again, it is inappropriate to go down to many rabbit trails when we are in a hurry. But what we have today of course is junk mail known as spam. It is an issue of growing concern to many members, including Senator Torricelli and myself. It is a big business. Internet service providers and government agencies responsible for controlling fraud all have an interest in this. Junk E-mail is a particular burden, however, on many rural people in my State and in your State of Idaho, who must pay a significant long distance charge to access the Internet, just simply to get their E-mail.

For instance, rural users with less than high quality, but average, telephone connections may spend more than 10 minutes a day just downloading junk E-mail, just to get the E-mail that they want. This costs an average Montanan or Alaskan constituent, who must pay about $6 an hour for a long distance surcharge to access America Online via a 1–800 number—and that is as much as 50 minutes a week—could mean $24 of additional charges a month. And the individual would have no choice. That is just the reality of what it takes to pull down your own E-mail.

So, I am pleased to see the panel testifying before you today. Joe Keeley of my staff and a number of others have worked diligently on this. I think it is fair to say that each of the witnesses today has participated, along with many other members and their staffs, in a workshop which was created at the request of the Federal Trade Commission.

The leader of the workshop, as I understand it, was Ms. Mulligan, who is with us today. And with the Center for Democracy and Technology, is to be commended for her efforts in hosting the forum, with a variety of views which were expressed at those forums and thoroughly debated. So, we look forward to the release of the final report on the workshop within the next few weeks.

We have been working to address the issue of junk mail for well over a year. Recognizing that junk E-mail has been a problem that deserved legislative attention, I introduced Senate bill 771 last May. Based upon comments that I have received from many interested parties and the work of CDT, I along with my colleague who is here today, Senator Torricelli, added a provision to the Telephone Slamming bill. And that is when you are basically taken off one carrier and put on another without your knowledge. That would represent a first step in controlling some of the problems of junk E-mail. And our measure would weed out the bad actors on the Internet by requiring identification of online marketers as well as requiring that "Remove" requests are honored.

For some in the Internet community, our solution, of course, does not go far enough. They propose an outright ban on unsolicited E-mail. I think such a ban would establish a dangerous precedent. It

would erode the protection of the first amendment. The government should simply not dictate, in my opinion, what a consumer sees in his or her E-mail box. We have been down that road before with the Communications Decency Act, which the chairman was involved in.

The Supreme Court, by unanimous vote, has made it very, very clear what it thinks of such sweeping bans on Internet material. Consumers, I think, should have the final word in deciding what comes into their mailboxes, and not the U.S. Government.

So, finally, Mr. Chairman, I would finish my statement this morning by pointing out that there are numerous views. And from your witness list, they are certainly going to be well represented before you today. So, thanks for the opportunity to spend a few minutes. And let me congratulate Ms. Anthony for her statement, as well.

And if you would excuse me, I will take my leave.

[The prepared statement of Senator Murkowski follows:]

PREPARED STATEMENT OF HON. FRANK H. MURKOWSKI, U.S. SENATOR FROM ALASKA

Thank you Mr. Chairman for calling this important hearing. Junk e-mail, also known as spam, is an issue of tremendous concern to consumers, businesses, Internet Service providers, and government agencies responsible for controlling fraud. Junk e-mail is a particular burden to our rural constituents in Alaska and Montana who must pay a long charge to access the Internet.

I am pleased to see the panel testifying before you today. Each of the witnesses today has been participating along with myself in a workshop created at the request of the Federal Trade Commission. The leader of this workshop, Dierdre Mulligan of the Center for Democracy and Technology, should be commended for her efforts in hosting a forum where a variety of views were expressed and debated. I look forward to the release of a final report of this workshop within the next few weeks.

I have been working to address the issue of junk e-mail for over a year. Recognizing that junk e-mail is a problem that deserves legislative attention, I introduced S. 771 last May. Based upon comments that I received from many interested parties and the work of CDT, I along with Senator Torricelli added a provision to to the telephone slamming bill that represents a first step in controlling the problem of junk e-mail. Our measure will weed out the bad actors of the Internet by requiring identification of online marketers as well as requiring that "remove" requests are honored.

For some in the Internet community, our solution does not go far enough. They propose an outright ban on unsolicited e-mail. I believe such a ban would establish a dangerous precedent and would erode the protections of the First Amendment. The government simply should not dictate what a consumer sees in his or her mailbox. We have been down this road before with the Communications Decency Act. The Supreme Court by a unanimous vote has made very clear what it thinks of such sweeping bans on Internet material. Consumers should have the final word in deciding what comes into their mailboxes, not the government.

Finally, Mr. Chairman, I will finish my statement this morning by pointing out that there are numerous views on this issue and they are well represented before you today.

Thank you again for holding this hearing.

Senator BURNS. Senator Murkowski, thank you very much. And we appreciate your concern and we appreciate the work that you have done on this.

We have been joined now by Senator Torricelli, who has similar concerns. Your full statement, Senator, will be made part of the record.

I never asked Commissioner Anthony if she would take questions from the Senators, but I suppose she would. But if you would like to ask her—she had a very forthright statement on this, and it

sounds like the problem is much larger than I think most of us realize at this point.

Thank you for joining us this morning.

STATEMENT OF HON. ROBERT TORRICELLI, U.S. SENATOR FROM NEW JERSEY

Senator TORRICELLI. Thank you, Mr. Chairman. I have read the Commissioner's statement. I did not want to address questions to her but, like Senator Murkowski, wanted to thank you for holding this hearing and giving me this opportunity, and briefly just to share a couple of comments with you.

First, I am grateful to have joined with Senator Murkowski in offering our junk E-mail amendment, and to Senator McCain, who has also offered his assistance throughout the course of the year. It is also important to acknowledge that there is no one approach to dealing with the proliferation of junk E-mail. Congressman Chris Smith, of New Jersey, has a different approach, in an outright ban, an approach that I would support, but have some constitutional reservations about.

Last year, we came together, many of us who share this concern, recognizing that there is a growing threat to Internet commerce and communication because of what Senator Murkowski has rightfully identified as the spam problem. It may be a problem in rural Alaska, but I can assure you it is also a problem in suburban New Jersey. And it is even a problem in this institution.

My official Senate E-mail address is inundated with E-mail every day. Even doing business in the U.S. Senate is being complicated. And this is not something that affects American life in the margins any longer. Sixty-two million Americans use the Internet every day, and traffic is doubling every 100 days.

Every American, in their business, in communication with their family, in access to general information, is going to be impacted by this problem of junk E-mail. Indeed, it is estimated today that 30 percent of all E-mail traffic could be junk mail, unwanted, unsolicited, interfering with commerce and everyday American life.

The problem is that not only is the problem large and growing, but the incentive is for even larger abuse. E-mailing millions of people can cost a few hundred dollars. There is no other form of communication in the country on any kind of economic basis that begins to compare. So, it is an invitation for even further abuse.

The question of course is how to deal with this on a constitutional basis, and without having the Government inappropriately involved in regulating the Internet. I would like to see government interference at a minimum, while offering some basic protection. The need for protection is also not just one of convenience, which is important in making this case of why we need to do anything at all.

If it were simply an inconvenience, it might be all right to be left alone. Last March, spammers crashed the Pacific Bell's network, leaving customers without service for 24 hours. So, it is not simply that this is an annoyance; it can break down the entire system.

I think, in the Murkowski-Torricelli approach, we have got the right balance. It does not go quite as far as Congressman Smith has gone, with a complete ban. Instead, it empowers E-mail users,

the customers, by doing several things. First, it gives citizens the power to stop future junk E-mail by replying to the sender. Federal law will give the E-mail addressee the right to stop E-mail to their address. Just as a citizen can go the post office and stop the delivery of mail to their home, or have an unlisted phone number for their telephone, it gives them some basic level of protection.

Second, the amendment would require junk E-mailers to identify themselves. If people from corporations knew that the receiver could identify who they were, they would not be as abusive, they would be much more careful about interfering with people's E-mail. This is simply a question of taking the cloak of secrecy off those who are originating all of this junk E-mail.

Mr. Chairman, I think that we have a fair and a balanced approach that addresses the ability of families and businesses to protect themselves. It prevents the breakdown of this vital new area of commerce, while being responsible to constitutional concerns of the right of people to use the Internet, and minimizing government involvement.

The Internet is one area of American life, communication and commerce where we have a chance to start all over again, keep the Government's role at a minimum, keep it free, fair and open. But that does not mean open to abuse and doing nothing.

Senator Murkowski and I have given you a suggestion that strikes that fair balance. And I appreciate very much the chance to present it to you today.

Senator BURNS. Thank you very much, Senator.

Just sitting here, trying to figure out how we craft legislation, but also I would like to ask you a question. It appears to me that this is going to be one of those issues that it is going to take a massive amount of educating the consuming public.

Senator TORRICELLI. I think it does, Mr. Chairman. Though I have been surprised, in discussing this around the country, how sophisticated the public is with the problem. In many respects, this is one where the American people are significantly ahead of their Congress. Because many Americans who run their businesses on the Internet and communicate with family and friends on the Internet, beyond what most of us are doing in the Senate, they are living this problem more than we are. They are aware of it more than we are. You may be surprised how far ahead of us they are.

Senator BURNS. Well, they usually are. [Laughter.]

That is the great elasticity and the imagination of the American people. They are always ahead of us a little bit, even whenever we thought we were ahead of the curve. You know, we started to restructure the communications industry, as you well know. And, again, we were behind the curve there.

Commissioner Anthony, I would just like to ask you, do we have to approach this problem with the same mind set as we did with the 900 numbers?

Ms. ANTHONY. Senator, I think it would be a very good model to utilize, particularly in the way that you might go about it—if, for example, you gave us the authority to enforce this area of the law—to conduct a rulemaking under the Administrative Procedures Act, which can be done very quickly. And also we would be happy

to work with you to refine legislation and to share with you the benefit of our experience and what we know about E-mail.

Senator BURNS. Now, we get junk mail. The postman brings us junk mail and puts it in our mailbox. But that does not cost us anything. And we can sort of see it in front of us and then just throw it away. There is a huge difference between electronic junk mail and the junk mail that you receive through the Postal Service.

Ms. ANTHONY. You are right about that. Because the recipient bears much of the cost and the service providers bear much more of the cost than the sender does. And the sender, for example, in the area that we look at, in deception and fraud, the sender, for very little amounts of money, does not need a big return when he sends out 100,000 pieces of E-mail. If he just gets a little back, it is very profitable for him.

So, we would like to see this stopped. And we would be happy to work with you in any way that we possibly can. I think the Senate's bill, Senators Murkowski and Torricelli's bill, strikes a fair balance, because it identifies deception as an extremely important problem, but it also gives the consumer the right to opt out of receiving E-mail, just as you have given consumers the right under telemarketing and junk mail.

Senator BURNS. Obviously you have looked into this with some depth. And I would ask both of you if this legislation provides an opt out for the consumer. That still does not prevent that person from receiving the first piece.

Ms. ANTHONY. That is true, it does not. But if the routing information is correct and there is something in your bill that requires the sender to identify himself, my best guess is that that will stop a great deal of the fraud.

Senator BURNS. Do senders identify themselves?

Ms. ANTHONY. No. In the fraudulent area, they usually give fictitious names and false messages. They can also route through a third party. So, it is very difficult for recipients to determine in fact who is sending them this E-mail.

Senator BURNS. Senator Torricelli, take a State like New Jersey. I would imagine that you are in a State—and this is a problem, where the person that wants to defraud and the people they are wanting to defraud, it does not make any difference where you are in this country electronically.

Senator TORRICELLI. Unfortunately technology has provided the one perfect new vehicle for fraud and abuse of our citizens. For all the wonders of the Internet, this is an opportunity for someone anywhere in the country, hiding in the complete cloak of secrecy, to issue these E-mail messages and perpetuate a fraud upon the American people. And that is exactly what is happening.

It is something that I think has a relatively easy solution. As Commissioner Anthony suggested, if these people are required to give, under penalty of Federal law, to properly identify themselves, where they are and who they are, you may get their message once, but if you do not like it and you do not want it and you do not want anything to do with them, you stop them.

So, yes, they get one shot free. And I think, constitutionally, we probably have to give them that. But that is all they get.

Senator BURNS. I am just looking down the questions here before—both of you I know have got other things to do today; this is not the only thing you have got going. And the next panel has to do with those folks who are involved in the Internet and its operation, which we have some more questions for. But that is all the questions I have at this time.

I want to thank both of you for your statements. And I appreciate your coming down this morning.

Ms. ANTHONY. Thank you, Senator.

Senator BURNS. And we want to work with you, too. And as this legislation moves along, we will be seeking, probably, advice on what you can do and what you cannot do as this moves through the Congress.

Ms. ANTHONY. We would be happy to provide it.

Senator BURNS. And we would hope that with the problem as you have described, the legislation is timely and needs to be moved.

Senator TORRICELLI. Thank you.

Senator BURNS. Thank you.

Now, we will call the next panel, Mr. Randall Boe, who is the associate general counsel for America Online; Jerry Cerasale, who is vice president, Direct Marketing Association; Ray Everett-Church, who is co-founder of the Coalition Against Unsolicited Commercial E-mail; and Dierdre Mulligan, staff counsel for the Center for Democracy and Technology.

We appreciate you coming this morning. We may have set an all-time record of a hearing scheduled to start at 9:30 a.m., and you are already at the table at 10. That is unusual in this 17 square miles of logic-free environment. [Laughter.]

I got a message the other day from a good friend of mine who was in the chair, and his replacement was 15 minutes late getting there, and he sent me a message down on the floor that says, rescue me from the cave of the winds.

We look forward to your testimony this morning.

Mr. Randall Boe, associate counsel for America Online. Thank you for coming this morning. And if you want to consolidate your statement, you may. If you have a longer statement, it will be made part of the record of this hearing.

STATEMENT OF RANDALL BOE, ASSOCIATE GENERAL COUNSEL, AMERICA ONLINE

Mr. BOE. Thank you, Senator Burns. And thank you for the opportunity to testify here. I do have a written statement that we will supply you, but I would like to give you a few comments first, if that is all right.

I am the associate general counsel at America Online, and helped develop AOL's unsolicited bulk E-mail policies, and I also head up our litigation efforts against spammers. And what I would like to do very briefly is give you a dispatch from the front lines of our war against spam. And that is how we view it at America Online. It has quickly become the largest single complaint of our members, and it is threatening to engulf the entire Internet.

We handle right now on a daily basis almost 30 million E-mail messages. And to give you an idea about the growth, 18 months ago we handled about 5 million E-mail messages every day. Our es-

timate is that as much as 30 percent of those 30 million E-mail messages may be junk E-mail.

You correctly identified an important distinction between junk mail in the offline world and junk mail in the online world. Last night, when I arrived home from work, I did what millions of Americans do, I picked up the mail and browsed through it. And there were four or five pieces of junk mail. But there are a couple of important differences between the junk mail I get in my mailbox on the front door of my house and the junk mail that floods Internet users' E-mailboxes.

First, I do not pay a dime to receive junk mail delivered by the Postal Service. I do pay, through higher service fees and through hourly plans if I am an hourly subscriber to an online service, to receive junk E-mail. Second, the person delivering or the company delivering the junk mail in the online world pays nothing to have that delivered. Whereas in the offline world, the junk mailers are required to at least pay the cost of delivering their mail.

Third, I can identify from whom I receive U.S. mail. Fourth, and I think a very critical point, I do not have a concern about my 6-year-old daughter wading into the mail in the mailbox at home and receiving inappropriate or pornographic images. I do not have that same assurance right now using the Internet and Internet E-mail.

None of those distinctions apply for spammers. First of all, consumers have to pay for the cost, in many instances, of receiving spam. Second, service providers, like AOL, bear enormous costs in terms of additional servers, additional capacity on the computer network, as well as personnel and time to deliver this huge flood of unsolicited mail.

Third, the standard operating procedure for spammers is to falsify the transmission data, so that it is impossible to tell with any accuracy where the mail actually came from. Which is intended, first of all, to prevent angry consumers from actually being able to reply to the person sending the E-mail, and second, to defeat the technological efforts of companies like AOL to prevent the spam from getting into the network.

And, fourth, and I think most problematically, while we offer tools to help parents select the right content for their children online, spammers, by sending pornographic E-mail without regard to the age or the sensibilities of the recipients, almost make a mockery of that entire process. And that is a significant problem for us.

We are fighting spam on a number of fronts at AOL. First of all, we have deployed probably the most stringent anti-spam policies in cyberspace. We strictly prohibit the use of AOL accounts to send unsolicited junk mail. We prevent the use of AOL accounts to harvest screen names to compile mailing addressed, or to do anything else that facilitates the transmission of junk mail.

In addition, we do not sell or distribute lists of our members' E-mail addresses. And we take extensive precautions to maintain our members' privacy. Second, we have developed some of the most robust technological tools available to try and block spam before it even enters our network, and before it gets distributed to our customers.

Third, we have created an extensive set of tools for our members to give them control over the E-mail they receive. Our members have the ability to create a list of people from whom they would like to receive E-mail, as well as blocking E-mail that they do not want to receive.

And, finally, we have waged a long and costly battle against spammers. In the last 9 months, we have filed suit against more than 20 junk E-mailers, and will probably sue five to six more this week.

We are pleased to see other companies step into the fray, but we think that there is a role for the Government, as well. We think that any legislative proposal should, one, outlaw the falsification of transmission data in E-mail, clarify that existing statutes, like the Computer Fraud and Abuse Act, do apply to E-mail, and add statutory civil penalties for spammers who are sending E-mail in an unauthorized fashion, and give ISP's the ability to recover the costs of bringing suit against these people to stop the sending of junk E-mail.

We think that junk E-mail is a problem that pervades the entire Internet, and poses a risk to the development of Internet commerce. And we think it requires a coordinated approach. We look forward to working with you, as well as the rest of our industry, to try and resolve this matter in a way that is beneficial for consumers and the Internet as a whole.

Thank you for the opportunity to testify.

[The prepared statement of Mr. Boe follows:]

PREPARED STATEMENT OF RANDALL BOE, ASSOCIATE GENERAL COUNSEL, AMERICA ONLINE

Mr. Chairman, members of the Subcommittee, my name is Randall Boe, and I am Associate General Counsel of America Online, Inc. In my position, I helped develop AOL's policy on unsolicited bulk e-mail, and I head up AOL's litigation efforts against spammers.

America Online is the world's largest online service, with over twelve million members. We offer our members a range of services, including e-mail, instant messages and access to the world-wide web and proprietary content developed by AOL and our partners. We also provide a range of tools that allow members to customize their and their children's online experience.

As you might expect, AOL has very broad experience with spam, or unsolicited bulk e-mail (UBE), experience which I hope will be of help as the subcommittee looks at this problem. Junk e-mail is one of the most serious issues facing not only AOL, but the Internet as a whole. The reasons are straightforward:

- Junk e-mail generates a tremendous volume of complaints—At AOL we receive thousands of complaints a week about junk e-mail, and
- The senders of junk e-mail misappropriate the network and computer resources of Internet Service Providers.

It is an unfortunate fact that even brand new Internet users are confronted with junk e-mail—almost as soon as they go online. The problem is not just that junk e-mail tends to promote hoaxes, scams and get-rich quick schemes-it is the sheer volume that confronts many users every time they open their mailbox. Lately, another worrisome trend has emerged—junk e-mailers indiscriminately sending messages promoting pornographic Web sites without regard to the age or sensibilities of the senders. Over the past year, the amount of e-mail traffic on AOL has continued to explode as consumers and business subscribers discover the benefits of the online medium, and the utility of electronic messages. We handle some 30 million messages a day, about half internal to our system, and half over the Internet. You may be surprised to learn that from 5 percent to 30 percent of our Internet e-mail traffic is unsolicited bulk e-mail on any given day.

AOL has attacked the UBE problem on three fronts.

First, AOL has deployed some of the most stringent anti-spam policies in cyberspace. We strictly prohibit the use of AOL accounts to send junk e-mail, to harvest

names or to promote or facilitate the practice of "spamming." It is also AOL's policy not to sell or otherwise distribute lists our Members' e-mail addresses, and we take extensive precautions to maintain our Members' privacy.

Second, we have developed technology for both our systems operators and our Members to block and filter spam. AOL's Mail Controls are easy to use and allow our Members to block email from specific mail address, or entire domains. They can also block all mail from the Internet (accepting only mail from AOL Members) and create a "permit list" of address they will accept mail from. Finally, they can block mail with attachments. While these tools do stop some UBE, junk e-mailers are proficient at subverting consumer safeguards and have no qualms about doing so. This willingness to game the system is one of the central problems with junk e-mailers and discussed in greater detail below.

Third, AOL has waged a series of court battles against spammers. In the last nine months, AOL has brought cases against more than 20 junk e-mailers—and we have yet to lose a case. We have been successful in obtaining injunctions barring spammers from sending their unsolicited mail to AOL members and fully expect to obtain significant monetary awards from them.

One excellent example of AOL's litigation campaign against junk e-mail is AOL's case against a company called Over the Air Equipment. Over The Air used deceptive practices, including falsifying e-mail transmission data, to avoid AOL's mail controls and to repeatedly transmit vast quantities of unsolicited e-mail to AOL members—all of it promoting a "cyber-stripper" service. To further confuse AOL subscribers, Over the Air copied an America Online trademark fraudulently suggesting that their site had AOL's approval. Over the Air Equipment blatantly ignored AOL member requests to be removed from Over the Air's spamming lists and continued to transmit unwanted junk e-mail to frustrated AOL members.

AOL won a preliminary injunction against Over the Air from a federal judge in Virginia. In December of last year, Over the Air Equipment agreed to a court order which prohibits the company from ever sending unsolicited e-mail to AOL members again. Over the Air Equipment also agreed to pay AOL a substantial sum of money in damages.

This case adds to a growing body of precedent that spammers do not have the right to appropriate the computer network of companies and bombard Internet users with unwanted and objectionable email in disregard of that networks policy against spam.

Despite these efforts, UBE remains a problem for service providers and their customers. These efforts have not been more successful because junk e-mailers are willing to game the system.

They forge the return addresses on UBE and they do not respond to requests to be removed from their lists. In fact, they use remove requests to compile lists of active addresses to spam. They are not concerned with the cumulative effect of UBE from all sources, either on the network itself, or on prospective customers.

They bear virtually none of the costs of sending their mail: in fact the cost of sending a million messages is the same as the expense of one, so they see no need to differentiate target groups. At the same time, ISP's and their customers are forced to shoulder those expenses. Among AOL's subscribers, 15 percent are on plans which meter, and charge for, time spent online. This group has to pay directly for the chore of personally screening and deleting messages most don't want in the first place.

There are several common tactics spammers use:

- One popular practice is called "dynamic" sender UBE, in which the sender address changes after every few messages while the domain remains the same, to prevent detection as a bulk mailing.
- Another common practice is to rotate the mail-out among several sites or domains making the activity difficult to identify as a bulk mailing.
- Yet another includes the use of forged or fictitious Internet domains.
- Increasingly the problem of relaying messages through unaffiliated servers for the purpose of disguising the source of message (which has been a problem for some time) has taken a turn towards the International arena—more and more senders are relaying off of foreign sites.
- Harvesting and distributing e-mail addresses.
- Distributing software that facilitates spammers and the falsification of transmission data.

To protect ourselves and our subscribers, we have experimented with software techniques to screen all messages from broad Internet addresses or domains which are known sources of UBE, but it is easy for a spammer to obtain a new address and move the business there in a matter of hours. And even when the hosting ISP is willing to cooperate with us in confronting the spammer, it is also a quick and

easy matter to change ISP's. We have also screened out individual messages with sender addresses of known UBE mailers. However, they have become expert not only in substituting fictitious sending addresses, but indeed in removing all external origination data.

We continue to use these approaches, and to confront identified spammers with demands that they cease unauthorized use of our network and unauthorized e-mail access to our members. If they persist, we have taken them to court and will continue to do so. Our litigation has been groundbreaking and successful. However, the ease, anonymity and proliferation of spamming ensure that we're always playing catch-up.

Consequently, we have had to invest considerable resources to handle the explosion of Internet email.

For these reasons, AOL is willing to see the government step in to a limited extent to help remedy a problem that may be beyond the capacity of any single company or industry to address, a problem which threatens the utility and appeal of the Internet, and, ironically, which threatens to diminish its potential as a true mass medium. Before I identify those areas in which we believe the government could play a constructive role, however, let me make a few critical points about the risk of going too far.

We must draw a distinction between legitimate marketing on the Internet and illegitimate activities which make up the bulk of UBE we see today. For example, when AOL markets to its members, it has a clear incentive to tailor marketing to consumers' preferences and to respond to consumer requests not to receive marketing materials, in order to build a relationship of trust with its members.

Thus, where there is a prior business or other relationship between sender and recipient, targeted marketing can be useful to consumers. Still, receipt of any such marketing should be controlled by the end user—users should have a choice.

In addition, private sector self-regulatory efforts have done some good. AOL has participated the formation of industry guidelines with the Interactive Services Association and the Direct Marketing Association, and we think it is critical for industry associations to take a leadership role in this area. Unfortunately many of the junk mailers are not members of those organizations and not likely to follow their guidelines.

Finally, the global nature of the Internet makes it critical that Congress not try to ban unsolicited e-mail completely. Such an approach would not only be unenforceable but would also undermine the U.S. government's policy that country-by-country content-based legislation is inappropriate.

The underlying message is that Congress and agencies like the FTC must be careful not to delegitimize marketing online while it is trying to deal with fraudulent activities.

Where can the government make a positive contribution? First, by choosing its approaches carefully and wisely. Government restrictions based on content, which require ISP's to open e-mail and use part of its text to filter out UBE, raise not only privacy but First Amendment concerns as well. In addition, given the elusive nature of junk e-mailers, and the tremendous effort involved in actually locating them, there is no reason to believe that they would comply with such a requirement—and no practical prospect for enforcement. We do not believe such suggestions are appropriate.

AOL's litigation efforts against spammers have achieved a substantial level of success—but the problem is not one that can be solved by one company's efforts. What we have seen is that there are gaps in existing law that make it more difficult to successfully prosecute cases against spammers. AOL and other Internet Service Providers have been successful in applying existing statutes and common law to the practice of junk e-mail—but these provisions could be strengthened and focused more specifically on the issues raised by junk e-mailing. Second, the jurisdiction of the FTC is largely predicated on the content of the e-mail.

Specifically, AOL believes legislative action can be taken to:

- Outlaw the forging of sender identification information.
- Make the Computer Fraud and Abuse Act a stronger weapon against junk e-mail.
- Add statutory civil penalties and the opportunity for ISPs to recover court costs and attorneys fees will help.

These steps, supported by the industry litigation and technological efforts will have real benefits for consumers. At the same time, legislation of this scope will not jeopardize legitimate business growth on the Internet and the attendant consumer benefits.

Unsolicited bulk email is a serious consumer and business issue on the Internet. The continued growth of the medium depends, in part, on ensuring UBE does not

overwhelm service providers' computer software and consumers' mailboxes. AOL and the rest of the industry are committed to doing everything we can to thwart the efforts of those who abuse the Internet and ignore the clearly expressed desires of Internet users.

Again, thank you for inviting AOL to testify. I'll be happy to answer any questions you or other members of the Subcommittee may have.

Senator BURNS. Thank you, Mr. Boe.

Now, Jerry Cerasale.

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

Mr. CERASALE. Thank you, Senator. I appreciate the opportunity to be here. And thank you very much, Senator. We appreciate the fact that you are holding this hearing and inviting us here to testify.

I am Jerry Cerasale, the senior vice president for Government Affairs for the Direct Marketing Association. I have a longer statement that I ask to be put in the record.

Senator BURNS. Your full statement will be made a part of the record.

Mr. CERASALE. Thank you.

The DMA represents over 3,600 corporate members who are direct marketers, both domestic and international, their suppliers and support services. And DMA is very interested in regulation of electronic commerce. Over 85 percent of our members are involved in some form of E-commerce. We estimate that E-commerce last year totaled about $4 billion.

With rapid changes in communications technology, we believe that no method of communication for commerce should be eliminated, however. But the DMA agrees that many current uses of unsolicited E-mail are not appropriate for legitimate marketing and must be curtailed. And we think that Congress should examine approaches to eliminate these inappropriate uses without eliminating the medium altogether.

The unsolicited E-mail of today may not be the unsolicited E-mail of tomorrow. Our marketers have been very creative in providing products that American consumers want through the traditional media of mail, telephone and direct advertising, and the DMA believes that the new option of electronic communication should remain open and not be eliminated by government regulation.

We also think that there are a lot of market forces discouraging legitimate companies from engaging in mass, unsolicited E-mail. The field is very customer-oriented. Legitimate companies must provide good customer service and not anger their customers. Therefore, we agree with Senator Torricelli and Senator Murkowski that marketers should identify themselves. And that is required, I think, in S. 1618 that was just recently passed.

Direct marketing is a growing business. It is $1.2 trillion every year, and creating jobs for over 12 million Americans. It is also growing rapidly internationally. And E-commerce helps that growth. American companies can export products without the need to build any infrastructure in foreign countries. All that is needed is the means to solicit orders—electronic commerce offers that; to

accept orders—electronic commerce offers that; and delivery of the product.

Electronic commerce is really new. And it is not mature yet. And we are going through a great deal of growing pains. And the Government, however good its intentions, should not strangle electronic commerce at its birth. We think that there are many means to combat fraud in existence. And there are in fact bills in Congress which now can provide American consumers with mechanisms to avoid unsolicited E-mail.

The Direct Marketing Association, along with the Interactive Services Association, has come up with some principles for marketing online, which will be included in the record, I ask. But let me tell you about electronic E-mail and the DMA's positions.

First, we think that any marketer should abide by the rules of the forum of the Internet service provider. We understand that unsolicited E-mail increases costs and uses server capacity of Internet service providers. We think that they should establish rules and that marketers should be required to follow them. This is an approach that was included by Senator Torricelli in S. 875.

We think that there should also be an opt out program, and a two-pronged opt out program. The first prong is that the recipient of unsolicited bulk E-mail should be able to request that the marketer not send any more E-mails to that address. This could be done by a reply key. It is the approach taken in S. 771, introduced by Senator Murkowski, and which was merged with S. 1618 and passed by the Senate.

There is a second prong, however. The DMA is actively working on a universal opt out. We are reviewing proposals to create an E-mail preference service, and hope to announce the award of that contract very soon. An E-mail preference service would allow consumers to add their E-mail address online to a list, at no charge. Marketers would then use this list to delete the addresses from their E-mail lists. It is very similar to the mail preference service and telephone preference service of the DMA that have been in existence since 1971 and 1985.

This is an approach that was also included by Senator Torricelli in S. 879. We think with these two prongs, plus a requirement that you honor the rules of the forum, that consumers can limit all E-mail through the EMPS, and company-specific E-mail through the opt out key. We think this approach is far superior to banning the use of E-mail to reach prospective customers.

Electronic commerce, and E-mail in particular, are going to be growing and changing. A ban on the use of commercial E-mail is premature at best, and may be counterproductive by chilling advancement of certain new technologies.

The DMA also believes that the Government should enhance its efforts to combat fraud on the Internet, and specifically in E-mail. And we applaud the efforts of the FTC, postal inspectors, and other law enforcement agencies to step up their anti-fraud campaigns. The DMA will continue its efforts to cooperate with them and their law enforcement efforts.

The DMA has consistently referred any ethics complaints it receives involving fraud or other violations of the law to the FTC, attorneys general, and the postal inspectors.

Fraud should be severely punished, whether it is made on paper, over the airwaves, over phone lines, or on the Net. It is a cancer to all commerce regardless of the medium used, and it should be eradicated. And the DMA wishes to work with you and your subcommittee to work on legislation to try and help solve this problem.

And I thank you for the opportunity, and am willing to answer any questions.

[The prepared statement of Mr. Cerasale follows:]

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

Good morning, Chairman Burns and members of the Subcommittee. It is an honor to be asked to testify today on behalf of the Direct Marketing Association concerning the issue of unsolicited commercial e-mail.

I am Jerry Cerasale, Senior Vice President, Government Affairs for the Direct Marketing Association (The DMA). The DMA represents over 3,600 corporate members who are direct marketers, both domestic and international, and their suppliers and support services.

The DMA is very interested in any regulation of electronic commerce. Over 85% of DMA members are involved in some form of electronic commerce, although we do not know of any members presently using e-mail for marketing to prospective customers, as opposed to reaching current customers. With the rapid changes in communications technology, we believe that no method of communication for commerce should be eliminated.

However, The DMA does agree that many current uses of unsolicited e-mail are not appropriate for legitimate marketing and must be curtailed. We believe that Congress should examine approaches to eliminate inappropriate uses without eliminating the medium of e-mail altogether. We can envision, for example, the use of e-mail to deliver coupons to consumers, a very different and far more positive use of e-mail than the current stream of often fraudulent and x-rated offers.

Marketers have been very creative in providing products that American consumers want through the traditional media of mail, telephone, and direct advertising. The DMA wants to keep the new option of electronic communication open, not eliminate it by government regulation, either domestically and internationally.

We also believe that there are market forces that discourage legitimate companies from engaging in mass unsolicited e-mailing. The direct marketing field is very customer-oriented, and legitimate companies must provide good customer service, not anger their customers.

Direct marketing is a growing business which meets the needs of time-pressed consumers. It is also growing rapidly in the business-to-business market as businesses discover the time-saving convenience of ordering directly. The economic impact of direct marketing in the United States is $1.2 trillion annually, creating over 12 million American jobs.

Direct marketing is also growing rapidly internationally. American companies can export products without the need to build any infrastructure in foreign countries. All that is needed are a means to solicit orders, accept orders, and deliver the product. Electronic commerce is a new medium that offers companies and customers throughout the world the convenience of at-home or at-the-office shopping. Any attempt to regulate electronic commerce must be tempered by consideration for its vast potential for commercial growth, convenience to customers, and new jobs created.

Electronic commerce, of which e-mail is a part, is new. It must be allowed to mature—with all its growing pains. The government, however good its intentions, should not strangle electronic commerce at birth. There are ample means to combat fraud in existence, and there are bills in Congress now which can provide American consumers with the mechanisms to avoid unsolicited e-mail.

The DMA position on unsolicited bulk e-mail is that individuals should be able to opt out from receiving it. The DMA has established principles for marketing online in conjunction with the Interactive Services Association. Those principles are attached to my testimony today. One section of these principles is "Unsolicited Marketing E-Mail". The principles state:

- Solicitations posted to news groups, bulletin boards, and chat rooms must be consistent with the forum's stated policies.
- Online e-mail solicitations should be clearly identified and should furnish a means to opt out.

• Individuals whose e-mail addresses have been collected from online activities should be offered a means to opt out.
• Operators of chat areas, etc., should inform individuals that any information disclosed in the chat area may result in unsolicited messages.

The DMA envisions a two-pronged opt-out program. First, however, any e-mail marketer should abide by the "rules of the forum" unless the marketer has an existing relationship with the addressee. Thus, the rules on e-mail established by Internet service providers, AOL, for example, would apply to all e-mails sent to an AOL address. This approach is contained in S. 875, introduced by Senator Torricelli. We understand that unsolicited e-mail can increase costs and use up server capacity. This approach gives Internet service providers some control over the use of their capacity and costs.

The first prong of any opt-out plan is that the recipient of an unsolicited bulk e-mail should be able to request that the marketer not send any more e-mails to that address. This could be done via the reply key. This is the approach taken in S. 771, introduced by Senator Murkowski, which was merged into S. 1618 and passed by the Senate.

The DMA is actively working on the second prong for opt-out. We are now reviewing proposals to create an "e-mail preference service" (e-MPS) and hope to announce the award of a contract in the near future. An e-MPS would allow consumers to add their e-mail addresses, on line, to a list at no charge; marketers would then use this list to delete the addresses from their e-mail list. This is similar to The DMA's mail and telephone preference services, which have been working in the marketplace for many years (MPS began in 1971 and TPS in 1985). This approach is also in S. 875. In addition, starting in July 1999, DMA members will be required to use e-MPS as well as MPS and TPS as a condition of membership.

With these two prongs, consumers can limit all e-mail through e-MPS or company specific e-mail through the reply key opt-out. Moreover, Internet service providers can create and then market different "rules of the forum" concerning e-mail.

This approach is far superior to banning the use of e-mail to reach prospective customers. E-mail, the Internet, and the World Wide Web are still new means of communications for most Americans. They are also ever-changing technologies. The DMA believes that these new forms of communication should be allowed to grow and mature. Prohibition of e-mail will not allow the growth of the medium. New filtering technologies, more rapid access, and new means of connection to the Internet could alter the use and efficacy of e-mail solicitations. A ban on the use of commercial e-mail is premature at best and may be counterproductive by "chilling" advancement of certain new technologies.

The DMA believes that the government should enhance its efforts to combat fraud on the Internet and, specifically, in e-mail. Fraud should be severely punished whether made on paper, over the air waves, over phone lines, or on the Net. It is a cancer to all commerce regardless of the medium used, and it should be eradicated.

Again, I thank you for the opportunity to be here today, and I am available to answer any questions.

Senator BURNS. Thank you very much. I would call on Dierdre Mulligan, staff counsel for the Center for Democracy and Technology. Thank you for coming this morning, and we look forward to your testimony.

STATEMENT OF DIERDRE MULLIGAN, STAFF COUNSEL, CENTER FOR DEMOCRACY AND TECHNOLOGY

Ms. MULLIGAN. Thank you very much. I want to first take the opportunity to thank the chairman. My organization, as you know, works on first amendment, privacy, and other issues that are critical to the Internet, and we have really appreciated your leadership on issues such as encryption, and also to thank Senators Murkowski and Torricelli for their ongoing effort to look at the use issue in partnership with you and Senator McCain.

I am very pleased to have the opportunity to talk about use today as many of you have commended, the growth of the Internet, and particularly E-mail, is leading to a rapidly evolving, what the Supreme Court recently called worldwide conversation. E-mail par-

ticularly is giving us the opportunity to communicate, share information, and spread ideas in a way that no other medium has ever been able to mirror.

However, the same traits—the low barriers to access, the ability to communicate both one-to-one and one-to-mass that are so powerful for freedom of speech are also very powerful for some of the marketing community and, as the Federal Trade Commission has found out, generally a fairly unscrupulous section of the marketing community to use this medium to send hundreds, thousands, and even millions of messages to consumers which they frequently are not interested in receiving.

Unlike postal mail, as Senator Torricelli pointed out, the cost of E-mail is not borne by the sender, it is borne by the intermediaries, the ISP's, the backbone provider. It is borne by the recipients and, unfortunately for the recipients in rural areas such as Montana and Alaska, those costs, when there are dial-up accounts, when there is storage on local ISP's, can be quite substantial and, at times, I think some of your constituents have found prohibitive.

Both the frustrations of the Internet community and the complexities of addressing the quandary of unsolicited commercial E-mail in a way that meshes with our constitutional protections for speech were aired at the Federal Trade Commission's half-day work shop on use that was held last June.

At its conclusion, and at the request of then-Commissioner Varney, the participants at the workshop agreed to undertake an effort to look at these issues, to look at a broad array of possible solutions. I think too often we tend to seek Government solutions and regulatory solutions and what we have found, and I think particularly what the Communications Decency Act and the Supreme Court decision striking it down have told us is that in this medium those tools may need to be coupled with other tools that are more appropriate to this medium that deal with the decentralized and the global context.

So some of the solutions that we have looked at are not just legislative and regulatory but also include technical approaches, such as the filtering tools that are employed in different E-mail programs, the technical measures such as the companies such as AOL and Compuserve have put in place to deal with protecting their consumers, and many of the self-regulatory efforts that have ranged from opt-in E-mail to global opt-out lists, to free services that offer cleaning of lists so that when marketers want to send messages they ensure that they do not send them to people who have indicated they have no desire to receive them.

For the past year, CDT has coordinated this working group, and it has been a privilege to work with organizations and companies—everyone who is represented at this table this morning has participated, or someone else from their organization, along with many others.

While the report is not yet available, it is our intention and it will be our pleasure to share that report with the committee, and I think that you will find that it both maps out the issues, helps identify both the role that Government can play and also the role that the private sector and that technical tools can play in dealing with this very complex issue.

Finally, I want to come to the recent bill, the amendments to S. 1618 by Senators Torricelli and Murkowski. I believe that S. 1618 is a very important first step in addressing this issue and that if it was enacted, that it would lead to a reduction in unsolicited commercial E-mail, and I will get to why in a second.

However, I think it is unclear whether S. 1618 on its own will be the silver bullet. I think the reason that it will reduce unwanted commercial E-mail on the Net is that if the history of E-mail has told us anything, and the history of the Internet, it is that Internet users are a very vocal bunch, and that when they are able to respond to practices that they do not like, they do so vociferously loudly, and in the case of unsolicited commercial E-mail, with a fairly resounding no, and I think that there is one example I would point you to.

Canter & Siegel are real Internet lore, and they have often been called one of the most hated folks on the Net, and they sent out a massive blast to over 6,000 Use Net news groups, which are groups that are usually very issue-focused for discussions among like-minded individuals, but they put their return address.

Very quickly, their ISP not only crashed once, but crashed 15 times, and Canter & Siegel business people who were trying to operate in this medium found out that they could not get an ISP to carry them. I think the recent incident with Sanford Wallace also tells us that when people are identified as using this medium in a way that the community thinks is inappropriate, that they find the community is not ready to open their door.

That said, I believe that the impact of legislation, whether it is S. 1618, if passed by the House and Senate, or others has to be monitored. Regulating activities on the Internet poses really unique issues. As I said earlier, this is a global decentralized medium. I do not think legislation in this medium will ever provide a full answer and that it is going to need to be coupled with technical tools, with self-regulation, to really create a robust infrastructure to provide individuals with the ability to control the information coming into their homes.

I very much look forward to working with you, and appreciate the opportunity to be here. Thanks for your time.

[The prepared statement of Ms. Mulligan follows:]

PREPARED STATEMENT OF DIERDRE MULLIGAN, STAFF COUNSEL, CENTER FOR DEMOCRACY AND TECHNOLOGY

The Center for Democracy and Technology (CDT) is pleased to have this opportunity to testify on the issue of unsolicited commercial email (UCE).

CDT is a non-profit, public interest organization dedicated to developing and implementing public policies to protect and advance First Amendment freedoms, individual privacy, and democratic values on the Internet. CDT is pleased that the Senate has recognized the important implications for these issues raised by the growth and prevalence of UCE.

Over the past few years, the Internet has rapidly become the cornerstone of an immense, global, multimedia communication network for culture, science and commerce. The Internet has proven wildly beneficial not only in fomenting free speech, but in facilitating the operations of the commercial marketplace as well. The first, most popular, and widely used application on the Internet is electronic mail, or email. Across the globe, email is spanning distances and cultures by easing the exchange of knowledge, information, and resources.

Unfortunately, the very popularity and efficiency of email has created several problems. The one we address today is that of unsolicited commercial email. Because of the effortlessness with which one sender can transmit a message to hun-

dreds, thousands, or even millions of recipients, sending unsolicited commercial inducements to vast email address lists has been an irresistible temptation to some businesses.

Unlike postal mail, which is paid for piece by piece by the sender, the full cost of unsolicited commercial email is not borne by the sender. The current system of allocating the costs of moving information, including email messages, on the Internet allows the costs of sending bulk missives to be shifted from the sender to intermediaries, such as Internet service providers (ISPs), and to the recipients. While each individual email message only requires a minimal amount of Internet resources, when multiplied by the millions, such bulk messages can easily clog data pipelines and force both ISPs and recipients to spend time and resources to deal with what are frequently unwanted messages. Additionally, UCE, which can flood an individual's home or office email accounts, is viewed by many recipients as the computer equivalent of unsolicited telemarketing pitches.

However, responding to the problems caused by UCE is not simple. Not only does this very complicated issue touch upon First Amendment and privacy concerns, it also involves regulating a decentralized and global technical infrastructure. Both the frustrations of the Internet community and the complexities of addressing UCE were aired at the Federal Trade Commission's half-day workshop on UCE held last June. At its conclusion, and at the request of then-Commissioner Varney participants agreed to undertake a collaborative effort to explore possible responses to the growing problems associated with UCE.

For the past year CDT has coordinated a diverse group of organizations and businesses to explore the problems associated with UCE and identify potential solutions. Participants in this effort include representatives from all my fellow panelists organizations this morning—America Online, the Coalition Against Unsolicited Commercial Email, the Direct Marketing Association—and many others. The work of the Ad-hoc Working Group on Unsolicited Commercial Email is detailed in the report to be delivered to the Federal Trade Commission in July.

While the report of the working group is not yet public, I believe that the detailed review of legislative, technical and self-regulatory approaches to this issue and the broad recommendations of the working group will provide a useful roadmap to those seeking solutions to the problems associated with UCE.

Of course, the Senate has already taken some action by passing the amendment targeted at UCE, sponsored by Senators Murkowski and Toricelli, to the Telephone Anti-Slamming Bill, S. 1618. These amendments require creators and senders of UCE to provide accurate contact and routing information as well as permitting recipients to request removal from mailing lists. The bill empowers the Federal Trade Commission, state governments, and ISPs to enforce its provisions.

CDT believes that S. 1618 is a good first step that will reduce the problems caused by UCE. We believe the bill, unlike other approaches, steers clear of many of the thorny First Amendment issues, and does not unduly burdens speakers or ISPs. However, we do believe that the current definition of commercial email is overbroad and may unconstitutionally prohibit anonymous, non-commercial speech—clearly not the intent of its drafters.

CDT believes that S. 1618 would if enacted begin to address the problems of UCE. However, CDT believes that the impact of legislation, particularly in an environment like the Internet, must be monitored. CDT appreciates the Committee's effort to focus on this issue and encourages the Committee and Congress—whether or not S. 1618 becomes law—to monitor this issue. CDT and other members of the Ad-hoc Working Group individually, and perhaps as a group, will also be carefully monitoring the implementation of both state and federal laws. The Working group's report will be available soon. We look forward to working with you and thank you for your effort to address this important issue.

Senator BURNS. Thank you. We appreciate your time and your efforts on this.

Mr. Ray Everett-Church, cofounder, Coalition Against Unsolicited Commercial E-mail.

STATEMENT OF RAY EVERETT-CHURCH, CO-FOUNDER, COALITION AGAINST UNSOLICITED COMMERCIAL E-MAIL

Mr. EVERETT-CHURCH. Thank you, Mr. Chairman, and to the Members of the committee, I appreciate the chance to address you. I hope your staff warned you that by the end of this year you will

be such an expert in technology that your grandchildren will expect you to program the VCR. [Laughter.]

I come here today on behalf of the Coalition Against Unsolicited Commercial E-mail. I have also been authorized to say that my remarks today represent the views of our coalition partners, the Internet Service Providers Consortium and the Forum for Responsible and Ethical E-mail.

The coalition is an all-volunteer ad hoc group of technology professionals, consumer activists, Internet servers, provider owners and operators, and the operators of many Internet-based businesses. In just a year of existence we have become one of the Nation's largest Internet advocacy groups with over 10,000 registered members from nearly every State.

Our coalition was formed for just one purpose, to advocate for a legislative solution to the problem of junk E-mail. We took on this task because as technology experts we found that the technology and self-regulatory solutions have proven to be no solution at all in stopping the damage done by junk E-mail.

As you have heard from many people, and I will not recount all of it, the problem of junk E-mail imposes tremendous cost on many parts of the system, including Internet service providers and users, particularly customers in rural communities, but there is a larger issue at stake.

As a greater and greater percentage of our gross domestic product revolves around the explosion of computer-related and Internet-related commerce, I do not exaggerate when I say that junk E-mail has the potential to harm our economy in ways that terrorists could only dream about.

With alarming frequency, media report system crashes and network outages caused by junk E-mail attacks knock out systems by large providers such as AT&T, Pacific Bell, Netcom, GTE and others. Just to give you an idea of the volumes we are talking about on an individual level, during calendar year 1997, the E-mail account I use for my business received over 6,000 pieces of unsolicited commercial E-mail. That is an average of about 16 messages per day, for a total volume of 41 megabytes.

While the costs of becoming a junk E-mailer are tiny, as you have heard, the cost to those who have to transport, process, store, and retrieve that E-mail are quite tremendous. Particularly for users in rural communities and Internet service providers serving those users, the costs can be extraordinary.

For many of the victims of junk E-mail attacks, these unsolicited commercial messages are like a telemarketer's phone call to their cellular phone. They have paid to receive a message they did not ask for and invariably do not want.

For this reason, many people have called junk E-mail a form of postage-due marketing. I am not so charitable. I quite simply call it theft. It is the stealing of time and resources from others against their will.

Now, you have heard several different legislative approaches discussed today, and what I want to share with the committee is that the coalition feels that any legislation which would legalize the sending of any form of junk E-mail is nothing short of legalizing a type of theft. If this committee gets a chance to review junk

E-mail legislation, I urge you to reject any solution which gives legal sanction to the practice.

Now, outlawing junk E-mail such as Congressman Smith's approach would not make it impossible to advertise on the Internet, not in the least. It will simply require that marketers show some more creativity in convincing consumers to opt in for their messages.

Now, you have already recognized the differences between postal mail and E-mail, and we believe that the postal opt-out approach is a misguided approach for the E-mail venue. We favor an opt-in approach.

Now, legislation mandating opt-in approaches for situations where costs are shifted to the recipients is not unheard of. In fact, the existing statute outlawing junk fax transmissions has been on the books for almost a decade now, more than a decade, and has been extremely successful.

The economics of junk faxes and junk E-mail are quite similar in that they both consume the resources of the recipient at much lower cost to the sender. However, there is an important difference. With junk faxes, it is much more difficult to press one button and send to 10 or 20,000 people very easily without some incremental cost, but in the world of junk E-mail, the 10-millionth E-mail message costs no more than the 11-millionth E-mail message.

Just as we find H.R. 1748 a clear solution we find Senators Murkowski and Torricelli's approach inadequate and, indeed, something of a threat. Although CAUCE certainly endorses the intent behind their approach, we are concerned that their proposal will increase the burden on businesses and consumers by setting a very low threshold for the legitimacy of junk E-mail.

Now, some have questioned the constitutionality of an outright ban on junk E-mail. Let me assure you that there is ample precedent for supporting Congressman Smith's legislation.

In the case of *Rowan* v. *U.S. Post Office,* the Supreme Court held that nothing in the Constitution compels citizens to view unwanted communications and specifically the Court held that "a mailer's right to communicate must stop at the mail box of an unreceptive addressee." To hold any less would be licensing a form of trespass.

Certainly, in the junk E-mail context a Federal district court held, "There is no constitutional requirement that the incremental cost of sending mass quantities of unsolicited advertisements must be borne by the recipients."

In conclusion, Mr. Chairman, like the fax machine before it, electronic mail is a marvelous tool of business and personal communication. It is simple and accessible, but unless Congress acts to stop the growing flood of advertisements, the viability of the media will be severely threatened.

Thank you very much.

[The prepared statement of Mr. Everett-Church follows:]

PREPARED STATEMENT OF RAY EVERETT-CHURCH, CO-FOUNDER, COALITION AGAINST UNSOLICITED COMMERCIAL E-MAIL [1]

Thank you Mr. Chairman and members of the Committee. I am very grateful to have been asked to speak to you today on behalf of the Coalition Against Unsolicited Commercial Email, also known as CAUCE. CAUCE is an all-volunteer, ad hoc group of owners and operators of Internet-based businesses, service providers, technology professionals, and consumer activists. We are now the largest Internet advocacy group in the United States with over 10,000 registered members in nearly every state. Our coalition was formed to advocate for a legislative solution to the problem of "junk email," because it has become clear to us that technical and self-regulatory solutions have proven to be no solution at all.

The Coalition represents a wide range of Internet users and Internet-based businesses. Our Board of Directors includes long-time Internet Users, the owners of two small ISPs, a marketing and public relations professional, a lawyer, a college student, and the author of the best-selling book The Internet for Dummies. What we all have in common is that we make our livings, to some degree or another, from the Internet. We all want the Net to thrive, and we want to do business online. We are willing to pay our own way, but we are not willing to subsidize the advertising of others.

I should note that I have been authorized to say that my remarks today also represent the views of our colleagues at the Forum for Responsible and Ethical Email (FREE). Their founder, Jim Nitchals, passed away quite unexpectedly a little over a week ago. I know Jim was very much looking forward to these hearings and I'm sure watching from above on this important day for the Internet.

UNSOLICITED COMMERCIAL EMAIL THREATENS THE FUTURE OF ONLINE COMMERCE

Let there be no mistake that this is an important day for the Internet; you are taking up an issue of tremendous importance for the future of online commerce. As a greater and greater percentage of our gross domestic product revolves around the explosion of computer-related and Internet-related commerce, I do not exaggerate when I say that junk email has the potential to harm our economy in ways that terrorists could only dream about.

The technology news media reports with alarming frequency system crashes and network outages caused by junk email attacks. Junk email has knocked out systems belonging to major Internet service providers such as AT&T,[2] @Home,[3] Pacific Bell,[4] Netcom,[5] GTE,[6] and literally hundreds of smaller ISPs serving rural communities across the nation. And the volumes of junk email are increasing every day.

If junk email were as innocuous as the mail ads you get through the U.S. Postal Service, we would probably not be discussing this here today. But the fact that your committee is holding these hearings today is testament to the fact that junk email—also called UCE, unsolicited commercial email, and "spam"—is a very different animal with tremendous costs and consequences for the future of the Internet. There are some who would have you believe that junk email is no different from any other type of advertising media, but I urge you not to believe that. There is no other medium quite like junk email in its ability to damage Internet systems and impede legitimate Internet commerce. I know of no more efficient means of consuming the time, money and resources of millions, against their will.

---

[1] This testimony was prepared with the advice and assistance of the CAUCE Board of Directors: Scott Hazen Mueller, Chairman, John Mozena, John Levine, Doug Muth, J.D. Falk, Edward Cherlin, Corey Snow, George Nemeyer, and Ray Everett-Church. Some portions have been excerpted from the testimony of David H. Kramer, Esq., before the Washington State Legislature. Mr. Kramer may be contacted at Wilson Sonsini Goodrich & Rosati, Palo Alto, CA 94304, (650) 493–9300.

[2] "Spam Slows WorldNet Mail"—C\Net News (7/16/97) http://www.news.com/News/Item/0,4,12512,00.html

[3] "Spam Snags @Home Mail System"—C\Net News (2/25/98) http://www.news.com/News/Item/0,4,19487,00.html

[4] "Pacific Bell Suffers Slowdown"—C\Net News (3/13/98) http://www.news.com/News/Item/0,4,20046,00.html; "PacBell Fights Spam Explosion"—ZDNet (3/13/98) http://www.zdnet.com/zdnn/content/zdnn/0313/294405.html

[5] "Spam Clogs Netcom Lines"—C\Net News (4/29/97) http://www.news.com/News/Item/0,4,10204,00.html

[6] "Sprint Down for 5-hour Count"—C\Net News (9/3/96) http://www.news.com/News/Item/0,4,3039,00.html (discussing problems at both Sprint and GTE).

UNSOLICITED COMMERCIAL E-MAIL SHIFTS TREMENDOUS COSTS ONTO RECIPIENTS

Unlike virtually every other communications medium, the majority of email costs are paid by the recipients—not the sender. This is, for better or for worse, the nature of the Internet. It grows out of the cooperative arrangements upon which the Internet was created, where each participant pays for their portion of the infrastructure. This means that once an email is sent, whether it is an advertisement or a letter from a college student to her parents, the costs for relaying, transmitting, receiving, storing, and downloading the message borne by any number of people, except the sender. When you are not paying the freight, as is the case with the sender, it is only natural to be less concerned with the costs involved. And therein lies the problem.

Even if the problem were limited to just one or two messages a day, forcing a recipient to pay for receiving advertising would be unacceptable, but we are not talking about just a few messages. I know this first hand: During calendar year 1997, the email account I use for my business received over six thousand pieces of junk email, weighing in at 41 megabytes of data. That is an average of sixteen (16) pieces of junk email each day. Indeed, the economics of junk email create a strong incentive to send such mail as frequently and as broadly as possible. Given that the cost of sending one hundred messages is the same as one million, a mailer has every incentive to send his message to as many e-mail addresses as possible. With such a miniscule investment, even if only one out of every million recipients buys the mailer's miracle cure or multi-level marketing scheme, not only will he have recovered his tiny investment, he may well have turned a handsome profit.

The problem with junk email stems from the realization by unscrupulous mass marketers that they can force unwanted and unwelcome messages on millions of consumers, with just the touch of a button, at virtually no cost to themselves. For less than a hundred dollars, you can outfit your computer with all the necessary hardware and software to generate a million pieces of junk email each day. You can even buy databases of email addresses on CD–ROM; the going rate right now is under $10.00 per million addresses. Top it off with an unlimited Internet account for $19.95, and a junk emailer is born.

While the costs are small for the junk mailers, the same cannot be said for the people who have to transport, process, store, and retrieve that email. Millions of Internet users, businesses and consumers alike, pay for their access to the Internet in increments of time. Many more, particularly those in rural communities and those who travel extensively, must make toll calls to obtain a connection. For these individuals, each unsolicited commercial message they receive is like a telemarketer's call to their cellular phone—they pay to receive messages they did not ask for and inevitably do not want. Like many millions of people, I pay for my Internet access by the minute. I estimate that the Internet connection time alone for those six thousand unsolicited messages cost me in the hundreds of dollars—and that is before I even begin to calculate the amount of time wasted in sorting through all that junk to find my important email.

It also presents a problem for those who do not immediately review their e-mail. When these individuals do check their electronic mailboxes, they find they must wade through dozens of unsolicited advertising messages in order to find their legitimate email. During that time, their company or service provider has been forced to store that tremendous volume of mail until the user can retrieve it. Just a few days worth of junk email for a service provider the size of America Online would easily fill all the disk storage space of all the computers in all of the offices on Capitol Hill.

Junk email forces Internet users to become a captive audience for whatever advertising message anyone wishes to send them, at any time, any number of times. Yet the hard costs are miniscule when compared to the non-monetary costs of junk email. Unlike direct mail from the post office, junk e-mail arrives throughout the day at home and at work, and there is no effective technical means of blocking it.[7]

[7] Blocking and filtering of junk email has proven extremely ineffective in combating junk email. In order to block or filter email, you must first know where it is coming from. Then once you implement a block for that location, a junk mailer can rapidly change their location. For example, they may send mail via an America Online connection, then once that route is blocked, they will reconnect via CompuServe, then via Netcom, and so on. In Internet parlance, these kinds of mailers are called "whack-a-moles," a reference to the popular carnival arcade game where you strike the mole with a mallet only to have it reappear somewhere else. Junk mailers obtain throw-away Internet accounts for one-time usage, bouncing from one ISP to the next, making up an address and launching their messages. While a receiving site can add that address to its filters, the spammer will seldom use that address again. Senator Murkowski's original bill, S. 771, proposed a mandatory "tag" on commercial email. However, filtering based upon

Junk email in the workplace interrupts employees who must wade through pornographic ads and "get rich quick" schemes to find work-related email. Parents and their children often have no choice but to accept, pay for and dispose of these unwanted and sometimes highly offensive messages. Major junk email campaigns can also knock out Internet systems, resulting in lost data, lost business, and lost productivity.

THE ECONOMICS OF "JUNK EMAIL" ENCOURAGES MASSIVE ABUSE

When turned into an advertising medium, the skewed economics of email turn traditional notions of advertising on their head. In virtually no other advertising medium does the advertiser get to force the recipient to bear more costs than they do. At least with television, print ads in newspapers, or advertisements in the U.S. Mail, the sender incurs significant initial costs and is forced to target their advertising carefully because each additional ad bears in incremental cost. But in the world of junk email marketing, it costs no more to send the first email than it does to send the ten millionth email. Thus, there is every incentive for the marketers to cast their advertisements as widely and indiscriminately as possible.

Not only is there no incentive to carefully target the mailing lists, there isn't even an incentive to reduce duplication. So today many people, myself included, regularly receive multiple copies of the exact same advertisement.[8] And why not? When advertisers pay so little of the costs involved, there is no incentive for them to be careful; indeed, time spent on editing a mailing list is time wasted.

You will undoubtedly hear from representatives of the marketing industry who will say that electronic mail represents a low cost method of marketing which will put mass advertising into the hands of even the smallest businesses. That is certainly true. But what they never acknowledge is that what makes junk email so inexpensive is that every recipient is forced to subsidize that advertising whether they want to or not. I am continually astonished that the marketing industry defends the need for junk emailers to steal money and resources from their would-be customers. No other industry would dream of stealing from potential customers in this fashion, and no other industry would dare come before Congress and ask that their right to steal from the public be protected.

For this reason, many people have called junk email a form of "postage due" marketing. I am not so charitable. Quite simply, I call it theft. It is stealing the time, money, and resources of others against their will. And any legislation that sanctions the sending of unsolicited email, however well-intentioned, does nothing short of legalizing a kind of theft. Therefore I urge the members of this committee to reject any so-called solution which would permit the practice of theft by email to continue.

THE THREAT TO BUSINESSES AND SERVICE PROVIDERS IS ENORMOUS, AND GROWING

I am sure you will hear horror stories from many Internet Service Providers about the volumes of junk email coursing through their systems, but some larger companies have publicly estimated that upwards of 30% of their daily email traffic is junk email. As a former consultant to America Online's email administrators, I can tell you that they have made major investments in equipment and personnel to keep their systems running in the face of the onslaught. Companies like Hotmail, AT&T, Earthlink, UUNet, Netcom, CompuServe, and Erols also invested millions and hired numerous full time administrative staff to do nothing but combat the effects of junk email.

But I am not here today to tell you about the problems of large ISPs—they will tell you that themselves. I am here to tell you that even a fraction of AOL's daily junk email dose is more than enough to put small businesses and small Internet Service Providers out of business. With more and more companies conducting their critical business over the Internet, junk email is costing those businesses millions. Moreover, junk email threatens to put hundreds of small ISPs out of business, particularly the kinds of small, local service providers who provide the only cost-effective Internet access to thousands of consumers, businesses, and schools in rural areas all across the United States. Even as I speak, this committee and others in Congress are debating whether FCC-imposed fees should subsidize Internet access for schools and libraries. As you wrangle over that issue, let me remind you of this fact: junk emailers peddling porn sites and miracle potions are already subsidizing

---

advertising tags would not relieve the burden on Internet services providers or businesses whose facilities are already overwhelmed with massive quantities of junk email.

[8] One particular junk mailer has permutations of my email address on his list no less than five times. Whenever they take on a new client, I always get five copies of each and every ad. From the complaints received from CAUCE members, such situations are not at all uncommon.

themselves on the backs of schools, libraries, businesses and consumers all across this nation.

CAUCE has heard from many dozens of small- and mid-sized ISP all across this country, all of whom are crying out for relief from the damaging and costly practices of unscrupulous advertisers. Technology shows little promise of solving the problem, and hauling junk mailers into court on cutting-edge theories in cyberspace law is just not a reasonable or affordable answer. Small ISPs exist on notoriously tiny profit margins. Seemingly little things, such as the number of milliseconds it takes for a computer to process a piece of email, become looming problems when you are facing the demands of Internet services. For an Internet Service Provider, the processing capacity of their mail servers is a precious commodity and when their systems are tied up processing junk email, it creates a drag on all of the services they provide to their customers.[9]

The problem is also compounded by the fact that ISPs purchase bandwidth—their connection to the rest of the Internet—based on projected usage by their prospective user base. For most small- and mid-sized ISPs, bandwidth costs are among one of the greatest portions of their budget and contributes to the reason why many ISPs have a tiny profit margin. Without junk email, greater consumption of bandwidth would normally track with increased numbers of customers. However, when an outside entity (e.g., the junk emailer) begins to consume an ISP's bandwidth, the ISP has few choices: One, let the paying customers cope with slower Internet access, occasional crashes, and degraded services; two, eat the costs of increasing capacity; or three, raise rates. No matter the choice, the recipients are still forced to bear costs that the advertiser has avoided.

The Nobel Prize-winning economist Ronald Coase has written eloquently about the damage done to the economy when these kinds of costs are chronically externalized onto an ever-widening base. In his writings, Coase has discussed the dangers to the free market when an inefficient business—one that cannot bear the costs of its own activities—distributes its costs across a greater and greater population of victims. What makes this situation so dangerous is that when millions of people only suffer a small amount of damage, it becomes too costly for the victims to recover their tiny share of the overall damages. Such a population will continue to bear those unnecessary and detrimental costs unless and until their individual damage becomes so great that those costs outweigh the transaction costs of fighting back.

The classic example is pollution: It is much cheaper, in raw terms, for a chemical manufacturer to dump its waste into the local river. Such externalities allow one person to profit at another's—or everyone's—expense. Certainly those who are harmed might have a cause of action under civil law to recover their actual damages. But for the vast majority of victims, there are significant transaction costs involved in bring individual lawsuits. For most, those costs will prohibit them from ever seeking redress. As a result, the skewed economics of pollution will give incentive to the polluters while making it prohibitive for victims to seek a remedy. Much is the same when it comes to junk email. While some companies have successfully sued junk emailers for the damage they have caused, very few ISPs can afford to fight these kinds of cutting edge cyberlaw battles.[10] As a result, the economics favor

---

[9] Small ISPs are often unable to afford the massive redundant systems that larger companies can afford. Thus, processing junk email can slow down all of the functions on servers that might be filling multiple critical functions such as a mail server, a web server, and a domain name server. Constraints on server capacity are also one of the reasons "filtering" schemes are not viable solutions for many ISPs; filtering email consumes vast amounts of processing capacity and is the primary reason most ISPs cannot implement it as even a partial strategy for eliminating junk email.

[10] In fact, in nearly every lawsuit on junk email-related issues, the actions of junk emailers have been found unlawful in one form or another. See, e.g., *Cyber Promotions, Inc.* v. *America Online,* Inc., C.A. No. 96–2486, 1996 WL 565818 (E.D. Pa. Sept. 5, 1996) (temporary restraining order), rev'd (3d Cir. Sept. 20, 1996), partial summary judgment granted, 948 F. Supp. 436 (E.D. Pa. Nov. 4, 1996) (on First Amendment issues), reconsideration denied, 948 F. Supp. 436, 447 (Dec. 20, 1996), temporary restraining order denied, 948 F. Supp. 456 (E.D. Pa. Nov. 26, 1996) (on antitrust claim), settlement entered (E.D. Pa. Feb. 4, 1997); *America Online, Inc.* v. *Over the Air Equipment, Inc.* (E.D. Va. complaint filed Oct. 2, 1997), preliminary injunction entered (Oct. 31, 1997), settlement order entered (Dec. 18, 1997); *Bigfoot Partners, L.P.* v. *Cyber Promotions, Inc.* (S.D.N.Y. complaint filed Oct. 6, 1997); In re Canter, No. 95–831-O-H (Tenn. Bd. Prof. Resp. Feb. 25, 1997), disbarment order entered (Tenn. June 5, 1997); *CompuServe Inc.* v. *Cyber Promotions, Inc.,* No. C2–96–1070 (S.D. Ohio Oct. 24, 1996) (temporary restraining order), preliminary injunction entered, 962 F. Supp. 1015 (S.D. Ohio Feb. 3, 1997), final consent order filed (E.D. Pa. May 9, 1997); *Concentric Network Corp.* v. *Wallace,* No. C-96 20829-RMW (EAI) (N.D. Cal. complaint filed Oct. 2, 1996), stipulated judgment entered (Nov. 5, 1996); *Earthlink Network Inc.* v. *Cyber Promotions, Inc.,* No. BC 167502 (Cal. Super. Ct. L.A. County May 7,

the abusers and disfavor those victimized. Indeed the mailers are counting on the fact that their incremental theft will not be noticed or that people will just hit the "delete" key and move on. They hope that if they steal only a tiny bit from millions of people, very few will bother to fight back.

As Coase pointed out, this is a prescription for disaster. When inefficiencies are allowed to continue, the free market no longer functions properly. As we all remember from our college Microeconomics classes, the "invisible hands" that would normally balance the market and keep it efficient cannot function effectively when the market is carrying dead weight and perpetuating chronic inefficiencies. Unchecked, businesses that are otherwise unprofitable will indefinitely leech off the indirect subsidies they extract from the public at large.

In the context of the Internet, the costs of these externalities can be seen every time you have trouble accessing a web site, whenever your email takes 3 hours to travel from AOL to Prodigy, or when all your email is lost in an ISP server crash. But the costs do not stop there. With junk email already the number one complaint of most Internet users, consumers have deserted many public discussion forums for fear that their email addresses will be "harvested" and added to junk mail lists. Customers are afraid to give their addresses out in legitimate commerce for fear of being added to and traded among thousands of mailing lists. Legitimate businesses are afraid to use email to communicate with their existing customers for fear of being branded "net abusers."

CONGRESS HAS ACTED TO STOP COST SHIFTING BEFORE

In the pollution context and in many other situations where the marketplace has failed to maintain its own natural equilibrium, governments have appropriately stepped in to alter the skewed economic balance. By enacting substantial fines and penalties as a matter of public policy, governments have remedied the marketplace failure and made responsible behavior more cost effective. A perfect case in point is the federal statute that outlawed the sending of unsolicited advertisements via fax machine.

Email is increasingly becoming a critical business tool in much the same way as the fax machine became an indispensable took during the late 1980s. As more and more businesses began to use fax machines, marketers decided that they could fax you their advertisements. For anyone in a busy office in the late 1980s, you will undoubtedly remember the piles of office supply catalogs and business printing ads that came pouring out of your fax machine. On far too many occasions, you had to shut off the fax machine in mid-advertisement so your business colleagues could try and send their fax before the advertiser could redial.

The similarities between junk faxes and junk email are many: both forms of advertising shift the costs onto recipients, both of them tie up expensive resources without compensation to the victims, and both require federal legislation to cure. There are also some compelling differences that make email more pernicious than faxing. Certainly the average email costs a recipient less than a fax, however you cannot easily send ten million faxes at the touch of a button the way you can with email. In addition, the fax advertiser must bear some marginal cost for each fax sent, particularly if a long-distance call is involved. But with junk email, recipients and ISPs bear most of the cost while the advertiser bears little—and with a few keystrokes, you can quadruple the amount of damage done. With greater and greater abuse not merely a possibility, but an everyday reality, a legislative solution as strong as the junk fax prohibition becomes a necessity.

When looking for a legislative solution to the problem of junk email, we found that the fax statute, 47 USC 227, has been tremendously successful at virtually eliminating the problem of junk faxes and points the way to a real and meaningful solution to the problem of junk email. Therefore we strongly urge the passage of Representative Smith's bill, H.R. 1748. The bill is a model of logic and simplicity. It assures that those who wish to receive such mass mailings can continue to do

---

1997) (preliminary injunction), consent judgment entered (Mar. 30, 1998); *Expert Pages* v. *Universal Networks, Inc.*, No. 97–1542 SI ENE (N.D. Cal. May 2, 1997) (temporary restraining order); *Parker* v. *C.N. Enterprises*, No. 97–06273 (Tex. Travis County Dist. Ct. complaint filed May 26, 1997), temporary injunction entered (Sept. 17, 1997), permanent injunction entered and damages awarded (Nov. 10, 1997); *People* v. *Lipsitz*, 663 N.Y.S.2d 468 (N.Y. Sup. Ct. 1997); *Prodigy Services Corp.* v. *Cyber Promotions, Inc.* (S.D.N.Y. filed Oct. 18, 1996), settlement entered (Dec. 13, 1996); *SimpleNet* v. *VNZ Information & Entertainment Services* (S.D. Cal. complaint filed Nov. 13, 1997), default judgment entered (Apr. 15, 1998); *Web Systems Corp.* v. *Cyber Promotions, Inc.*, No. 97–30156 (Tex. Harris County Dist. Ct. complaint filed June 1997), temporary restraining order entered (June 6, 1997).

so by simply asking, while those who do not want them, will not get them, or will have a legal remedy if they do.

S. 1618 AND H.R. 3888 PORTEND DISASTER FOR THE INTERNET

Just as we find H.R. 1748 a clear solution, we find S. 1618 and its House counterpart H.R. 3888 to be a tremendous threat. Although CAUCE endorses the intent behind Senator Murkowski's and Senator Torricelli's amendment to the anti-slamming bill, we are deeply concerned that this proposed law will, if anything, make the burden on businesses and consumers even greater.[11]

As written, the bill sets basic standards of legality that are easily met, even by today's current crop of disreputable scammers and brazen porno spammers. The legislation would allow marketers to indiscriminately send massive volumes of email with no recourse for the victim other than begging to be taken off the list. Furthermore, by placing enforcement solely in the hands of government bureaucracies, we believe it is unreasonable to expect that the Federal Trade Commission will ever be able to ferret out thousands of violators operating out of their basements. Finally, the legislation could be seen to preempt state laws on junk email.[12]

By setting such a low threshold for legitimacy, we fear it would allow for increasing volumes of junk email. In fact, CAUCE has already received numerous reports of junk emailers making slight modifications to their tactics and proclaiming that their mail is protected by the Murkowski-Torricelli amendment. It is a very bad sign when the "remedy" for a problem gives cover to the most egregious abusers.

We should not presume, as S. 1618 and H.R. 3888 appear to do, that people are willing to incur both direct and indirect costs for advertisements that they did not ask for and invariably do not want. These bills would force people to continuously incur out-of-pocket monetary costs, unless and until they spend more time and money getting themselves removed from thousands of mailing lists they did not ask to be on in the first place. Because of the almost limitless potential for continued abuse under S. 1618 and H.R. 3888, CAUCE believes that this legislation has the consequence of legitimizing massive abuse, making things worse than the status quo, thereby contributing to the demise of email.

H.R. 1748 IS AN EFFECTIVE, NARROWLY TAILORED, AND CONSTITUTIONAL APPROACH

Legislation is desperately needed, as it was in the case of junk faxes, to stop the cost-shifting problem inherent in junk email. Because the cost shifting nature of junk email is so similar to junk faxes, CAUCE believes that amending 47 USC 227 is a well-tailored solution to the problem. H.R. 1748 amends the anti-junk fax statute to prohibit the sending of unsolicited commercial advertisements by email. Like the fax law, it defines a deceptive and unfair business practice that is damaging and costly to consumers and sets statutory damages. In doing so, it counterbalances the economics of junk email and places enforcement in the hands of the consumer, not in the hands of any government agency.

Although some have questioned the constitutionality of H.R. 1748's approach, let me assure you that there is ample precedent for supporting Representative Smith's legislation. When addressing a similar issue of unsolicited advertisements, the Supreme Court said it best in the case of *Rowan* v. *U.S. Post Office:*[13]

Nothing in the Constitution compels us to listen to or to view any unwanted communication. . . . We categorically reject the notion that a vendor has a right under the Constitution or otherwise to send any unwanted communication into the home of another. . . . We repeat, the asserted right of a mailer stops at the outer boundary of every person's domain.

In another Supreme Court case, *Breard* v. *Alexandria,*[14] the Court upheld the constitutionality of a local ordinance prohibiting door-to-door solicitation, stating that it is a misuse of the guarantees of free speech to force anyone to admit solicitors against their will. In *Bland* v. *Fessler,*[15] the Ninth Circuit upheld California's ban

[11] CAUCE expressed our concerns with that language directly to Senator Murkowski prior to the amendment's introduction. A copy of our letter to Senator Murkowski is attached and I wish to incorporate that letter into my testimony by this reference.

[12] Washington and Nevada already have measures on the books dealing with problems created by junk email. And numerous other states are considering legislation to address the harm done to businesses. Bills are pending in California, Colorado, Connecticut, Kentucky, Maryland, Massachusetts, New Hampshire, New Jersey, New York, Rhode Island, Virginia, and Wisconsin. Professor David Sorkin from the John Marshall Law School in Chicago maintains a web site tracking current legislation at: http://www.jmls.edu/cyber/statutes/email/.

[13] 397 U.S. 728 (1970)

[14] 341 U.S. 622 (1950)

[15] 88 F.3d 729 (9th Cir. 1996)

on the use of automated dial and delivery devices, ruling that advertisers had no right to turn consumers into a captive audience, forcing them to receive any message the advertiser wished to send. The Ninth Circuit concluded such a prohibition was a reasonable time, place and manner restriction and was reasonably tailored to serve the state's substantial interest in protecting peoples' right to be left alone.

In addition to these fundamental precepts, every court to look at the constitutionality of the junk fax law, upon which H.R. 1748 is based, has upheld its constitutionality. In *Destination Ventures* v. *FCC,*[16] the Ninth Circuit, after noting that commercial speech receives less protection than political or religious speech, concluded that the statute served a substantial government interest in preventing recipients from having to bear the cost of third party advertising. It found that the prohibition on junk faxes directly advanced that interest. That is the very same interest served by H.R. 1748.

In this and other regards, H.R. 1748 is the antithesis of the Communications Decency Act. The approach in H.R. 1748 comes from the Internet community, by their request, rather than being enacted over the objections of an unwilling Internet community. As was argued in the CDA challenge, the government should not be in the position preventing people from viewing material that they want to see. Representative Smith's bill would do just the opposite: It protects people from being forced to view material that they don't want to view while preserving their right to see it upon request.[17] Finally, any remaining questions about free speech issues can be assuaged by the fact that H.R. 1748 has received wide-spread praise from staunch supporters of free speech and has been endorsed in editorials by USA Today, The Seattle Times, The Philadelphia Enquirer, and The Sacramento Bee, among others.

CONGRESS IS JUSTIFIED IN ACTING TO PROTECT THE EMAIL INFRASTRUCTURE

Like the fax machine before it, electronic mail is a marvelous tool of business and personal communication. It is simple, it is accessible, and it is becoming more and more an indispensable part of our professional lives. But there are even more far-reaching potentials of email that may be lost if its functionality and utility are destroyed by the proliferation of junk email.

The Internet is an incredible tool for spreading information critical to the development of freedom and democracy around the world. Indeed, email is often cited as a critical tool for communicating with and between Chinese democracy activists. Recent media stories have also credited email as a critical tool in the overthrow of the Suharto regime in Indonesia.[18] If Congress does not take immediate steps to rescue email from the grips of snake-oil salesmen, there are real implications for the growth of free speech and democracy both at home and abroad.

Electronic mail is a marvel of accessibilty and ease of use for tens of millions of Americans, and is a critical growth component of America's young Internet economy. Yet in just a few short years, unsolicited advertisements by email have already begun to strangle Internet commerce in its crib. Unless Congress acts to preserve the viability of the medium, today's crop of scammers and thieves will soon give way to more legitimate marketers who will replace the flood of offensive and fraudulent messages with even greater quantities of ads for snack chips and laundry powder. When that terrible day comes, our electronic mailboxes will cease to be a useful tool for business and personal communications and we will have squandered one of the most powerful tools of communication this planet has ever known. On behalf of the Coalition Against Unsolicited Commercial Email, I urges you to protect Internet commerce against the damaging and costly effects of junk email. No less that the future of electronic commerce and our information economy may be at stake.

Thank you, Mr. Chairman. I would be happy to answer any questions the committee might have.

---

[16] 46 F.3d 54 (9th Cir. 1995)

[17] The bill also allows for businesses any number of ways to utilize the Internet to reach a prospective customer. For example, businesses can utilize banner advertising on popular web sites, create their own web site and register them with search engines, provide mechanisms for opting-in to email mailing lists, enter into linking arrangements with companies sharing common markets, and make targeted and topical postings to appropriate Internet bulletin boards.

[18] "Indonesia Revolt was Net Driven"—Boston Globe (5/23/97) http://www.boston.com/dailyglobe/globehtml/143/Indonesia—revolt—was—Net—driven.htm

COALITION AGAINST UNSOLICITED COMMERCIAL EMAIL,
May 12, 1998.

JOE KEELEY,
Office of Senator Murkowski,
Washington, DC.

DEAR JOE: First, I want to thank you for the chance to comment on your proposal. We continue to be impressed with and grateful for your commitment to seeking diverse opinions on this contentious topic. Now that I have had a chance to review the new amendment, I wanted to give you the following feedback on behalf of the members of CAUCE's board.

Although CAUCE warmly endorses the bill's intended goal of removing the cost and time burden that UCE places on Internet users in Alaska and elsewhere in the country, we believe that this proposed law will, if anything, make that burden greater.

Specifically, we have the following issues of concern:

- The bill legitimizes UCE, making it possible to legally deliver vast quantities of UCE to Alaska citizens and all Internet users.
- The bill's valid header/address requirements pose little obstacle to delivering larger and ever-increasing quantities of UCE.
- The bill's removal requirements are little deterrent to millions of home-based, do-it-yourself junk emailers, and with government agencies as the sole enforcement body, the likelihood of meaningful enforcement is minimal.
- Even if all legal requirements are met, the bill will allow each of thousands of marketing organizations "one free bite" at every email recipient, allowing citizens to legally be inundated with increasing volumes of UCE.
- The bill could be seen to preempt private rights of action based on state laws.

First, we are extremely concerned that this amendment goes farther than any existing proposal in establishing UCE as a legitimate method of marketing. This amendment legalizes any UCE that meets minimal standards for truthfulness in delivery, making this bill worse than staying with the status quo. This bill would legitimize an utterly unconscionable practice. It would create a legal framework in which it would be perfectly permissible to harass millions of people on a daily basis with uninvited and unwelcome solicitations; uninvited and unwelcome solicitations that interrupt workers productivity and invade the home at all hours of the day; uninvited and unwelcome messages that advertise explicit pornography, and all varieties of illegitimate business practices; uninvited and unwelcome solicitations that recipients have no choice but to receive, process, and pay for.

No legitimate form of advertising forces the recipient to pay an out of pocket charge to receive advertising messages they did not ask for and invariably do not want. No legitimate form of advertising forces the deliverer to bear enormous out of pocket costs for processing, storing and delivering unsolicited advertising messages. Junk email does both. By contrast, every form of legitimate advertising imposes some marginal cost per message on the advertiser, creating a natural cap on the number and frequency of messages. Every form of advertising supports the media in which it is transmitted, thereby rendering the medium cheaper for all to use. Junk email imposes no marginal cost per message, creating perverse incentives for advertisers to flood the medium with mass solicitations. Further, rather than supporting the Internet infrastructure, junk email burdens it to an incredible degree, forcing ISPs to spend millions of dollars a year, to process unwanted junk email, and forcing increased expenses on end users—particularly those whose Internet access is already costly and tenuous. The only way to reduce the cost to end users in Alaska and elsewhere is to create a disincentive to send large quantities of UCE; any legislation that legitimizes the twisted economics of UCE does a disservice to the citizens you would seek to protect.

Second, we appreciate your efforts to address the issue of fraudulent headers and fraudulent or nonexistent contact information. However, while large quantities of UCE today are delivered using fake header information and invalid return addresses, the requirement of a valid return address and valid headers doesn't provide a tremendous obstacle to most junk emailers. For example, I could open an account with a local ISP and send a million messages out, in violation of their policies. The mail would have valid routing and would have a valid return address—valid, that is, until the ISP terminates the account and renders the address invalid. But that invalidity would be beyond the control of the perpetrator and could provide a defense to charges under that provision of the law. (The question of whether the junk mailer defrauded the ISP is, of course, beyond the scope of your proposed law. That issue is, however, addressed by the California bill I mentioned in our phone con-

versation—a bill that we have endorsed and which been gaining support from large ISPs, including companies like AOL.)

Third, the bill would impose removal requirements on established junk email companies who maintain large lists, but would not realistically affect the large numbers of do-it-yourself junk emailers who harvest addresses on their own and may only send UCE a handful of times. Most of the UCE sent at present comes from these small-time, mercurial operators, not from established bulk email companies. These people operate with a large degree of anonymity, using specially designed "spamware" to facilitate defrauding ISPs, hijacking mail servers, harvesting addresses, etc. Tracking these perpetrators requires significant investigation and protracted legal action to determine their identities—and they know this. These people will not be deterred by the fear that the FTC would devote extensive enforcement resources to launch an action based on a dozen rounds of UCE sent from their basement workstation. And there is little incentive for the FTC to pursue them at any length since most of these people stop sending UCE of their own accord after having all of their Internet accounts terminated. But for each junk emailer who retires, there are constant replacements entering the UCE market everyday. With dozens—possibly even hundreds—of home-based junk emailers entering the market every day, the FTC would require funding to rival a branch of the military if there was to be any hope of pursuing the small-time, do-it-yourself junk emailers in a timely or effective manner. As you well know, any law that requires centralized enforcement decreases the likelihood of effective enforcement, thus we encourage private rights of action in all UCE-related legislation, encouraging citizens and ISPs to take on the burden of enforcement. A few hundred million users will be a more effective police force than a handful of government prosecutors.

Fourth, even with effective enforcement of removal restrictions, this would still permit every junk emailer "one free bite" at every recipient. A hundred pieces of UCE from each of 10 junk emailers imposes no less cost on Alaska's email users than one piece of UCE from a thousand individual companies. Moreover, with such a low threshold for making UCE legitimate, more companies will be tempted to try bulk email. Indeed, more legitimate businesses are already entering the bulk email market everyday: In recent weeks I have seen reports of bulk email campaigns from an ISP in New Jersey, several Web Site Hosting firms, a car dealership near Seattle, an online auction house, a major U.S. automobile manufacturer, a North Carolina supreme court candidate, a political consulting firm in California, and a mid-sized multimedia software company. If it is your intention to reduce the costs of Internet service for Alaskans, this bill will not do that—indeed, it would likely do exactly the opposite.

Finally, while this bill clearly gives the FTC jurisdiction over some types of offenses relating to UCE and permits state officials to proceed with their own prosecutions, we are somewhat concerned that, as written, the bill could be construed as preempting individual rights of action either under common law or under state statutes relating to UCE. Unless it is your intention to occupy the regulatory field on the issue of UCE (something CAUCE would vigorously oppose), it should be made clear that any other state action or individual action under common law or state statute would be unaffected.

In summary, CAUCE is deeply concerned that this bill would do little to stem the rising flood of unsolicited commercial email, and by setting such a low threshold for legitimacy, would allow for increasing volumes of junk email for Alaska residents and others. As written, the bill sets standards which are easily met—even by today's crop of disreputable and brazen junk emailers—and would allow them to continue after only a moment's hesitation. By placing enforcement solely in the hands of government bureaucracies, there is a minimal likelihood of actual enforcement against the most virulent and prolific kinds of fly-by-night, do-it-yourself junk emailers. Finally, it should be made clear that state statutes and other remedies under law (particularly individual causes of action) would be unaffected by this legislation.

Please let me know if we can provide any further information.

Sincerely,

RAY EVERETT-CHURCH,
Counsel.

Senator BURNS. Thank you. Thank you, Mr. Church.

I want to direct a question, and we are supposed to open up here in a little bit with a conference, but Mr. Boe, is there a way that a member of AOL, is there a way technically that you can block for that member what he or she receives?

Mr. BOE. We have tools that allow members, if I understand your question correctly, that allow members to decide what they will or will not receive, so I can establish a list, for example, of the E-mail, known E-mail addresses—her grandparents—and she will receive E-mail only from those people and all other mail will be blocked, and we allow the members to do that themselves.

Senator BURNS. And that is done on the computer of the member himself?

Mr. BOE. Correct, and we believe that allows the members to choose what mail they will receive.

Senator BURNS. Can you do that for the customer at a cost?

Mr. BOE. Well, we do have technical solutions that are designed to try and identify junk E-mail and block it from ever entering the AOL network, and we do that, and there is a substantial cost associated with that.

Senator BURNS. How do you do that?

Mr. BOE. It gets very complicated.

Senator BURNS. I know, but just give me the outer shell.

Mr. BOE. Well, we do a couple of things. We identify domains—we call them spam havens, domains from where spam originates. We also look at the characteristics of the transmission. So, for example, if we see a batch of a million E-mails all coming at the same moment from the same place, we are likely to identify that as junk E-mail and take efforts to block part of it. That is a thumbnail sketch of how that works.

Senator BURNS. OK.

Mr. BOE. But I should add, it is very difficult to do that, and the spammers are very adept at defeating the countermeasures, disguising the source of their transmissions, falsifying the transmission data to prevent us from doing that effectively.

Senator BURNS. Ms. Mulligan, you mentioned encryption, and I have often said—and correct me if I am wrong—robust encryption is one of the keys that the individual American is going to have to understand and use in order to prevent some of this. Is that a correct assumption, and it also goes a long way in protecting the integrity of the service that Mr. Boe offers.

Ms. MULLIGAN. There are a number of folks that are experimenting with the role cryptography may play in addressing E-mail issues. There is some work going on in a number of very important technical labs looking at, for example, a way in which—it is not quite a costing of E-mail, but it would allow me to indicate that I want to communicate with a specific person. You can certainly use public key cryptography to selectively identify people with whom you want to communicate and those with whom you do not.

However, whether or not cryptography will be a central tool in addressing, on the technical side, unsolicited E-mail, I am not so sure.

I think that some of the filtering tools that have been discussed such as the ones my colleague here was talking about are probably more likely to be effective, and one of the important things that he pointed out was what makes filtering difficult today is the falsification of information, the fact that people are falsifying domain names so that when AOL blocks a spam haven the spam haven will then try to disguise itself as somewhere else, and so some of the

accuracy requirements we think would go a long way to help with that specific kind of filtering.

Senator BURNS. Jerry, tell me about your organization. Has your organization developed a code of ethics and guidelines for direct marketing, and if there are violators, do they lose their membership, or how do you police that if you have set up an ethical means of doing business?

Mr. CERASALE. Yes. Yes, we have. We have set up—we have an ethical—an ethics program with ethics committees that have the authority to try and correct a problem that comes up and also the authority to bring to the board to throw someone out.

We have started a new program that there are certain requirements that will be mandatory that people, members participate in to remain members. That will begin in July 1999. They have to give the ability to opt out, the notice and ability to opt out, and honor that opt out. They must use our mail preference service, our telephone preference service, and when we get it up, our E-mail preference service. That would be for all members.

And also our guidelines, our principles for electronic E-mail would be that they have to follow the rules of the forum, and so in essence trying to send unsolicited E-mail, a big batch to AOL, and AOL says they do not accept it, that is the rule of the forum of AOL. Our guidelines would say that you cannot send that batch to AOL, and we have a committee that works and looks at that.

The committee also, when it finds fraud, we immediately send that information to either the FTC, the State Attorneys General, or the Postal Inspection Service, or to all three if it is appropriate, and so we work in that way. That is our ethics program.

Senator BURNS. Tell me about, do your members use the tool of unsolicited E-mail?

Mr. CERASALE. We do not think so. There maybe one—we believe there is one. There is one member who uses unsolicited E-mail and offers an opt-out. As I said in my testimony, this is a new medium, and our marketers have not found it to be useful at the moment. They are looking at it. We do not want it closed up, but they are not using unsolicited E-mail, basically.

This is a very customer-oriented business, and if your customers are angry about it you do not want to use that, so we are looking at new ways—as technology and creativity continues, there may be ways to use unsolicited E-mail, but right at the moment I would have to say basically the Direct Marketing Association members do not use it.

Senator BURNS. Mr. Church, we are going to have to draw this down, but there will be questions from other members on this committee, because we are in this sort of a compact situation here today about moving some information of our own.

In your testimony—and I have not read your testimony, I am sorry—did you specifically lay out some of the concerns that you have with the pending legislation?

Mr. EVERETT-CHURCH. Yes, we did. In fact, we attached a copy of the letter that we sent along to Senator Murkowski's office prior to the introduction of that legislation outlining the major concerns that we had with that bill.

Senator BURNS. Oh, I am sure you will be hearing, all four of you be hearing from us on the committee as that legislation moves and takes its shape.

I am just sorry we have to cut everything—I thought we did pretty well, getting everything into an hour, and your recommendations, and we will certainly recommend to other members if they want to visit with you, I would certainly recommend that they do so on a personal basis. Any questions that you might return to individual Senators I wish you would also copy to the committee.

We appreciate that, and your coming down here this morning. Thank you.

[Whereupon, at 10:35 a.m., the subcommittee adjourned.]

○

DOCUMENT NO. 57