SPAMMING: THE E-MAIL YOU WANT TO CAN

HEARING

BEFORE THE

SUBCOMMITTEE ON TELECOMMUNICATIONS, TRADE, AND CONSUMER PROTECTION

OF THE

COMMITTEE ON COMMERCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTH CONGRESS

FIRST SESSION

NOVEMBER 3, 1999

Serial No. 106–84

Printed for the use of the Committee on Commerce

U.S. GOVERNMENT PRINTING OFFICE
61–040CC WASHINGTON : 1999

COMMITTEE ON COMMERCE

TOM BLILEY, Virginia, *Chairman*

W.J. "BILLY" TAUZIN, Louisiana
MICHAEL G. OXLEY, Ohio
MICHAEL BILIRAKIS, Florida
JOE BARTON, Texas
FRED UPTON, Michigan
CLIFF STEARNS, Florida
PAUL E. GILLMOR, Ohio
Vice Chairman
JAMES C. GREENWOOD, Pennsylvania
CHRISTOPHER COX, California
NATHAN DEAL, Georgia
STEVE LARGENT, Oklahoma
RICHARD BURR, North Carolina
BRIAN P. BILBRAY, California
ED WHITFIELD, Kentucky
GREG GANSKE, Iowa
CHARLIE NORWOOD, Georgia
TOM A. COBURN, Oklahoma
RICK LAZIO, New York
BARBARA CUBIN, Wyoming
JAMES E. ROGAN, California
JOHN SHIMKUS, Illinois
HEATHER WILSON, New Mexico
JOHN B. SHADEGG, Arizona
CHARLES W. "CHIP" PICKERING,
Mississippi
VITO FOSSELLA, New York
ROY BLUNT, Missouri
ED BRYANT, Tennessee
ROBERT L. EHRLICH, Jr., Maryland

JOHN D. DINGELL, Michigan
HENRY A. WAXMAN, California
EDWARD J. MARKEY, Massachusetts
RALPH M. HALL, Texas
RICK BOUCHER, Virginia
EDOLPHUS TOWNS, New York
FRANK PALLONE, Jr., New Jersey
SHERROD BROWN, Ohio
BART GORDON, Tennessee
PETER DEUTSCH, Florida
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
RON KLINK, Pennsylvania
BART STUPAK, Michigan
ELIOT L. ENGEL, New York
THOMAS C. SAWYER, Ohio
ALBERT R. WYNN, Maryland
GENE GREEN, Texas
KAREN MCCARTHY, Missouri
TED STRICKLAND, Ohio
DIANA DEGETTE, Colorado
THOMAS M. BARRETT, Wisconsin
BILL LUTHER, Minnesota
LOIS CAPPS, California

JAMES E. DERDERIAN, *Chief of Staff*
JAMES D. BARNETTE, *General Counsel*
REID P.F. STUNTZ, *Minority Staff Director and Chief Counsel*

SUBCOMMITTEE ON TELECOMMUNICATIONS, TRADE, AND CONSUMER PROTECTION

W.J. "BILLY" TAUZIN, Louisiana, *Chairman*

MICHAEL G. OXLEY, Ohio,
Vice Chairman
CLIFF STEARNS, Florida
PAUL E. GILLMOR, Ohio
CHRISTOPHER COX, California
NATHAN DEAL, Georgia
STEVE LARGENT, Oklahoma
BARBARA CUBIN, Wyoming
JAMES E. ROGAN, California
JOHN SHIMKUS, Illinois
HEATHER WILSON, New Mexico
CHARLES W. "CHIP" PICKERING,
Mississippi
VITO FOSSELLA, New York
ROY BLUNT, Missouri
ROBERT L. EHRLICH, Jr., Maryland
TOM BLILEY, Virginia,
(Ex Officio)

EDWARD J. MARKEY, Massachusetts
RICK BOUCHER, Virginia
BART GORDON, Tennessee
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
ELIOT L. ENGEL, New York
ALBERT R. WYNN, Maryland
BILL LUTHER, Minnesota
RON KLINK, Pennsylvania
THOMAS C. SAWYER, Ohio
GENE GREEN, Texas
KAREN MCCARTHY, Missouri
JOHN D. DINGELL, Michigan,
(Ex Officio)

CONTENTS

SPAMMING: THE E-MAIL YOU WANT TO CAN

WEDNESDAY, NOVEMBER 3, 1999

HOUSE OF REPRESENTATIVES,
COMMITTEE ON COMMERCE,
SUBCOMMITTEE ON TELECOMMUNICATIONS,
TRADE, AND CONSUMER PROTECTION,
Washington, DC.

The subcommittee met, pursuant to notice, at 10:10 a.m., in room 2123, Rayburn House Office Building, Hon. W.J. "Billy" Tauzin (chairman) presiding.

Members present: Representatives Tauzin, Oxley, Stearns, Gillmor, Cox, Largent, Rogan, Shimkus, Wilson, Ehrlich, Markey, Eshoo, Luther, Green, and McCarthy.

Staff present: Linda Bloss-Baum, majority counsel; Mike O'Rielly, majority professional staff; Cliff Riccio, legislative clerk; and Andrew W. Levin, minority counsel.

Mr. TAUZIN. The subcommittee will come to order. Good morning.

The Chair will recognize himself for an opening statement.

The Internet offers us new and exciting ways to communicate with others across the globe with unprecedented speed and certainty. But just as we experienced in our non-cyberspace everyday lives, the digital world has also inundated us with communications that sometimes we do not want to receive. The problem of unsolicited e-mail, commonly known as spam, is becoming more prevalent as the technology which allows for massive distribution of digital material increases.

America Online, the largest online service provider, estimates that one-third of the e-mail messages coming into its network from the Internet are spam. That is between 10 million and 24 million spam e-mails per day just on AOL alone. Consumers not only find the practice of spamming annoying and inconvenient, they also find it expensive. More often than not, the receiver must pay for e-mail advertisements. This is akin to receiving junk mail with postage due or having a telemarketer call your cell phone and you find out your cell phone bills have gone up.

These financial costs are only aggravated by the time and energy it takes for consumers to determine which e-mail is spam, and which is not before deleting the spam. Oftentimes this leads to accidentally discarding personal and solicited messages in the process of trying to filter out the unwanted spam. Furthermore, ISPs must, as well, spend money and time to try to filter spam—that is, buy more sophisticated computers, hire additional staff to keep the spamming problem under control. The unsolicited e-mails also cause quite a burden on the ISP's network and technical capabili-

ties. I am glad we have representatives from several ISPs with us this morning to discuss the profound effect that spam has had on their businesses.

Several States have enacted anti-spam laws such as California, thanks to my colleague, Mr. Miller, who is here today. We now have several pieces of Federal legislation pending before the committee which would allow for national guidelines on the issue of spamming. Our own colleagues from the subcommittee, Mrs. Heather Wilson and Mr. Green, have both also filed bills and are joined this morning by Mr. Miller. And Chris Smith, who was supposed to be with us, unfortunately is required to chair a hearing across the hall and has called me to apologize and to express his strong interest in this subject matter and his interest, Mr. Miller, Mr. Green, Mrs. Wilson in working with the three of you in hopefully crafting a solid piece of legislation.

We look forward to hearing from each of our members this morning to discuss their legislative proposals to help us put a stop to the practice of spamming that has become so prevalent in the digital world. I do want to say at the outset, however, that we must be careful in legislating in this area. Any legislation must be carefully crafted in order to be hard on spam without interfering with legitimate practices of businesses using e-mail to build stronger relationships with existing customers.

The information age depends upon free-flowing—constantly free-flowing and efficient systems of information. For example, when someone visits a website and indicates interest in receiving further information or updates, any e-mail that business then sends to the individual is not technically spam because it has been actually solicited. And, obviously, we have to take into account those legitimate needs of both consumers and businesses in communicating with each other.

Again, I want to thank our witnesses for taking the time to educate us today about this exciting issue regarding the digital economy. It is one of many hearings our committee has held on electronic commerce and each time we come away better educated and hopefully better informed in terms of how to make decent policy in this critical area.

I will now ask if any of the members have opening statements.

The gentleman from Florida, Mr. Stearns.

Mr. STEARNS. Thank you, Mr. Chairman, for holding this hearing.

I think I know most about this hearing. I had the opportunity to hear my colleague, Mrs. Wilson, on I guess C-SPAN radio or something when I was coming in. All the questions around the country were coming in, and I think she sort of explained it and talked about it, but I thought I would mention some of the statistics here.

I think a lot of us have been on the Internet, and we see these sort of commercial e-mails. And they appear to be legitimate commercial, unsolicited e-mails, and they talk about how you can make $50,000 in less than 90 days or you can eat as much as you want and you can lose 10 pounds a week and it is guaranteed. Of course, you double click on this and then something else is selling you different products.

Most of these e-mails are too good to be true. Then of course it goes from there all the way down, as Mrs. Wilson said on the radio this morning, into lots of different other sites.

I am also a co-sponsor of H.R. 3888, the Telecommunication Competition and Consumer Protection Act of 1998, which addressed the issue of junk mail, but I want to congratulate our colleagues for what they are doing here. H.R. 3113, the Unsolicited Electronic Mail Act of 1999 introduced by Mrs. Wilson and my good colleague, Mr. Green, is an extremely positive step in attempting to tackle the problem of spamming, and so I look forward to hearing their testimony.

Thank you, Mr. Chairman.

Mr. TAUZIN. The Chair thanks the gentleman.

The Chair now yields to the ranking minority member of the committee, Mr. Markey of Massachusetts.

Mr. MARKEY. Thank you, Mr. Chairman.

I want to commend you for calling this hearing today on spamming issues and welcome our colleagues to our committee today. We look forward to their expert testimony.

There is no question that unsolicited commercial e-mails are a problem for millions of consumers and for the industry. In particular, large bulk spamming is clogging computer networks and is a burden to local telecommunications networks as well as a terrible nuisance to the computer users who receive them.

The issue of spamming is, in fact, a particularly thorny issue to address because there are multiple players involved in resolving these problems in the telecommunications industry, the Federal Government as well as at the State level.

Part of the wonder of the net is its wide-open, chaotic nature. It allows individuals to freely communicate with others and to upset the established order. And although this speech will sometimes call consternation in some quarters, I think we all recognize that regulating speech is a very touchy subject. It is my hope that as we proceed with any legislation that we carefully fine tune the definition of what is covered and which parties ought to be held responsible and when and for what.

This year we have had a number of public policy issues arise relating to the Internet that have prompted legislative solutions—from alcohol sales online, cyberporn, filtering requirements in schools for pornography, online privacy, gambling online. And earlier this week the House passed a cybersquatting bill to regulate some of the terms and conditions of digital domain name registrations.

With respect to spamming, we are again asking that we deal with an issue that the constituents are concerned with to solve a problem particularly to the Internet and that is a great nuisance to many of them. And we have as guideposts certain precedents in how Congress has previously addressed junk fax problems, telemarketing rules. We have indeed in this committee over the last 10 years dealt with and passed laws dealing with each one of those areas.

My hope is that we can come up with a solution for dealing with spamming that preserves the best of what the Internet offers to consumers and to our economy. Again, when we proceed with fur-

ther regulation of the Internet, I believe that this subcommittee must be careful to protect the first amendment rights of individuals on the net.

Again, I want to commend you, Mr. Chairman, for this hearing this morning, and I want to commend in particular our committee colleagues, Mrs. Wilson and Mr. Green, as well as Mr. Miller and Mr. Smith, for their efforts in bringing this issue forward and for pressing us to act.

Thank you, Mr. Chairman.

Mr. TAUZIN. The Chair thanks the gentleman.

Are there further requests for opening statements?

[Additional statements submitted for the record follow:]

PREPARED STATEMENT OF HON. TOM BLILEY, CHAIRMAN, COMMITTEE ON COMMERCE

Thank you, Mr. Chairman.

For years this Committee has reviewed the regulation of unwanted solicitations to consumers. Whether they come in the form of junk mail, door to door salespeople, unwanted telemarketers, or—a form that is becoming increasingly prevalent—e-mail, these messages can annoy consumers and invade their personal privacy.

This morning, we focus on this new medium for delivering these unwanted messages, e-mail. The Internet is one of the most powerful mediums for the exchange of ideas that we have ever known. E-mail offers an affordable way for people to reach one another with rapid speed and reliable delivery.

For obvious commercial reasons, marketers have teamed to take advantage of this new capability to reach folks. Businesses now commonly engage in a practice known as "spamming" which is sending unsolicited e-mail to multiple online users at one time.

"Spamming," has a profound effect on consumers, Internet services providers and the Internet as a whole. Consumers must spend time and often money to sift through the many messages to determine which are unsolicited. Many consumers are also concerned about their personal privacy, claiming that the spammers are intruding into their homes, uninvited, through the e-mail system.

Internet service providers—or ISPs—also encounter many problems related to spamming. The excessive number of e-mails tie up network bandwidth and monopolize staff resources. ISPs also worry that their customers will blame the ISP for the unwanted e-mails thus harming their reputation and possible market share. I am sure that the liability of ISPs in these matters will be discussed fully this morning.

I am perhaps most concerned, however, about the indirect effect that spamming may have on Internet commerce as a whole. Studies have shown that this is one of the main problems leading consumers to distrust doing business online.

E-Commerce will be the driving force of the American economy in the next millennium. I have worked hard with the Commerce Committee this year to develop initiatives to help foster the growth and use of e-commerce. But without consumer confidence in the medium, E-commerce will never reach its full potential.

We need to ensure that consumers' concerns, are addressed in order to encourage the growth of e-commerce. At the same time, we must find a proper balance between businesses and online customers.

I look forward to learning more about the four bills that have recently been introduced in the House to address spam e-mail burdens. I am not yet convinced that legislation is needed in this area, but I do think that this morning's discussion is a good start. I remain interested, as I've consistently stated, in finding an industry-developed mechanism to reduce any burden on consumers for receiving unwanted e-mails. I am hopeful that this will be addressed in this morning's testimony.

I thank today's witnesses in advance for their thoughtful testimony and I thank Mr. Tauzin for holding this hearing this morning.

PREPARED STATEMENT OF HON. EDWARD J. MARKEY, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF MASSACHUSETTS

Mr. Chairman, I want to commend you for calling this hearing today on spamming issues.

There's no question that unsolicited commercial e-mails are a problem for millions of consumers and for industry. In particular large, bulk spamming is clogging com-

puter networks and is a burden to local telecommunications networks as well as a terrible nuisance to the computer users who receive them.

The issue of spamming is, in fact, a particularly thorny issue to address because there are multiple players involved in resolving these problems in the telecommunications industry, the Federal government, and at the State level as well.

Part of the wonder of the Net is its wide open, chaotic nature. It allows individuals to freely communicate with others and to upset the established order. And although this speech will sometimes cause consternation in some quarters, I think we all recognize that regulating speech is a very touchy subject. It is my hope that as we proceed with any legislation that we carefully fine tune the definition of what is covered and which parties are to be held responsible and when.

This year we have had a number of public policy issues arise relating to the Internet that have prompted legislative solutions—from alcohol sales online, cyber-porn and filtering requirements in schools, online privacy, gambling online—and earlier this week the House passed a so-called "cybersquatting" bill to regulate some of the terms and conditions of domain name registrations. With respect to "spamming," we are again asked by our constituents to solve a problem particular to the Internet that is a great nuisance for many of them and we have as guideposts certain precedents in how Congress previously addressed junk fax problems or telemarketing rules.

My hope is that we can come up with a solution for dealing with spamming that preserves the best of what the Internet offers to consumers and our economy. And again, when we proceed with further regulation of the Internet, I believe that this Subcommittee must be careful to protect the First Amendment rights of individuals on the Net. Again, I want to commend Chairman Tauzin for this hearing this morning and I want to commend in particular our Committee colleagues Ms. Wilson and Mr. Green, as well as Mr. Miller and Mr. Smith, for their efforts in this area and I look forward to continuing our efforts as we proceed on this subject sometime next year. Thank you.

PREPARED STATEMENT OF HON. ANNA G. ESHOO, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Thank you Mr. Chairman for calling this hearing.

I look forward to learning from my colleagues about the intricacies of their respective legislative approaches to dealing with the issue of "spam" e-mails.

As everyone in this room knows, the Internet is changing everything . . . from the way we are communicating with each other to the way commerce is taking place, the Internet has revolutionized the way Americans are interacting.

This revolution is necessitating the constant review of our laws and regulations to ensure they apply to this new medium.

This committee and Congress, I believe, has done a commendable job in avoiding overly burdensome regulation of the Internet, with the exception of the Communications Decency Act in the 1996 Telecommunications Act.

The burden is again on us with regard to the various legislative proposals that address the issue of spamming. Spamming exploits the core strength of the Internet—the system's openness.

America Online (AOL) has reported that spam represents over one-third of the 45 million e-mail messages it handles each day. And spam is not only annoying, its cost are borne by consumers, not marketers.

Consumers are charged higher fees by Internet service providers that must invest resources to upgrade equipment to manage the high volume of e-mail, deal with customer complaints, and mount legal challenges to junk e-mailers.

I look forward to hearing my colleagues proposals for dealing with this increasing problem and to the testimony of our witnesses and I yield back the balance of my time.

Mr. TAUZIN. The Chair is pleased to welcome our first panel, and I want to remind the members we have two panels today. We normally try to do everything in a single panel, but, because we have our own colleagues here today, we of course welcome them as a separate panel.

But the separate panel will consist of representatives of the Bureau of Consumer Protection; iHighway.net Incorporated; Sidley & Austin, here in Washington, DC; SBC Communications; Morrison

& Forester; Direct Marketing Association; as well as Alladvantage.com. So we will learn a lot from the industry with reference to the comments and suggestions we hear from our colleagues this morning. So stick around.

First, let me introduce our first panel. Of course, they are well known to all of us here on this side of the aisle, but Mr. Green, Mr. Miller, Mrs. Wilson, we want to thank you for the efforts you have already made in drafting and pursuing legislation.

We will begin with the Honorable Mr. Green from Texas with your statement. Again, all written statements are part of our record by unanimous consent. Without objection. And you are recognized to make your presentation, Mr. Green.

STATEMENT OF HON. GENE GREEN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS

Mr. GREEN. Thank you, Mr. Chairman. It is interesting to be on this side of the dias this morning. And I will submit my written statement and briefly say how I got involved in it.

Before I get started, I want to thank the witness here today from SBC, Michael Russina, who will be testifying in a few minutes. He is a Senior Director of Systems Operations of Southwestern Bell Communications where he originated SBC's Internet service company, although he did spend time with Microsoft as a systems engineer.

My first experience with spam was about 3 years ago. I had a town hall meeting which I do and all of us do in our districts, and it was a typical January day in Houston. It was 30 degrees and raining, and so I actually had three people show up at a town hall meeting at 9 on a Saturday morning.

One of those three constituents came in, a young man, and had said I don't care what you do—we talked about budget and everything else—he said, I want something done with spam. At that time, not being totally Internet friendly, I joked about I like it with A-1 steak sauce.

But he brought it to my attention and realizing what it is and I did just what the chairman and our ranking member said, well, unsolicited e-mails—we have laws against unsolicited junk mail, we have laws against unsolicited telephone calls, and even on the State levels we have regulated unsolicited faxes. And so to draft legislation on that. And so that is why originally I introduced H.R. 1910 that would talk about the fraud and the e-mail user protection act and introduced that earlier this spring.

Since that time, my colleague, Mrs. Wilson, and I have worked together to come up with our bill, H.R. 3113, which goes to basically what Mr. Chairman and Mr. Markey, our ranking member, said that it tries to do within the market is to be as least invasive as we can and to benefit from what the Internet is providing us. One, to let the ISPs have some control of their systems to where they can regulate spam. Let the individual be able to say, no, I do not want to receive spam. But also to continue the growth in Internet and the telecommunications.

Again, Mr. Chairman, what you mentioned, spam could be a business tool, and we want to continue it as a business tool without the lose 30 pounds in 5 minutes or something like that. And I

think we can deal with that, with my colleagues on H.R. 3113, because, again, it was drafted to be the least invasive and really a first step.

Now, I hope our committee would look at dealing with the fraud that we have, and our colleague from Florida mentioned it. But that is not in H.R. 3113.

But, again, to empower the individual, to empower the ISPs—and one of the best parts I think of our bill is, having owned businesses in the past and helped manage them, if I was an ISP owner and someone was using my network that I had an interest in for their profit, I would like to have them to pay a portion out of their profit. And that is just a business transaction. So our bill also allows the ISP to earn some type of revenue to work with someone who is using their network for that type of purpose.

Again, that would—we don't want to limit it. In fact, we want it to grow. And I wouldn't be a member of the Telecom Committee if I didn't appreciate the growth we have in technology and literally the next generation that we are seeing. But we also need to provide some guidelines that our constituents want us to do for unsolicited e-mails.

With that, Mr. Chairman, thank you.

[The prepared statement of Hon. Gene Green follows:]

PREPARED STATEMENT OF HON. GENE GREEN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS

I would like to take a moment and thank Mr. Michael Russina from SBC for coming to DC and testifying about spam before the Subcommittee. Mr. Russina is the Senior Director, Systems Operation at SBC, where he originated SBC's Internet Service Company, he helped establish the necessary infrastructure to provide SBC customers with internet access, email, and personal web pages. Before that he worked for Microsoft as a systems engineer. He is a 1989 graduate of Southwest Missouri State.

Spam is an unsolicited commercial email which advertises many products including: health cures, get rich quick schemes, chain letters, or can prompt a person to a pornographic website. Spam is deceptive and annoying. It displaces normal email and shifts all cost to the recipient. As email becomes more prevalent, complaints about spam will continue to rise. Spam affects everybody. For example, a few weeks ago the House of Representatives's email system was slowed to a crawl because of an unsolicited mass email about a diet pill. Spam floods an ISP's network and slows down their communications. Consumers unfairly bear the cost of the advertisement, with no recourse but to accept and then delete the message. Also, it increases cost to consumers by forcing ISPs to spend time, money, and staff on addressing this increased and unwanted traffic. In this digital age, spam is the one problem of the internet that we should address on a nation-wide basis.

This problem was brought to my attention a few years ago. In town hall meetings, letters, and emails constituents say spam is quickly becoming a priority. I recently received an email from a constituent. In her message she said, "I know there is a verbal trend to get away from 'big government,' but I, myself, think there must be an agency somewhere that has the people or budget enough to answer complaints to the extent of tracking, fining, and shutting down people who just don't get the message that other people do not appreciate their solicitations. While I don't scream, holler or throw violent fits when I receive spam, I absolutely do not appreciate getting mail from sex sites or Viagra, nor am I interested in buying anything over the internet that I have not personally sought out on my own."

Recently, a survey of 1,200 internet users conducted on the behalf of the Coalition Against Unsolicited Commercial Email found that an average person receives 24.11 messages a day, of which they consider 39% to be spam. Also, of the 1,200 person surveyed, over 76% believe that spam should be regulated by the government. Another 70% said they dislike receiving email from companies they do not do business with, and 81% object to receiving email from companies they have not heard of. In addition 86.5% dislike email promoting pornography, and 95.5% object to companies that use false addresses to avoid responses.

Why do we need to address the issue of fraud in terms of spam and the internet? Informal estimates are that over half of unsolicited commercial email contains fraudulent content. Most spam misrepresents or hides who and from where these messages originate. False email and domain addresses are an enormous source of the problem. This fraudulent information can cause mass systems overload by misrouting replies, and it can hurt the reputation of individuals and ISPs that are portrayed as the spammer. The most important reason to stop fraudulent spam is to make sure that spam does not affect consumer's confidence in electronic commerce.

Finding "a fix" for spam is not an easy task. I believe that there are multiple ways to stop spam, such as fighting fraud and allowing ISPs to enforce their own spam policies. Many of the bad actors associated with spam use fraud to mask their true identity. They want to make sure that the recipient never realizes who is sending these messages. Spammers, by hiding their identity force individuals to open and delete unwanted messages placing the financial burden on the receiver.

I address fraud in H.R. 1910, the Email User Protection Act. My bill prohibits the use of false email addresses and routing information, it makes it illegal to use or create software primarily designed to spam, and it makes it illegal to takeover another person's email account to send out spam. A few states have addressed email fraud. For example, both Washington and Virginia have passed anti-spam laws that addresses fraud. Washington's anti-spam is fairly simple. It prohibits: 1) the use of a third party's internet domain name without their permission; 2) misrepresented information in identifying the point of origin or the transmission path; and 3) messages that contain false or misleading information in the subject line. Combating fraud is just one part of an overall spam solution. Because of the nature of the problem there is more then one solution. That is why I have joined with my colleague Rep. Heather Wilson in introducing H.R. 3113.

H.R. 3113, the Unsolicited Electronic Mail Act allows both Internet Service Providers and email users to say that they do not want the financial and time burden of deleting spam. The most empowering provision of this legislation gives a person, who is on a network that accepts spam, the right to opt-out of that network's spam policy, retain their email address and post an individual sign saying they do no want spam in their in-box. This legislation gives individuals and ISPs complete control over what messages they receive. This bill's efforts coupled with my spam legislation introduced earlier this year, are good starting points in fixing this problem.

I am proud to be working with my colleagues from across the aisle and in committee on this issue.

Mr. TAUZIN. Thank you very much, Mr. Green.

Now I am pleased to welcome the honorable Gary Miller of California, who has a separate, distinct proposal; and we would love to hear from you, Gary.

STATEMENT OF HON. GARY G. MILLER, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Mr. MILLER. Good morning, Mr. Chairman, members of the subcommittee.

I would like to thank Chairman Tauzin for calling this hearing today. We have discussed it over months. I appreciate your giving all of us the opportunity to discuss this issue. And I want to commend my colleagues for being involved in the issue of spam which is a growing problem.

For those who are unaware, the use of the term spam is not meant to inject Hormel into the program. It was taken from a Monty Python skit years ago, and that is how it grew into how the word is used today.

When a spammer sends an e-mail message to a million people, it is carried by a number of other systems on its way to its destination. The carriers in between must bear the burden of transporting the bulk of advertising for the spammer, thus forcing third parties to bear the load of unsolicited advertising.

The number of spams arriving in people's mailboxes each week is growing. A recent study done by the Gardner Group shows that

90 percent of all Internet users receive spam at least weekly or bi-weekly. In effect, spam levies a tax on Internet consumers because it causes ISPs to spend money and time to filter spam, obtain additional bandwidth, buy more sophisticated computers and hire additional staff to keep the spam problem under control. Those costs are passed on to Internet consumers.

The reason the current spam situation is so serious is because millions of people only suffer a small amount of damage, making it impractical for Internet users to go to court and recover the modest amount of money that is taken from them in the spamming process. Moreover, most Internet users think spam is merely an annoyance and do not understand the cost and time associated with it is passed on to them in users' fees.

Spammers are profiting from this phenomenon. They know if they steal only a tiny bit from millions of people, they will make a substantial profit and few, if any, will bother to hold them accountable.

The problem of spam was brought to my attention over 2 years ago while I was a member of the California State assembly when a constituent of mine, Nick Anis, had his business shut down for over 3 days because his computer system was inundated with spam. After looking into the issue, I decided that legislation was needed to help people like Nick. However, I wanted to make sure the solution restored common-sense incentives and involved the government as little as possible.

I came up with seven guiding principles to help formulate the bill which eventually became law in California. I would like to go over the seven principles.

No. 1, anti-spam legislation cannot legitimize spam. Currently, Internet service providers, ISPs, can sue spammers for trespass. However, it is very expensive and time-consuming to bring these suits. Even the courts have recognized that property rights of ISPs exist. My bill clarifies existing property rights and quantifies damages. Anything that allows someone a free spam before making it illegal or in any other way allows spam, would be taking away the existing private property rights of ISPs. We do not want to take a step backwards.

No. 2, anti-spam regulation cannot regulate the Internet. We do not want this committee to ever have to do a deregulation of the Internet bill. The Internet is an ever-changing medium, relatively free of government regulation. That is why it works so well, is growing so quickly, and why Internet companies are driving our economy. We need to jealously guard the freedom of the Internet and keep the government out of it.

No. 3, anti-spam legislation has to protect free speech and not be thrown out by the courts. The courts have outlined very specific levels of protection of free speech from political, religious, commercial to obscene. These standards are already in case law. The courts have ruled that laws can be passed to curb commercial speech that transfers costs on to recipients. Outside of correcting cost shifting in commercial speech, any law that regulates specific speech content not ruled to be obscene by the Miller test—that is not the Gary Miller test; that is Miller versus California, 1973—would probably fail to pass a judicial challenge.

No. 4, anti-spam legislation cannot create a new cost or tax on the Internet. Most plans to stop spam would end up costing Internet service providers or government money.

No. 5, anti-spam legislation should guard the privacy of individuals. Information is a powerful tool for law-abiding citizens and for those who break the law. Any solution to spam cannot put personal information, including e-mail addresses, in the public domain which would put privacy at risk.

No. 6, anti-spam legislation cannot hurt Internet service providers. The Internet is a completely new communication tool. Unlike faxes or phones, which are person-to-person communication devices, e-mail is routed through numerous private computers and Internet service providers before they reach their destination. As a result, any legislative solution to spam must not hamstring the numerous Internet service providers that make up the Internet. Anything that would force ISPs to be a party to numerous lawsuits or force them to keep special regulated lists would hurt the entire Internet system, and the solution that harms ISPs is worse than the problem we currently face.

And, seven, anti-spam legislation has to work. Any solution has to be usable for those who have the ability and the desire to stop spam.

Using these principles, I came up with the Can Spam Act of 1999. Like the California State law, H.R. 2162 gives ISPs the power to put the authority of law behind their anti-spamming policies. Under this bill, if an ISP chooses to have a published policy prohibiting spam and a spammer sends out unsolicited commercial e-mail on the network that violates that policy, the ISP would have a civil right of action against the spammer for 50 dollars per message, up to $25,000 per day, thus eliminating the incentive to spam against an ISP's will.

In addition, H.R. 2162 would make illegal the act of hijacking another person's domain name for the purpose of sending out spam. H.R. 2162 is grounded in the recognition that mail servers are the private property of the businesses, schools, and service providers who own and operate them. The bill codifies the rights of ISPs to control the use of their property and to be free from intrusion and damages from third parties.

In conclusion, H.R. 2162 allows ISPs to set and enforce their own anti-spamming policies based on the needs and the desires of their customers. It counts in a marketplace solution, encouraging advertisers to strike a bargain with ISPs for mail delivery before flooding their system with unwanted mail. Should advertisers ignore the warning or fail to negotiate a deal, ISPs can bring legal action to recover damages to the system and to their customers.

The Can Spam Act will give ISPs an effective tool to stop unsolicited commercial e-mail. Currently, the financial incentive to send free mass e-mail advertising is causing spam to grow exponentially. The Can Spam Act ends that incentive by forcing spammers to pay for breaking ISPs' anti-spamming policies.

I would like to present to the FTC a disc by Chooseyourmail.com which has 1 million spam messages that were just collected in recent months.

Mr. Chairman and members, thank you for your time.

Mr. TAUZIN. Thank you very much, Mr. Miller.

Can Spam is the name of your bill. I want you to know I resisted the temptation in introducing you in saying that it was Miller time.

Mr. MILLER. Spam is one of the most popular foods in Hawaii and Japan, so I am well received there.

Mr. TAUZIN. You will have to explain the Monty Python reference.

[The prepared statement of Hon. Gary G. Miller follows:]

PREPARED STATEMENT OF HON. GARY G. MILLER, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Good morning, Mr. Chairman and members of the Subcommittee. I would like to thank Chairman Tauzin for calling this hearing this morning. I would also like to thank my colleagues, as well as all of the witnesses here today, for joining in the fight against spam. I appreciate this opportunity to appear before the Subcommittee to testify on behalf of my legislation, H.R. 2162, "The Can Spam Act of 1999."

THE PROBLEM WITH SPAM

When a spammer sends an email message to a million people, it is carried by a number of other systems on the way to its destination. The carriers in between must bear the burden of transporting the bulk advertisements for the spammer, thus forcing third parties to bear the load of unsolicited advertising. The number of spams arriving in people's mail boxes each week is growing. A recent study done by the Gartner Group shows that 90% of Internet users receive spam at least on a weekly basis.

In effect, spam levies a tax on all Internet consumers because it causes ISPs to spend money and time to filter spam, obtain additional bandwidth, buy more sophisticated computers and hire additional staff to keep the spamming problem under control. These costs are passed on to Internet consumers.

The reason the current spam situation is so serious is because millions of people only suffer a small amount of damage, making it impractical for Internet users to go to court and recover the modest amount of money that is taken from them in the spamming process. Moreover, most Internet users think that spam is merely an annoyance and do not understand that it costs them in time and user-fees.

Spammers are profiting from this phenomena. They know that if they steal only a tiny bit from millions of people, they will make a substantial profit, and few, if any, will bother to hold them accountable.

THE CATALYST

The problem of spam was brought to my attention two years ago while I was a member of the California State Assembly, when a constituent of mine, Nick Anis, had to shut down his business for three days because he was inundated with spam. After looking into the issue, I decided that legislation was needed to help people like Nick. However, I wanted to make sure that the solution restored common sense incentives, and involved the government as *little as possible.* I came up with 7 guiding principles to help formulate the bill which eventually became law in California last year:

GUIDING PRINCIPLES:

1. Anti-Spam Legislation Cannot Legitimize Spam

Currently Internet Service Providers (ISPs) can sue spammers for trespass. However, it is very expensive and time consuming to bring these suits, even though the courts have recognized the property rights of ISPs. My bill clarifies existing private property rights and quantifies damages. Anything that allows someone a free spam before making it illegal, or in any other way allows spam, would be taking away existing private property rights of ISPs that we are trying to clarify. We do not want to take a step backward.

2. Anti-Spam Legislation Cannot Regulate the Internet

We do not want this committee to ever have to do a deregulation of the Internet bill. The Internet is an ever changing medium, relatively free of government regulation. That is why it works so well, is growing so quickly, and that is why Internet companies are driving our economy. We need to jealously guard the freedom of the Internet, and keep the government out of it.

3. Anti-Spam Legislation Has to Protect Free Speech, and Not Be Thrown Out By the Courts

The courts have outlined very specific levels of protection of speech from political, religious, commercial to obscene. These standards are already in case law. The courts have ruled that laws can be passed to curb commercial speech that transfers costs onto the recipient. Outside of correcting cost-shifting in commercial speech, any law that regulates specific speech content not ruled to be obscene by the "Miller test" would probably fail to pass a judicial challenge.

4. Anti-Spam Legislation Cannot Create a New Cost or Tax on the Internet

Most plans to stop spam would end up costing Internet Service Providers or the Government money.

5. Anti-Spam Legislation should Guard the Privacy of the Individual

Information is a powerful tool for law abiding citizens and for those who break the law. Any solution to spam cannot put personal information, including email addresses, in the public domain, which would put privacy at risk.

6. Anti-Spam Legislation Cannot Hurt Internet Service Providers

The Internet is a completely new communication tool. Unlike faxes or phones, which are person to person communication devices, email is routed through numerous private computers and Internet Service Providers before they reach their destination. As a result, any legislative solution to spam must not hamstring the numerous Internet Service Providers that make up the Internet. Anything that would force ISPs to be a party to numerous lawsuits, or would force them to keep special regulated lists would hurt the entire Internet system. A solution that harms ISPs is worse than the problem.

7. Anti-Spam Legislation Has to Work

Any solution has to be usable for those who have the ability and the desire to stop spam.

H.R. 2162, "THE CAN SPAM ACT OF 1999"

Using these principles, I came up with the "Can Spam Act of 1999" (H.R. 2162)

Like the California state law, H.R. 2162 gives ISPs the power to put the authority of law behind their anti-spamming policies. Under the bill, if an ISP chooses to have a published policy prohibiting spam, and a spammer sends out unsolicited commercial email on their network in violation of that policy, the ISP would have a civil right of action against the spammer for $50 per message, up to $25,000 per day, thus eliminating the incentive to spam against an ISP's will. In addition, H.R. 2162 would make the act of hijacking another person's domain name for the purpose of sending out spam.

H.R. 2162 is grounded in the recognition that mail servers are the private property of those businesses, schools, and service providers who own and operate them. The bill codifies the right of ISPs to control the use of their property and to be free from intrusion and damage from third parties.

CONCLUSION

H.R. 2162 allows ISPs to set and enforce their own anti-spam policies, based on the needs and desires of their customers. It counts on a marketplace solution, encouraging advertisers to strike a bargain with ISPs for mail delivery *before* flooding their system with unwanted mail. Should advertisers ignore the warnings or fail to negotiate a deal, ISPs can bring legal action to recover damages to their systems and their customers.

The Can Spam Act will give ISPs an effective tool to stop unsolicited commercial email. Currently, the financial incentives to send free mass email advertisements is causing spam to grow exponentially. The Can Spam Act ends this incentive by forcing spammers to pay for breaking an ISPs' anti-spamming policy.

Thank you again, Mr. Chairman and members for the opportunity to appear before you today. I look forward to answering any questions you may have.

Mr. TAUZIN. Finally, and certainly not least, our own Heather Wilson of New Mexico for your testimony.

STATEMENT OF HON. HEATHER WILSON, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEW MEXICO

Mrs. WILSON. Thank you, Mr. Chairman. I appreciate the opportunity to testify today.

I didn't know it was the Monty Python skit. I figured it was called spam because everybody has some and nobody likes it.

Rather than—I appreciate the opportunity to put my testimony in the record, and rather than talk in detail about the problem, because I think our second panel will give us ample firsthand information about that, what I would really like to talk about a little bit is the approach we try to take in H.R. 3113 to address this problem.

I began to look at this problem about a year ago, shortly after I was elected to Congress when I started to get spammed with pornographic e-mail at home. The first one had a very innocuous subject line that said something like, what the Federal Government doesn't want you to know; and I assumed that it was some constituent informing me about fraud, waste and abuse in the Federal Government. And when I clicked on that link to find out what this was all about, I found myself in a pornographic website. This went on for several months, and I began to talk to Internet service providers as well as other people who were having the same problem and began to learn more about it and read more about it.

My greatest concern—I learned subsequently about cost shifting and those kinds of things, but it is not only adults that have e-mail addresses. It is children as well. And these innocuous subject lines which can say, the latest games you want to play, can attract a child to click on that website, and they find themselves somewhere where you don't want your child to be. So I felt as though we needed to do something about this to give power to consumers to not receive things that they did not want to have in their own homes.

Early on, looking at what had been introduced, and talking to Mr. Green particularly about his bill, H.R. 1910, and while we initially looked at merging the bills, what we decided to do was two separate ones. And I am also a co-sponsor of his H.R. 1910, which includes many of the fraud provisions and Internet fraud provisions which I think we do also need to deal with.

But H.R. 3113 is very targeted. It does not deal with fraud. It does not deal with the problem of restricting data that can be collected on the Internet from consumers or deal with criminal sanctions. It is narrowly crafted to deal with the problem of unsolicited commercial e-mail and unsolicited pandering e-mail.

We spent quite a bit of time thinking about and reading about the constitutional protection of free speech, because we knew that we had to identify very narrowly a substantial government interest and narrowly draw how the law was going to attack that. Sometimes when something is annoying and bothering you, you know you just want to stop it. You just want to stop it. But just because something is offensive or you disagree with it doesn't mean that you have a right to tell somebody else to stop doing it. But there is a right of privacy, and there is a right of Internet service providers to be compensated for their work that they do as computer providers.

I also was conscious of the need to continue to promote commerce on the Internet and that it is a wonderful new medium for people to buy things. And I have said elsewhere that sometimes I get catalogues because, like all of us here, I fly a lot on American Airlines, and I suspect that they—all those American Airlines Advantage members probably get the same catalogues I do for travel clothing that I have never heard of before. And I don't really mind that, but I would like to have the option not to receive that on e-mail just as I have the option not to receive it on regular mail.

Finally, there is the right of privacy. Everyone has the right to say what they want to say within some fairly broad parameters in this country, but they don't have the right to force us to listen. We have a right to privacy in our own homes and a right to decide to turn away that which we don't wish to hear.

H.R. 3113 does a couple of things. It clearly states what the government interest is and does not ban unsolicited commercial e-mail. It puts the power in the hands of consumers to opt out, to send a reply e-mail that says, take me off your list, or to put their name on a national opt-out list that commercial electronic mail providers or direct mail folks using e-mail have to scrub their lists.

It prevents cost shifting to the Internet service providers by giving them the right to publish a privacy policy or a commercial e-mail policy and enforce it and say that you can't send commercial e-mail without compensating me for my company's time and effort. It requires a viable return address and that companies honor opt-out addresses, and it allows parents to protect their minor children, particularly, with provisions on pandering or pornographic mail.

We use exactly the law that exists for regular mail with respect to pandering and pornographic mail, and that has already withstood constitutional scrutiny in a Supreme Court case.

Mr. Chairman, I think I will suspend there so that we can have as much time as possible with questions and with the second panel.

[The prepared statement of Hon. Heather Wilson follows:]

PREPARED STATEMENT OF HON. HEATHER WILSON, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEW MEXICO

> "If this prohibition operates to impede the flow of even valid ideas, the answer is that no one has a right to press even 'good' ideas on an unwilling recipient. That we are, often 'captives' outside the sanctuary of the home and subject to objectionable speech and other sound does not mean we must be captives everywhere. The asserted right of a mailer, we repeat, stops at the outer boundary of every person's domain."
>
> CHIEF JUSTICE BERGER
> *Rowan v. Post Office Department, 397 U.S. 728 (1970)*

The Problem

Unsolicited electronic-mail (Spam) is the "junk" e-mail that is the digital version of the material that shows up in your mail box at home. Unlike sweepstakes entries and advertisements for department stores, however, consumers have no right or means to stop it, it costs the spammer almost nothing to send it, the source and subject of the mail is often disguised, and a large portion of Spam is pornographic in nature.

Most pornographic Spam contains a luring or innocuous subject line, and a link in the text of the e-mail that takes you to a pornographic web site. I have included some examples for the record. Children who unknowingly click on a link in an e-mail *in their home e-mail box* are often presented with "teaser" images and text that many parents would find unsuitable for their viewing.

Spammers are also getting more clever as the technology advances and creating "sticky" web sites that do not let you leave easily. For example, there are sites that

have "back" keys that Internet users recognize as a way to "undo" or walk away from the entrance to a pornographic site. Instead, trying to exit takes you deeper and deeper into the site itself.

The sheer volume of Spam has led to several nationally-publicized lawsuits between major Internet Service Providers (ISPs) and bulk e-mailers. Many recipients of Spam are forced to wade through the daily barrage of "junk e-mail" to find the e-mail they want to read.

Spam is particularly troublesome for parents who want their children to have access to the advantages of the Internet while protecting them from its seamier side.

The practice of bulk distribution of Spam places burdens on the recipient, who must filter out the good from the bad; on the ISPs, who lose bandwidth capacity to serve *their* customers because the pipes are clogged with Spam; on parents, who are seeking to protect their children; and on people, who just don't want to find offensive stuff in their in-boxes.

When something is particularly annoying or offensive, our natural reaction is to prohibit it.

But there are other public interests here.

We enjoy in this country a constitutionally protected right of free speech—including commercial speech. All of us spend a lot of time on this committee marveling at and stewarding this new phenomenon called electronic commerce that is transforming how we buy products, get information and communicate with each other.

H.R. 3113

H.R. 3113 attempts to set out a clear statement of public policy and a substantial government interest in regulation of Spam and to provide a targeted remedy specifically related to that governmental interest.

H.R. 3113 does not ban Spam. It gives the power to the recipient to opt out of receiving it. The bill recognizes that Americans have a right to stand on the electronic town square on a soap box and speak, but no American can be forced to listen if they don't want to. This is particularly true when that "speech" invades the "castle" of one's home.

H.R. 3113 requires all senders of Spam to include a viable return address which can be used by a recipient to remove his or her e-mail address from the transmitters distribution list. Use of the "Reply to Sender" e-mail address to "harvest" or collect viable e-mail addresses—a common practice today—is prohibited.

H.R. 3113 requires Spammers to honor requests not to receive commercial e-mail. If a family does not want to receive Spam from a particular sender, the sender must honor that request. If the request is not honored, the family can either sue the violator to recover the actual cost of the violation or for $500 per violation, whichever is greater.

H.R. 3113 gives ISPs the right to establish privacy policies and the right to decline to carry commercial electronic e-mail without compensation. They, too, can recover actual costs or $500 per violation, whichever is greater.

If an individual, family, or IS does not want to sue a violator, they can turn to the FCC to enforce their decision.

Allowing ISPs to set and enforce their own policies will result in a market niche: spam-free ISPs. Individuals who never want to receive Spam will be drawn to such ISPs. However, in the event that an IS allows a third-party to send Spam to its customers, and the subscriber still never wants to receive Spain, H.R. 3113 also creates a global opt-out list to which e-mail users may add their name and e-mail address. If, after 30 days on the list, a bulk e-mailer sends Spam to any recipient who's e-mail is included in the opt-out list, the FCC can order the bulk e-mailer to stop all future transmissions. In effect, bulk e-mailers are required to clean their distribution lists—at their own cost—every thirty days.

This mechanism is similar to the law for postal direct marketers.

Constitutionality

We considered the problem of constitutionality very carefully as we crafted this bill. The most important case that establishes the standard by which restriction of commercial speech will be judged, *Central Hudson Gas & Electric Corporation v. Public Service Commission of NY,* was decided in 1980. There is a three part test:

There must be a substantial governmental interest at stake
The restrictions imposed must directly advance that governmental interest
The regulation must be narrowly drawn

We spent a great deal of time in H.R. 3113 crafting the findings and statement of policy to make it clear to any court considering this law in the future what the governmental interest is and why it is substantial.

The restrictions in the bill are narrowly drawn only to advance those governmental interests.

In addition to commercial e-mail, H.R. 3113 also addresses pandering e-mail. This section of the bill is drawn directly from existing statutes on junk mail that have already withstood judicial scrutiny

In *Rowan v. Post Office Department*, Justice Berger, commenting on the First Amendment considerations of the postal statute, stated: "If this prohibition operates to impede the flow of even valid ideas, the answer is that no one has a right to press even 'good' ideas on an unwilling recipient. That we are often 'captives' outside the sanctuary of the home and subject to objectionable speech and other sound does not mean we must be captives everywhere. The asserted right of a mailer, we repeat, stops at the outer boundary of every person's domain."

The Supreme Court of the United States has traditionally respected the right of a household to bar, by order or notice, solicitors, hawkers, and peddlers, from his property.

In his decision, Chief Justice Berger stated, "To hold less would tend to license a form of trespass and would make hardly more sense than to say that a radio or television viewer may not twist the dial to cut off an offensive or boring communication and thus bar its entering his home. Nothing in the Constitution compels us to listen to or view any unwanted communication, whatever its merit; we see no basis for according the printed word or pictures a different or more preferred status because they are sent by mail. The ancient concept that 'a man's home is his castle' into which 'not even the king may enter' has lost none of its vitality, and none of the recognized exceptions includes any right to communicate offensively with another."

Several proposals before Congress in recent years have attempted to ban all Spam. I believe this approach may be unconstitutional because it would ban unsolicited mail that people do not mind receiving—or even want to receive—as well as commercial speech that is unwanted. In this way, the complete ban is probably too broad to pass constitutional muster.

Others have pointed to the junk fax law as a model for banning spam. The federal government enacted legislation that outlaws all unsolicited commercial faxes because the cost of transmitting a "junk fax" is borne almost entirely by the recipient. The government acted to prevent the bulk fax industry from shifting the burden of the advertising onto the recipient.

Spam is different.

The "cost" of Spam for the recipient is not as tangible as that of unsolicited commercial faxes. Instead of toner and paper, the cost is time spent online downloading and sorting unwanted e-mail. There is no doubt that the government should help protect Americans from this burden, but an outright ban of Spam would probably fail the *Central Hudson* test.

Instead, H.R. 3113 provides a "more limited restriction" on speech by removing the government from the equation as much as possible, leaving the decision as to the prohibition of Spam solely in the hands of the private citizen. As Chief Justice Berger wrote in Rowan, "In effect, Congress has erected a wall—or more accurately permits a citizen to erect a wall—that no advertiser may penetrate without his acquiescence. The continuing operative effect of a mailing ban once imposed presents no constitutional obstacles; the citizen cannot be put to the burden of determining on repeated occasions whether the offending mailer has altered its material so as to make it acceptable. Nor should the householder have to risk that offensive material come into the hands of his children before it can be stopped."

Promoting Commerce

All of us want to see commerce flourish on the Internet. The technology and the marketing strategies are evolving daily in this new medium. H.R. 3113 specifically recognizes that, just like the advertisements in your mailbox or the new catalogues that get sent to you that you didn't ask for, the Internet can be an important mechanism through which businesses advertise and attract customers. This is yet another reason to craft a targeted piece of legislation that addresses a problem without overreacting to it.

Conclusion

H.R. 3113 allows individuals, families, and ISPs to identify specific transmitters they do not want to receive Spam from or to prohibit all Spam.

H.R. 3113 intentionally leaves all decisions about content and regulation to the individual e-mail user and ISP. The government will merely play the role of a backstop in the event that individual e-mail users are unable to protect the privacy of their e-mail boxes.

I look forward to hearing the testimony of the witnesses who have joined us here today and working on meaningful legislation that serves the public interest.

Mr. TAUZIN. I thank the gentlelady.

We have about 10 minutes. Let's get a little done before we have to run to vote.

Let me ask you. You all looked at each other's bills. You are obviously closely attuned to what each other is proposing in the three different bills. Could you summarize for us the differences—if there are any real differences in the approaches you have taken on any one of the issues you have described in this larger issue?

Gary, you want to start for me?

Mr. MILLER. Well, that is—doing it in a way where we are not attacking each other's bill.

Mr. TAUZIN. I would appreciate that. Thank you.

Mr. MILLER. The problem I have with opt-outs, and when I presented this bill in California most major Internet service providers had opposition to opt-outs, because it opens privacy concerns. If we are going to create a national list, that list is made to the public. It is not like going down to the post office where you put your name on the list, and you say I don't want certain information. That is not made public.

The issue of privacy, people who tend to want opt-outs might be enticing certain groups who want that list to approach them for other purposes. It might not be considered commercial e-mail for the purpose of selling a product, but it could be for some other purpose.

So opt-outs are something I tried not to include because I was trying to provide for privacy, and opt-outs—how do you deal with a company who has a hundred different computers: Company A—computer one, computer two, computer three, computer four? You have a security problem all of a sudden when you try to include opt-outs for businesses, especially large corporations who don't want their domain names released to the public.

So immediately when you start having opt-outs with a national list, you have a problem with security. That is not to impugn their bill. That is a major debate we had——

Mr. TAUZIN. If I could jump in, one of the differences—you don't have opt-outs and you don't have national——

Mr. MILLER. My bill does not inject government at all. My bill clarifies a gray issue in the law and turns private property rights back to the Internet service providers.

When they go to court, they have a clear cause of action. If they decided to publicly post that they do not accept spam without prior authorization, that means a spammer has to go to them and either cut a deal to send spam or it is illegal. If spammers don't do that, when they go to court, they don't have to debate their case. They have a clear, defined cause of action when going to court.

Mr. TAUZIN. I am trying to, under the different approaches—your approach calls—really counts upon the ISP provider themselves to take action to prevent the use of the network for spamming purposes.

Mr. MILLER. It is not mandatory.

Mr. TAUZIN. It allows them. What rights under your approach does the consumer have to stop e-mail?

Mr. MILLER. I didn't include consumers in the bill specifically, but it doesn't preclude consumers from taking a spammer to court if they so choose.

The problem with doing that and the reason I decided not to—as you are probably aware, if somebody sues a spammer the ISP is going to be named in the suit also. That is just going to be a normal course of action. So did I want to come up with a regulation that mandated that ISPs are going to be forced into court day after day after day for a $50 lawsuit? I didn't think that was productive.

An individual receives one spam. An Internet service provider might have 100,000 spams go through the service or a million on one hit. Well, there is sizable damage of $25,000 for those. The problem with notifying the FCC and that you had to notify the spammer before you can go against the spammers, spammers are very crafty, as you know, and many spamming companies change their names every week. So by the time you receive a spam, you notify the FCC, they track down the spammer, notify them, that spammer has set up a new name or business name and they are spamming the same people again under a different name.

Mr. TAUZIN. Let me give Mrs. Wilson and Mr. Green a chance to tell me why you think your approach, which is different—you apparently are empowering the individual to do something. Why do you think that approach is better and why does it not run into the problem Mr. Miller has pointed out to us?

Mrs. WILSON. Let me talk about a couple of differences.

H.R. 3113 does not deal with fraud, which Mr. Green's bill does. It also does not set up penalties for harvesting e-mails, which is often done, or selling information from people's e-mails accounts so those issues are not dealt with in H.R. 3113. It is narrower in that sense. Not that we don't have to deal with those issues, as I have said.

H.R. 3113 gives rights to consumers and to ISPs. So a consumer can opt out, but an ISP can also say I have a privacy policy or we don't—we are a spam-free ISP or spam free or here's our tariff rate for how much it costs us to carry your commercial e-mail. Fairly fundamentally, we don't ban commercial e-mail in this bill and recognize that there is legitimate commercial electronic mail. The question is, can you prohibit the cost shifting and can you give rights also to the consumers? So it is a different approach.

Finally, I would note the front end of the bill which we often ignore. The statement of findings and the statement of policy we worked very carefully on with respect to judicial review.

Mr. TAUZIN. Mr. Markey?

Mr. MARKEY. Gary, do you make a distinction between commercial and noncommercial?

Mr. MILLER. Yes, it is unsolicited commercial e-mail.

Mr. MARKEY. Unsolicited commercial e-mail. So noncommercial is not covered.

Mr. MILLER. Is not covered. It doesn't cover political speech or anything else.

Mr. MARKEY. Do you make that same distinction between commercial and noncommercial?

Mrs. WILSON. I do. I also have a definition of pandering e-mail.

Mr. MARKEY. Do you make a distinction between commercial e-mail and bulk e-mail solicitations?

Mrs. WILSON. No.

Mr. MARKEY. How would you define unsolicited? For example, in the financial services bill that we are voting on today, once you have some communication with the financial institution, you don't have an ability to opt out at all. They can solicit you forever, and you have no right to say, no, I don't want to receive any additional communication in any form. You are just now on their list. Would you give under your legislation the ability to—would you define that as unsolicited or solicited? The fact that you had a transaction with the site, that you had visited a site, is any subsequent communication then considered to be solicited or unsolicited?

Mr. GREEN. I would view it as you can visit the site, but you have the right then to say, yes, I have visited but, no, I do not want to continue receiving it whether it be from a bank or whatever. Of course, our legislation is going to be different from the financial institution bill.

Mr. MARKEY. Gary?

Mr. MILLER. You can spam 5 million people and you will have visited 5 million sites, but that does not justify unsolicited commercial e-mail. It is very easy to define. It has to be bulk. It has to be of a commercial nature and it has not been requested by individuals.

Mrs. WILSON. We define it as any electronic mail message that advertises a product for service or profit and for a business purpose that is sent to a recipient with whom the initiator does not have an existing business relationship. In addition to that, if you get an e-mail from somebody whose Internet site you visited, you can send a reply. The reply address has to be legitimate. Say take me off your list.

Mr. MARKEY. If I visit a site, even though we don't purchase anything, do I have an existing commercial relationship or do I have to have purchased something?

Mrs. WILSON. It is my view you do not.

Mr. MARKEY. You do not have to purchase something. Just the fact that you visited it now exempts them from any restrictions on subsequent e-mail solicitations?

Mrs. WILSON. It is my view that is not an existing business relationship.

Mr. MARKEY. Thank you. I thank you all very much.

Mr. SHIMKUS [presiding]. You all want to vote, don't you? We will call recess until——

Mr. GREEN. Mr. Chairman, I don't know if there are still questions for committee members. We might want to go on to the second panel so we can have the questions of the experts. We can always talk to each other.

Mr. SHIMKUS. The desire will be to recess until about 5 after. We will go to the second panel. You all are dismissed.

[Brief recess.]

Mr. TAUZIN. Before the Chair introduces our next panel, I would like to offer into the record the written testimony of Mr. Smith, who, as I pointed out, could not be here because he is chairing an-

other hearing, and also—that will be introduced without objection. So ordered.

[The prepared statement of Hon. Christopher H. Smith follows:]

PREPARED STATEMENT OF HON. CHRISTOPHER H. SMITH, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEW JERSEY

Anyone who uses the Internet knows about unsolicited commercial email (UCE). Often called spam, UCE is not only annoying, it is expensive. Internet Service Providers (ISPs) have had to constantly upgrade their equipment to allow for a higher volume of email, and many have invested in filtering and tracking software to prevent unwanted mail. Who pays for these costs? Consumers do.

Spam costs consumers money and time, and it could be dangerous. Unwanted email reduces productivity because it takes time to delete, and it can damage a computer if someone opens an email that contains a damaging virus. Often, users accidentally delete important messages while trying to clear out their email in-box. Some email programs aren't able to recover messages that have been inadvertently deleted.

Congress has an obligation to protect Internet users from unwanted email that often promotes illegitimate business practices, uninvited pornography that can be improperly accessed by children, and other unwelcome solicitations. Spam is intrusive and represents a form of theft. It shifts the burden of paying for something—advertising in this case—from solicitors to consumers.

To protect consumers, I have introduced an improved version of my bill from the previous Congress: H.R. 3024, the Netizens Protection Act of 1999. My legislation not only allows ISPs to take strong action against spammers, it also gives those adversely affected by spam the right to take civil action against the sender. H.R. 3024 makes it unlawful to send UCE if the message does not include the physical address and email address of the initiator of the transmission. Further, senders must provide a way for consumers to electronically opt out and be removed from their list. Additionally, H.R. 3024 would make it illegal to include information in the email subject line that is false or misleading about the content of the message.

However, unlike other anti-spam bills, the Netizens Protection Act directly empowers consumers to take individual action against their spammer. My bill would allow someone harassed by UCE to seek up to $500 for each unsolicited email message, plus the cost of damages. Someone could seek treble damages if a spammer sent them additional email after being requested to stop. To enhance consumer rights, ISPs would be required under H.R. 3024 to make their unsolicited electronic mail messaging policies known. This would include any option that providers have to allow customers to elect to receive or not receive unsolicited email. Therefore, spammers would be forewarned and users could make an informed decision about what ISP to use, and whether to block unsolicited email. The decision to send or receive spam would be up to consumers and the marketplace.

The Netizens Protection Act would also allow ISPs to seek legal remedies if someone violated their policies against UCE, or illegally used their equipment to transmit unwanted mail. This happens all too often today, and my bill would give ISPs the tools to end it. Additionally, my bill would protect ISPs that make good faith efforts to stop spam. Lawsuits against ISPs for any harm resulting from their failure to prevent the receipt of UCE would be preempted under H.R. 3024.

My bill is aimed at the big spammer. It would not go after someone who just sent a few messages either inadvertently or even intentionally. Language in H.R. 3024 would allow someone to send up to 50 identical or substantially similar messages to recipients within a seven-day period. The legislation would not interfere with, or affect, direct email advertising or marketing; it would only block unwanted email solicitations. If any previous business relationship existed between email senders and email recipients, my legislation would not affect their transactions. A purchase at a retail store or from a catalogue would establish a business relationship. All avenues of legitimate direct marketing would remain.

Spam can only discourage Internet use, thereby impeding the expansion of Internet business and commerce which is expected to top $500 billion this year. The Internet and its many communication capabilities are here to stay, and more people are using them each day. Consumers should not have to relinquish control over their email during this rapid expansion. Users should be able to decide who they want to correspond with and what messages they want to receive. They should not have to invest their time and money for something they do not want, and neither should their Internet Service Provider.

I believe in the First Amendment, and in the traditional right for anyone to advertise their products as much and as widely as they can. However, I do not believe American consumers should have to pay for anyone's advertising. Marketing by email does not have the same costs associated with it as other forms of advertising—including the use of direct mail to which it has been compared. Direct mail advertising includes a predetermined cost for each advertisement. That cost is born mostly by advertisers and includes paper, printing, handling, and postage. Spammers, however, can send out millions of messages with a few clicks of a mouse and keyboard. Unlike direct mailers, spammers' marginal costs of sending another 1,000 advertisements are minimal, and do not increase in proportion to the number of additional people receiving their advertisement. Spammers bear almost no cost and instead shift it to consumers, who pay higher ISP rates for extra band width and screening software. I believe that the Netizens Protection Act is a fair and balanced plan to protect e-commerce, and to empower both ISPs and consumers by granting them an appropriate way to fight spam.

Mr. TAUZIN. And also ask unanimous consent to introduce a letter I received from the Honorable Ben Gilman regarding this bill and other issues related to communications that he asked me to introduce into the record. Without objection, introduce that letter into the record.

[The letter follows:]

CONGRESS OF THE UNITED STATES
HOUSE OF REPRESENTATIVES
November 1, 1999

The Honorable W.J. "BILLY" TAUZIN
Chairman, Subcommittee on Telecommunications, Trade and Consumer Protection
Committee on Commerce
U.S. House of Representatives
2183 Rayburn House Office Building
Washington, D.C. 20515

Re: **H.R. 1817, Rural Cellular Legislation**

DEAR CHAIRMAN TAUZIN: Thank you for holding a November 3 hearing on H.R. 2162, H.R. 3113, and H.R. 1910, three bills to control unsolicited commercial E-mail or "spam."

In October 1998, the House of Representatives approved H.R. 3888, the Telecommunications Competition and Consumer Protection Act of 1998, which unfortunately failed to pass the Senate because of a dispute over non-telecommunications issues. Although H.R. 3888 focused on slamming (Title I), it also included a Sense-of-Congress relating to spamming (Title II), an FCC auction provision (Title III), and a new cellular license provision (Title IV.

Accordingly, Title IV of H.R. 3888, the rural cellular license provision, was based on H.R. 2901, a bill introduced in November 1997 by former Rep. Joe McDade and cosponsored by Rep. Anna Eshoo and former Rep. Scott Klug, members of your Subcommittee. In September 1998, the Subcommittee held a hearing on H.R. 2901 and heard testimony in support of the bill from Phil Verveer, an attorney with Wilkie Farr & Gallagher. The full Commerce Committee subsequently approved H.R. 3888, with a bipartisan Tauzin-Dingell substitute, approved by voice vote, incorporating a modified version of H.R. 2901 (House Report 105-801). H.R. 3888, with further modification of the rural cellular license provision made by managers' amendment after consultation with the FCC, passed the House on suspension by voice vote on October 12 (Congressional Record H10606-10615).

Title IV of H.R. 3888, the rural cellular license provision, is the basis for H.R. 1817—a bill I introduced in May 1999, with Rep. Eshoo and Rep. Carolyn Maloney as cosponsors, now before your Subcommittee.

As noted at your September 1998 hearing, most rural areas of this country have two permanent cellular licensees company to provide quality service over their respective service territories. Competition between two licensees improves service for businesses, governments, and private users and, at the same time, improves response times for emergency services.

Unfortunately, three rural service areas in Pennsylvania, Minnesota, and Florida do not enjoy the benefit of this competition. The Pennsylvania rural service area has only one cellular operator. The Minnesota rural service area and the Florida rural service area each have two operators, but one of the operators in each area is operating under a temporary license and thus lacks the incentive to optimize service.

The reason for this lack of competition is that in 1992 the FCC disqualified three partnerships that had won the licenses, after finding that they had not complied with its application rule under the foreign ownership restrictions of the Communications Act of 1934. Significantly, the FCC had allowed other similarly situated licensees to correct their applications and, moreover, Congress repealed the relevant foreign ownership restrictions in the Telecommunications Act of 1996.

H.R. 1817 would direct the FCC to allow the partnerships denied licenses to serve the Pennsylvania, Minnesota, and Florida rural service areas to resubmit their applications consistent with FCC rules and procedures. The partnerships would pay fees to the FCC consistent with previous FCC auctions and settlements with other similarly situated licensees. To ensure speedy service to cellular customers, the FCC would have 90 days from date of enactment to award permanent licenses, and if any company failed to comply with FCC requirements the FCC would auction the license. The licenses would be subject to a five-year transfer restriction, and the Minnesota and Florida licenses would be subject to accelerated build-out requirements.

In light of the need to improve cellular service in these three rural areas and the Subcommittee's thorough consideration of the predecessor legislation in 1998, I respectfully request that the Subcommittee expeditiously act on H.R. 1817 as it moves forward with spamming, slamming, and other telecommunications legislation this Congress.

With best wishes,

Sincerely,

BENJAMIN A. GILMAN
Member of Congress

cc: Honorable Anna Eshoo and Carolyn Maloney

Mr. TAUZIN. Now I am pleased to introduce our second panel of witnesses. They will include Eileen Harrington, Associate Director of Marketing Practices of the Federal Trade Commission; John Brown, President of iHighway.net Incorporated; Alan Charles Raul of Sidley & Austin here in Washington; Michael Russina of SBC Communications; Charles Kennedy of Morrison & Forester in Washington, DC; Jerry Cerasale, a frequent visitor of our committee, of Direct Marketing Association; and Ray Everett-Church, Vice President for Public Privacy of Alladvantage.com of Hayward, California.

Gentlemen, ladies, thank you so much for being with us and for adding to our information base.

We will begin with Ms. Harrington. Remember, your written testimony is a part of our record by unanimous consent. We would appreciate a summary and as much of a conversational hearing setting as possible.

Ms. Harrington, thanks again for your keen attention to these and other issues as you educate our committee. We welcome you and appreciate your testimony.

STATEMENTS OF EILEEN HARRINGTON, ASSOCIATE DIRECTOR OF MARKETING PRACTICES, BUREAU OF CONSUMER PROTECTION, FEDERAL TRADE COMMISSION; JOHN M. BROWN, PRESIDENT, IHIGHWAY.NET INCORPORATED; ALAN CHARLES RAUL, SIDLEY & AUSTIN; MICHAEL RUSSINA, SENIOR DIRECTOR, SYSTEMS OPERATIONS, SBC COMMUNICATIONS INCORPORATED; CHARLES H. KENNEDY, MORRISON & FORESTER LLP; JERRY CERASALE, SENIOR VICE PRESIDENT, DIRECT MARKETING ASSOCIATION; AND RAY EVERETT-CHURCH, CHIEF PRIVACY OFFICER AND VICE PRESIDENT FOR PUBLIC PRIVACY, ALLADVANTAGE.COM

Ms. HARRINGTON. Thank you, Mr. Chairman. It is a privilege to be here again before your subcommittee. I am here this morning

to present the FTC's testimony on the subject of unsolicited commercial e-mail.

As you know, the FTC is the Federal Government's principal consumer protection agency, and while bulk UCE burdens Internet service providers and frustrates our customers, our main concern with unsolicited commercial e-mail is its use by deceptive and fraudulent marketers. While not all UCE is deceptive or fraudulent, it certainly is true that UCE has become the fraud artist's calling card on the Internet.

I want to focus this morning on three approaches that we have taken to protecting consumers from deceptive UCE: first, tough law enforcement; second, aggressive consumer education; and, third, the encouragement of marketplace innovations that empower consumers to keep unwanted UCE out of their electronic mailboxes.

First, the importance of law enforcement. The FTC has responded to the proliferation of deceptive or fraudulent UCE with tough law enforcement action. The Commission brought its first enforcement action against deception on the Internet in 1994—which is like a century ago in Internet years—and, not surprisingly, that case involved deceptive spam. Since that time, the Commission has brought over 100 additional law enforcement actions to halt online deception and fraud and, as importantly, to establish clear principles for non-deceptive marketing on the Internet. Seventeen enforcement actions targeted schemes that used deceptive spam as an integral part of their operation.

Let me give you a good example of the kind of scheme that we are attacking through law enforcement.

Last May, we filed a case, FTC versus Benoit. In the Benoit case, the defendants sent UCE to thousands and thousands of consumers. It arrived with a subject line that said that the message was concerning your order. The spam told recipients that their order had been received, it was being processed, and that their credit cards would be billed for charges ranging from $250 to $899. Of course, the consumers who received this spam had ordered nothing. They had no relationship whatsoever with the sender.

The spam told recipients to call a specified telephone number in the 767 area code if they had any questions about their order. Because the defendants used a deceptive header and other information, consumers who tried to reach them by hitting reply simply got an error message back. So calling on the phone was the only way that they had to reach the sender.

Now, when consumers called this telephone number, they learned a lot that the spam didn't tell them. The spam didn't tell them, for example, that the call to this phone number went to a foreign country, Dominica, in the West Indies, that the call would be billed at an expensive international rate, and that it would connect callers to a sexually explicit chat line.

We learned about this scheme from an irate grandfather in North Carolina whose preadolescent grandson received this spam. We have a special Internet fraud rapid response team of investigators and lawyers at the FTC. They jumped right on this, and within weeks we were in court obtaining a temporary restraining order that froze money in the telephone billing and collection system that was marked for these defendants. We also obtained, ultimately,

very strict injunctions that will prohibit these defendants from doing anything remotely similar to this in the future.

We target our modest enforcement and education resources at the FTC by using a very rich array of data—consumer complaint data that we collect around the clock each and every day. The FTC's Consumer Response Center receives thousands of complaints from consumers every week who use our online complaint form, call our toll-free consumer help line, or send us their complaints by fax or regular mail.

We also encourage consumers to send us examples of the spam that they receive and to send it to our special electronic spam mailbox, UCE, at FTC.gov. We have received over 2 million pieces of spam from consumers this way, and we receive an additional 3 to 4,000 pieces from consumers every day. Of course, Mr. Miller has now given us another million, so this is a red letter day. The spam that is sent to us at UCE at FTC.gov is stored in a special spam data base which we can search for the prior 6 months' worth of content.

On the public education front—if I may take just another minute, Mr. Chairman. I see my light is on—but we think that public education is also extremely important, and we have launched three aggressive education campaigns to warn consumers about deceptive UCE. To increase our reach we have asked for and received help from ISPs and other online businesses to reach as many consumers as we can with our fraud prevention messages. One of our campaigns was this FTC dirty dozen which we developed by searching our spam data base. These are the 12 most likely spam scams to arrive in your mailbox.

Now, the good news is that we think that this education is actually having an effect. Unlike in the case of telemarketing fraud where we know that millions of consumers have been defrauded of billions of dollars because of these deceptive telephone pitches, what we find is that very few consumers are actually taking the bait on these deceptive e-mails. When we have looked through our spam data base and called the consumers who sent us the spam, we have learned that they didn't bite, and we have a hard time finding others who have bitten. So while we see these ''lose weight while you sleep'' and ''earn zillions of dollars in your spare time'' messages, we have a hard time finding people who have parted with their money. Of course, the exception to that rule is the cases we have brought.

Last, we are great proponents at the Commission of encouraging marketplace solutions that empower consumers to control the content coming into their boxes, and you are going to hear about some of those from Mr. Cerasale and others. So we think that the solution to the spam problem, the deceptive spam problem, is found in tough and targeted law enforcement, aggressive education, and the encouragement of marketplace solutions that empower consumers to keep this kind of material from arriving in their inbox.

I would be happy to take your questions, Mr. Chairman.

[The prepared statement of Eileen Harrington follows:]

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

Mr. Chairman, I am Eileen Harrington of the Federal Trade Commission's Bureau of Consumer Protection. The Federal Trade Commission is pleased to provide testimony today on the subject of unsolicited commercial email, the consumer protection issues raised by its widespread use, and the Federal Trade Commission's program to combat deceptive and fraudulent unsolicited commercial email.[1]

I. INTRODUCTION AND BACKGROUND

A. FTC Law Enforcement Authority

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

B. Concerns about Unsolicited Commercial Email

Unsolicited commercial email—"UCE," or "spam," in the online vernacular—is any commercial electronic mail message sent, often in bulk, to a consumer without the consumer's prior request or consent. The staff of the Commission has amassed a database containing over 2 million pieces of UCE. Analysis of this UCE database shows that well-known manufacturers and sellers of consumer goods and services seldom send UCE. Rather, merchants of this type use *solicited* email 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 emails about discounted airfares.

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

Not all UCE is fraudulent, but fraud operators—often among the first to exploit any technological innovation—have seized on the Internet's capacity to reach literally millions of consumers quickly and at a low cost through UCE. In fact, UCE has become the fraud artist's calling card on the Internet. Much of the spam in the Commission's database 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.

---

[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).

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 FRAUD ON THE INTERNET

A. Law Enforcement

Deceptive UCE is 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 over 100 law enforcement actions to halt online deception and fraud. The pace of our Internet law enforcement has been increasing, in step with the growth of commerce—and fraud—on the Internet; over half of the FTC's Internet-related actions have been filed since the beginning of this year.

The Commission brings to the Internet a long history of promoting competition and protecting consumers in other once-new marketing media. These past innovations have included television advertising, direct mail marketing, 900-number sales, and telemarketing. The development of each of these advances in the market 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 way of doing business. In each instance, the Commission used its statutory authority under Section 5 of the FTC Act to bring tough law enforcement actions to halt specific deceptive or unfair practices, and establish principles for non-deceptive marketing.[5] In some instances, most notably national advertising, industry took an aggressive and strong self-regulatory stance that resulted in dramatic improvements in advertising and marketing practices.[6] In other instances, at the direction of Congress or on its own initiative, the Commission has issued trade regulation rules to establish a bright line between legitimate and deceptive conduct.[7]

B. Monitoring and Studying 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 stakeholders 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 global 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.

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

A. Monitoring the Problem

In June 1997, at a workshop addressing issues of privacy on the Internet, the Commission heard discussion of three distinct UCE problems: (1) deception in UCE content; (2) economic and technological burdens on the Internet and delivery net-

---

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

[5] Section 5 of the FTC Act, 15 U.S.C. §45, authorizes the Commission to prohibit unfair or deceptive acts or practices in commerce. The Commission may initiate administrative litigation, which may culminate in the issuance of a cease and desist order. It can also enforce Section 5 and other laws within its mandate by filing actions in United States District Courts under Section 13(b) of the FTC Act, 15 U.S.C. 53(b), seeking injunctions 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.

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

[7] For example, the Rule Concerning Cooling-Off Period for Sales Made at Homes or at Certain Other Locations (the "Cooling-off Rule"), 16 C.F.R. Part 429; the Mail or Telephone Order Merchandise Rule, 16 C.F.R. Part 435; the 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.

works 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. The FTC asked industry and advocacy groups that participated in the privacy workshop to focus on the economic and technological burdens caused by UCE and report their recommendations back to the Commission. Under the leadership of the Center for Democracy in Technology, these groups spent a year studying the problem and identifying possible solutions, and in July 1998 issued their "Report to the Federal Trade Commission of the Ad-Hoc Working Group on Unsolicited Commercial E-Mail"[9] ("Ad-Hoc Report"). The Ad-Hoc Report recommended the pursuit of technologies and public policies that would give more control to consumers over the UCE they received. Specifically, the report:

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

On another front, the FTC set up a special electronic mailbox reserved for UCE in order to assess, first hand, emerging trends and developments in 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 2,010,000 forwarded messages to date, including 3,000 to 4,000 new pieces of UCE every day. Staff enters each UCE message into the database; UCE received and entered in the database within the preceding 6 months is searchable. Periodically, staff analyzes the data, identifies trends, and uses its findings to target law enforcement and consumer and business education efforts.

B. Aggressive Law Enforcement

The Commission has responded to fraudulent UCE with a vigorous law enforcement program. To date, the FTC has brought 17 actions, most of them in federal district court, against schemes that employed spam as an integral part of their operation. For example, in May of this year the Commission filed *FTC v. Benoit, et al.*[11] This scheme used the ruse of a spam notification about charges purportedly to be billed to consumers' credit card accounts to lure the consumers into calling an expensive international telephone number.[12] The initial spam message purported to inform consumers that their "orders had been received and processed" and that their credit card accounts would be billed for charges ranging from $250 to $899. In fact, the consumers had not ordered anything. The spam advised recipients to call a specified telephone number in area code 767 with any questions about the "order" or to speak to a "representative." Many consumers were unaware that area code 767 is in a foreign country—Dominica, West Indies—because it was unnecessary to dial 011 or any country code to make the calls.

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

The Commission's complaint alleged that the defendants induced consumers to incur charges for a costly international audiotext entertainment service by falsely representing that consumers had placed a merchandise order that would be charged on their credit cards, and that consumers who called a specified telephone number—

---

[9] The Ad-Hoc Report is available at www.cdt.org/spam.

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

[11] No. 3:99 CV 181 (W.D.N.C. filed May 11, 1999). This case was originally filed under the caption *FTC v. One or More Unknown Parties Deceiving Consumers into Calling an International Audiotext Service Accessed Though Telephone Number (767) 445-1775.* Through expedited discovery, the FTC learned the identities of the perpetrators of the alleged scam by following the money trail connected to the telephone number. Accordingly, the FTC amended its complaint to specify the defendants' names.

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

actually the number for the audiotext entertainment service—would receive answers to any questions about the order.

The Commission, on October 26, 1999, approved a stipulated final order resolving the charges in the complaint and the settlement is now awaiting approval by the Court. Under the terms of the settlement, the defendants will be enjoined permanently from misrepresenting any material fact in the course of advertising, promoting, offering, or selling of any good or service. More specifically, the settlement will prohibit the defendants from sending or causing to be sent any email (including unsolicited commercial email) that misrepresents the identity of the sender of the email or the subject of the e-mail. The Order thus prohibits the defendants from falsifying information in the "from" and "subject" lines of e-mails, as well as in the text of the message.

Another recent case, this time targeting an alleged pyramid scheme that centered on spam, is *FTC v. Martinelli.*[13] The defendants in that case ran DP Marketing, a Connecticut-based alleged pyramid scheme, elaborately disguised as a work-at-home opportunity. The scheme solicited new recruits through "spam" and through newspaper classified ads across the country. The spam contained messages such as: "National Marketing Company seeks individuals to handle office duties from home. This is a full or part-time position with a salary of $13.50/hr. The position consists of processing applications for credit, loans or employment, as well as online consumer service."

Consumers responded by visiting DP Marketing's Web site or by calling the company. In either case, the defendants informed the consumers that the $13.50 per hour jobs were for processing orders for DP Marketing from the comfort of their own homes. The defendants further told consumers that no experience was necessary, and that for a "registration fee" ranging from $9.95 to $28.72 they would be sent everything they would need to get started, including telephone scripts, product sheets, time sheets and an ID number. What the consumers actually got was a kit instructing them first to place advertisements identical to the ones they had responded to, and then to read the same script to people who responded to their ads. Instead of $13.50 per hour, the money consumers could earn was based on the number of new victims they recruited.

The FTC charged that the defendants misrepresented to consumers that DP Marketing offers jobs at a specified salary; failed to disclose the material fact that they were offering a pyramid work-at-home scheme; and provided the "means and instrumentalities" to others to commit unlawful and deceptive acts. On September 23, 1999, the court granted the Commission's motion to approve a stipulated preliminary injunction prohibiting the defendants from continuing this scheme.

The Commission has also brought a number of cases against credit repair scams that used spam as an integral aspect of their deception.[14] In a particularly pernicious variation on this scheme, consumers are urged to create a new credit identity in order to fix their credit. Using spam messages such as "BRAND NEW CREDIT FILE IN 30 DAYS," these scammers induce consumers to purchase instructions about how consumers can obtain federally-issued, nine-digit employee identification numbers or taxpayer identification numbers, substitute them for social security numbers, and use them illegally to build new credit profiles that will allow them to get credit they may be denied based on their real credit histories. In fact, using a false identification number to apply for credit is a felony—a point these scammers omit from their solicitations. The Commission, either on its own or through the Department of Justice, filed cases against seven operations that used this type of deceptive spam.[15]

Other types of deceptive schemes that use UCE have also been targets of FTC enforcement action, such as allegedly deceptive business opportunities[16] and decep-

---

[13] No. 399 CV 1272 (CFD) (D. Conn. filed July 7, 1999). Other alleged pyramid schemes that thrived on spam have been targets of FTC enforcement action., *e.g., FTC v. Nia Cano,* No. 97-7947-IH-(AJWx) (C.D. Cal. filed Oct. 29, 1997); Kalvin P. Schmidt, Docket No. C-3 834 (final consent Nov. 16, 1998).

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

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

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

tive weight loss schemes.[17] As these cases illustrate, the Commission's focus has been on deceptive UCE.

C. Comprehensive Consumer and Business Education

The Commission has published three consumer publications related to UCE. *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, nearly 62,000 copies of the brochure have been distributed, and it has been accessed on the FTC's web site nearly 19,000 times.

How to Be Web Ready is a reader's bookmark that offers consumers tips for safe Internet browsing. It provides guidance for consumers on how to safeguard personal information, question unsolicited product or performance claims, exercise caution when giving their email address, guard the security of financial transactions, and protect themselves from programs and files that could destroy their hard drives. A number of corporations and organizations have provided a link from their web site to the tips on the FTC's web site, including Circuit City, Borders Group Inc., Netcom, Micron, and Compaq. More than 52,000 copies of the bookmark have been distributed, and it has been accessed more than 15,000 times on the FTC's web site.

In July 1998, the FTC launched a public education campaign called "*Spam's Dirty Dozen: 12 Scams Most Likely to Arrive Via Bulk Email*" to publicize the most prevalent UCE scams. The list of scams was culled from a sampling of more than 250,000 spam messages that consumers had forwarded to the FTC's mailbox at The consumer alert identified the following twelve types of deceptive solicitations and described how each operate: business opportunities schemes; bulk email programs; chain letters; work-at-home schemes; health and diet scams; effortless income; free goods; investment opportunities; cable descrambler kits; guaranteed loans or credit, on easy terms; credit repair; and vacation prize promotions. Nearly 10,000 copies of this consumer alert have been distributed, and it has been accessed more than 35,000 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, a small percentage of 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 emails), forwarding their UCE to the FTC, or automatically deleting all of their UCE, the Commission is concerned that the proliferation of deceptive UCE poses a threat to consumers' confidence in the Internet as a medium for personal electronic commerce.

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. Tens 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 Procedure 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

[17] *TrendMark International, Inc.*, Docket No. C-3 829 (final consent Oct. 6, 1998)

consumers lost confidence in pay-per-call commerce and stayed away from it in droves. Only now, some six 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 policy. The Commission generally 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.

Mr. TAUZIN. Thank you very much, Ms. Harrington.

The Chair would like to recognize Ms. Heather Wilson who will introduce our next witness from Albuquerque. Heather?

Mrs. WILSON. Thank you, Mr. Chairman.

It is my pleasure to introduce John Brown, who is the head of iHighway.net, who is the founder of—one of the co-founders of that country—company, rather. It is an Internet service provider. He is looking for a country. It is kind of a virtual country. It is an Internet service provider in Albuquerque, New Mexico, that he started in the Bay area in 1996, and then he got smart and came home to Albuquerque. Its goal is to serve rural markets, which we all appreciate in New Mexico. He has seven employees, all in Albuquerque, and they focus on business customers. It is a real pleasure to have John here; and he is, it seems to me, the poster child for the small Internet service provider that can be really severely impacted by spam. Thank you, John.

Mr. TAUZIN. Thank you very much, Heather.

We, of course, could have gotten John Brown to be here in virtual reality. Instead, we have John Brown's body here today. We are pleased to welcome you, Mr. Brown.

STATEMENT OF JOHN M. BROWN

Mr. BROWN. Thank you, Mr. Chairman. If I had a dollar for every time my body was used, I wouldn't necessarily have to be in the ISP business.

I would also like to thank Congresswoman Wilson for inviting me here today and for taking leadership out of our State and producing a bill, H.R. 3113, to help work with this.

As Congresswoman Wilson said, iHighway.net is an Internet service provider located in New Mexico. Sometimes it does seem like another country out there. And we do provide services for local businesses and rural Internet service providers located throughout our State.

I will try to keep my comments brief and just take some highlights out of my testimony.

These are exciting times and times of prosperity, growth, and technical advancement. These advancements are revolutionizing the way humankind interacts and conducts business not only on a local or domestic level but, more importantly, on a global level.

It is important that our local and national leaders carefully craft new laws governing these new times. We want to make sure that we protect those rights that have allowed our country to have a leadership role in this communications revolution. I strongly urge that we make sure that our rights of our citizens, our netizens are protected, that our rights are not eroded also with new laws.

Conversely, it is also important that we must protect our resources from those that misuse them or abuse them. Spam is bad. Let's just be blunt about that. It causes computer networks to crash, e-mail service to fill up, and netizens to pay for the delivery of this unwanted data. We must help to provide tools to allow people and businesses to control and prevent this unwanted data.

You will receive information today from several different groups on how spam is bad as a general issue. I would like to provide the members of this panel with specifics on how spam is bad for my business as a person trying to make a living off their own street.

A real-world data point, if you will. Spam impacts the bottom line of my company is several ways.

No. 1, distraction from productive work. Since our business is one of service, it is vital that we respond to our customers and potential customers quickly. Many of these people choose to communicate with us via e-mail. With this in mind, we must open and read each and every e-mail we receive. Currently, spam represents 8 to 12 percent of the daily new messages we receive in our mailboxes. This is time that could be spent in a more profitable way.

No. 2, use of limited resources. All e-mail coming into our company—and we are going to exclude our customers' mail service at this moment, just our own company—take up transmission time, disk space and other system processing resources. As our company grows and we receive more e-mail from potential customers, those that send spam get to add more people within our company to their mailing list as we add more employees and so forth. Our service must then be upgraded to store more mail, process more incoming mail, et cetera. This vicious cycle grows.

We recently upgraded our internal mail server systems. This has cost our company several thousands of dollars. Being in a rural market, we have to be very careful with the money that we spend on capital improvements.

Speaking from our customers' perspective for a few moments, we process somewhere between 300,000 and 350,000 e-mail messages for a majority of our customers every month. It is very easy to say that 10 percent of those messages are spam. They are messages trying to get a user to go to a pornographic site, sell some snake oil or something.

This takes away from our customers' ability to do their job. Those customers call us, complain to us about this unwanted e-mail, and basically ask us can you please stop it, I don't want to receive this mail again. We have to spend time explaining to the customer that we can attempt but not completely stop this unwanted mail.

The third issue is theft of service. Unsolicited commercial e-mail steals services and time from our company. In July of this year, I did some rough calculations on the cost of UCE or unsolicited commercial e-mail. I estimated that unsolicited commercial e-mail costs us around $1,300 per month in lost time, performance, and additional resources that needed to be purchased, money that could have been used to train additional people in our State or to pay for a part-time student from the local university to work and learn more about Internet technology, money that we will never recover

but we have so spend so that someone else could market their products to our customers.

How do I recoup this cost, that lost business opportunity and that loss of productivity? That is a question that we are all wrestling with and trying to figure out, and I believe that the only way we are going to truly be able to do that is to have particular bills put into law to allow us to have those tools, as I mentioned earlier. Things that we have to worry about is a forging of return addresses and forging of contact information.

If I may key on a couple of last points here. It is important that whatever bill is put forth does not inhibit the freedom to communicate. These are things that have made our country great, allows the recipient to decide if the material is objectionable, provides for penalties and recoveries of cost, requires accurate e-mail headers and prevents forged headers. I believe in an opt-in situation, as opposed to an opt-out. Provides a way for service providers to easily indicate that they do not accept UCE.

And also an important thing from listening earlier to the first panel, we want to make sure that what we do doesn't require an ISP to set up their own legal department to deal with the additional lawsuits and the subpoenas and the record information that we would have to provide for frivolous cases.

I thank you for your time on this matter, Mr. Chairman, Ms. Wilson.

[The prepared statement of John M. Brown follows:]

PREPARED STATEMENT OF JOHN M. BROWN, PRESIDENT, IHIGHWAY.NET, INC.

Thank you Mr. Chairman and members of the Committee. I am very grateful to have been asked to speak to you today on behalf myself and my company. iHighway.net is an Internet Service Provider located in Albuquerque, New Mexico and provides services to local area business and rural Internet Service Providers.

These are exciting times, times of prosperity, growth and technical advancement. These advancements are revolutionizing the way human kind interacts and conducts business. Not only on a local or domestic level but more importantly on a global scale.

It is very important that our local and national leaders carefully craft new laws governing these "new times". We want to make sure that we protect those rights that have allowed our country to have a leadership role in this communications revolution. I strongly urge that we make sure the rights of our citizens, our netizens are protected. That our rights are not eroded away with new laws.

It is equally important that we consider the rapid pace at which technology is changing the way we interact and conduct business. We do not want to be to slow or to fast with new laws. We do not want to be to slow in change. This is a challenge for our government.

As a small business owner it is vitally important that I be able to communicate using the Internet with potential customers and vendors. By using the Internet for business to business commerce, I am ableto act quicker than my competition. I am able to act not only locally, but globally.

Recently we finalized a sale of equipment to the country of Mozambique, Africa. This transaction was completely handled via E-mail and the Internet. This saved on phone costs, time zone changes and the like. Without these tools I would not have been able to transact this business.

Thus, it is the responsibility of government that we do not unduly restrict or slowdown these emerging and new technologies but, that we make sure new laws help promote economic growth for all.

However, we must also protect our resources from those that would miss use them or try to unfairly gain at the expense or cost of another.

Unsolicited Commercial E-mail does just that. It causes computer networks to crash, e-mail servers to fill up and netizens to pay for the delivery of this unwanted data. We must help provide tools to allow people and businesses to control and prevent this unwanted data.

SPAM is bad. There is no other way around it. You will receive information today from several different groups on how SPAM is bad as a general issue. I would like to provide the members with specifics on how SPAM is bad for my business and my customers.

A real world data point if you will.

SPAM impacts the bottom line of my company in several ways.

1. Distraction from productive work: Since our business is one of service, it is vital that we respond to our customers and potential customers quickly. Many of our customers choose to communicate with us via E-mail. With this in mind we must open and read each and every E-mail we receive. Currently SPAM represents around 8 to 12 percent of the daily new messages in our mail boxes. This is time that could be spent in a more profitable way.

2. Use of limited resources: All E-mail coming to our company (excluding our customers at the moment) take up transmission time, disk space and other system processing resources. As our company grows we receive more E-mail from our customers. Those that send SPAM get to add more people within our company to their mailing lists. Our servers must be upgraded to store more mail, process more incoming mail, etc. The vicious cycle grows. We recently upgraded our internal (not customer mail servers) mail server systems. This cost our company several thousands of dollars. Being in a rural market we have to be even more careful with the money we spend on upgrades.

Every month we process somewhere around 300,000 to 350,000 E-mail messages for some of our customers. An easy 10 percent of those messages are SPAM. They are messages trying to get a user to go to a pornographic site, sell some snake oil or something. This takes away from our customers ability to there jobs. Those customers call us and complain about this unwanted E-mail and ask us to "Can you please just stop it. I don't want to receive that mail again". We have to spend time explaining to the customer that we can attempt, but not completely stop the unwanted E-mail.

3. Theft of service: UCE steals services and time from my company. In July of this year I did some rough calculations on the cost of UCE. I estimated that UCE cost us around $1,300 per month in lost time, lost performance, and additional resources that needed to be purchased. Money that could be used to train people in our company or to pay for a part time student from the local university. Money that we will never recover, but yet we spent so that someone else could market their products to our customers.

How do I recoup that cost . . . that loss of business opportunity . . . that loss of productivity????

The forging of return addresses and other information is done by the senders of SPAM to make it more difficult to track them down and recover my losses. By being more difficult SPAMMERS know that I will be less likely to take action.

We have built several systems to help filter or block UCE from known sources. While this has helped it is not something that will scale as the volume of UCE increases. We will have to spend more time and money on equipment if we want to add more filtering equipment to our network. This is neither technically or economically scaleable.

As a small business that is completely dependant on the Internet for our lively hood we strongly urge Congress to work at protecting our netizins from the theft of service and cost shifted forms of advertisements or unwanted E-mail.

Congress should craft a law that allows both people and businesses to actively recover the losses they incur because of SPAM. Several key points of this law should be:

- Does not inhibit the freedom to communicate
- Allows the recipient to decided if material is objectionable
- Provides for penalties and the recovery of costs
- Requires accurate E-mail headers, prevents forged headers, etc
- Requires Opt-In, instead of an Opt-Out solution
- Provides a way for service providers to easily indicate that they do not accept UCE

If we do not work to stop this problem soon, E-mail and other forms of Internet communications may be reduced in there usefulness.There are plenty of references on the Internet that talk in more detail about the issue of SPAM. Below are some links to those locations. I would urge each of you to visit these sites and to read the collection of good information located there.

The Coalition Against Unsolicited Commercial E-mail **http://www.cauce.org**

The Mail Abuse Prevention System http://maps.vix.com

Spam Abuse Site **http://www.abuse.net**

Thank you for your time. I hope that my brief views from running a business that has been negatively impacted by SPAM has been helpful.

Mr. TAUZIN. Thank you very much, Mr. Brown.

Our next witness will be Mr. Alan Charles Raul of Sidley & Austin here in Washington, DC.

STATEMENT OF ALAN CHARLES RAUL

Mr. RAUL. Good morning, Mr. Chairman and members of the committee. My name is Alan Raul. I am a partner of Sidley & Austin in Washington, DC, where I head the CyberLaw practice. I am testifying today in a personal capacity, and thank you for inviting me here.

Nearly 3 years ago, the New York Times reported that, quote, humanity has never before encountered a form of advertising that costs its sender so little. Its targets, in fact, pay more. And anyone with an Internet correction and a list of e-mail addresses can send millions of letters for roughly nothing.

Since then, the proliferation of domestic e-mail intrusions has been a factor contributing even more to one of America's new great concerns, personal privacy. And for those of us who are carrying wireless e-mail the intrusions are not just domestic but in fact much closer to our physical persons.

A Wall Street Journal/NBC poll reported in September 1999 that loss of personal privacy was the first or second concern of 29 percent of respondents. Others issues like terrorism, world war, et cetera, had scores of 23 percent or lower.

Unlike junk postal mail, the costs of unsolicited bulk commercial e-mail, or spam, are borne by ISPs and recipients rather than the senders. There should be aggressive government enforcement of current laws against fraudulent and deceptive advertising and trade practices, and I think Ms. Harrington from the FTC demonstrated that the FTC is in fact active on that beat.

The anti-spam legislation being considered by this committee has important constitutional implications. There is an obvious and compelling need to balance the free speech rights of advertisers with the rights of the rest of us to govern our own space. However, to the extent that a bill clearly identifies the substantial governmental interests involved, such as protecting household privacy, privacy of children, preventing trespasses against personal property, deterring fraud and protecting consumers from bearing the costs of the very advertising that is directed at them, it should be possible to craft a constitutional bill.

The legislative process that you are engaged in right now must develop clear evidence in support of the need to remedy these wrongs and reflect that evidence in the bill's finding and purposes.

In addition, any legislative solution should rely on self-regulatory market-based measures rather than command-and-control government dictates. It is not possible to predict how new technologies and usage patterns will evolve, so rigid directives and bureaucracies should be avoided. The Internet, even e-mail in particular, is largely flourishing today as a result of enlightened governmental oversight and forbearance. So far at least when it comes to governing the Internet, it seems that to err is human and to forbear is divine.

To the maximum extent possible, therefore, Internet users and providers should be free to establish their own policies. Government must play the crucial role of encouraging the development and disclosure of applicable usage policies and then holding entities accountable for compliance with those policies. The current laws against fraudulent, unfair and deceptive practices provide the best framework.

Spam or unsolicited commercial e-mail is an inescapable presence for anyone hooked to the Internet. Along with a few tidbits of interesting purchase opportunities or promotion comes an enormous burden, and it ties up bandwidth for providers and trespasses on their property and intrudes upon the e-mail accounts of account holders. As a result, spammers shift their advertising costs to the conduits and recipients of the advertising instead of bearing it themselves.

With regard to the legislation before the committee, I would support the strong statements of governmental interest that Mrs. Wilson spoke about earlier with regard to her bill in her findings and purposes section. I would encourage the committee to consider the virtues of legislation that provides for maximum flexibility, that encourages the development and posting of private bulk e-mail policies by the ISPs and other providers and looks to market-based solutions and agreements between the e-mail providers and the bulk e-mail senders.

Truthful self-identification of senders is another crucial component, I think, to avoid fraud and deception. The ease of the individual's ability to remove himself or herself from lists they don't want to be on is another important factor and relying on traditional government enforcement such as that of the FTC against unfair and deceptive practices.

I would suggest that the committee should seek to avoid rigid governmental lists, a proliferation of private rights of action and, of course, any content-based restrictions on speech.

Thank you very much, Mr. Chairman.

[The prepared statement of Alan Charles Raul follows:]

PREPARED STATEMENT OF ALAN CHARLES RAUL, PARTNER, SIDLEY & AUSTIN

Mr. Chairman and Members of the Committee, my name is Alan Raul. I am a partner of Sidley & Austin in Washington, D.C., where I head the CyberLaw practice. I am testifying today in a personal capacity.

INTRODUCTION

Nearly three years ago, the New York Times reported that "humanity has never before encountered a form of advertising that costs its senders so little. Its targets, in fact, pay more . . . Anyone with an Internet connection and a list of E-mail addresses can send millions of letters for, roughly, nothing." New York Times, Dec. 22, 1996, sec. 6, at 22.

This proliferation of domestic intrusions runs directly into what Americans are most concerned about looking ahead to the coming century. In a Wall Street Journal/NBC News poll reported in September, 1999, "Loss of personal privacy" was the first or second concern of 29 percent of respondents. All other issues, such a terrorism, world war, and global warming had scores of 23 percent or less. Wall Street Journal, Sept. 16, 1999, at A10.

Unlike junk postal mail, the costs of unsolicited bulk commercial e-mail ("spam") are borne by ISPs and recipients rather than the senders. There should be aggressive government enforcement of current laws against fraudulent and deceptive advertising and trade practices.

The "anti-spam" legislation being considered by this Subcommittee has important constitutional implications. There is an obvious, and compelling, need to balance the free speech rights of advertisers with the rights of the rest of us to govern our own space. However, to the extent that a bill clearly identifies the substantial governmental interests—such as protecting household privacy, preventing trespasses against private property, deterring fraud, and protecting consumers from bearing the cost of the very advertising directed at them—it may be possible to craft a constitutional bill. The legislative process must develop clear evidence in support of the need to remedy these wrongs, and reflect that evidence in the bill's "findings" and "purposes."

In addition, any legislative solution should rely on self-regulatory measures as opposed to intrusive or heavy-handed governmental dictates. It is not possible to predict how new technologies and usage patterns will evolve, so command-and-control directives will not be helpful, and additional regulatory structures or bureaucracies should be avoided. The Internet—and even e-mail—is largely flourishing today as a result of enlightened governmental oversight and forbearance. So far, at least, when it comes to governing the Internet, it is plain that "to err is human, and to forbear is divine."

To the maximum extent possible, therefore, Internet users and providers should be free to establish their own policies. Government must play the crucial role of encouraging the development and disclosure of applicable usage policies, and then holding entities accountable for compliance with those policies. The current laws against fraudulent, unfair and deceptive practices provide the best framework.

THE PROBLEMS WITH "SPAM"

"Spam" or unsolicited commercial e-mail (UCE) is an inescapable and enlarging presence for any person or household hooked up to the Internet. Along with a few tid-bits of interesting purchase opportunities or promotions, comes an enormous burden. Vast quantities of e-mail that is "junk" to just about everybody ties up bandwidth and trespasses on the property of Internet Service Providers (ISPs) and e-mail account holders. As a result, "spammers" shift their advertising costs to the conduits and recipients of the advertising, instead of bearing it themselves. To add injury to this insult, we recipients of spam have our own home and e-mail accounts intruded upon, and our privacy disturbed. The best that can be said about it is that it is a nuisance. According to the Federal Trade Commission, it can be much worse than that: "Email boxes are filling up with more offers for business opportunities than any other kind of unsolicited commercial email. That's a problem . . . because many of these offers are scams. See FTC Consumer Alert!, "FTC Names Its Dirty Dozen: 12 Scams Most Likely to Arrive Via Bulk Email," <www.ftc.gov/bcp/conline/pubs/alerts/doznalrt.htm>.

FIRST AMENDMENT AND "COMMERCIAL SPEECH" ANALYSIS

Because the "Anti-Spam" legislation would curtail the ability of e-mail advertisers to "speak," the constitutionality of any pending legislation must be carefully considered.

"Reasonable Fit" with Substantial Governmental Interest.

In determining whether a statute regulating commercial speech violates the First Amendment of the Constitution, courts apply the test formulated in *Central Hudson Gas & Elec. Corp. v. Public Serv. Comm'n of NY,* 447 U.S. 557 (1980). Such a statute is valid if:

—it is supported by a substantial governmental interest.
—directly advances that governmental interest.
—is not more extensive than necessary to serve that interest.

The final two prongs of this test have since been explained as requiring that there be a "**reasonable** '**fit**' between the legislature's ends and the means chosen to accomplish those ends." *Board of Trustees of State University of N.Y. v. Fox,* 492 U.S. 469, 480 (1989)(emphasis added); *Cincinnati v. Discovery Network Inc.,* 507 U.S. 410, 416 (1993).

The mere existence of some imaginable alternative that might be less burdensome on speech does not mean that the restriction is not narrowly tailored for purposes of First Amendment analysis.

Mailbox Privacy.

The Supreme Court has upheld a federal statute under which a person could require that a mailer remove the person's name from its mailing lists and stop all future mailings to the householder. *See Rowan v. U.S. Post Office Dep't,* 397 U.S. 728,

729- 30 (1970). The statute provided a procedure whereby householders could insulate themselves from "pandering advertisements" directed to them in the mail, "which the addressee in his sole discretion believes to be erotically arousing or sexually provocative." It was Congress' objective to protect the privacy of homes from such material and place the judgment of what constitutes and offensive invasion of these interests in the hands of the addressee.

The Supreme Court concluded that:

—"a sufficient measure of individual autonomy must survive to permit every householder to exercise control over unwanted mail." 397 U.S. at 736.
—"a mailer's right to communicate must stop at the mailbox of an unreceptive addressee." 397 U.S. at 736-37.
—"To hold less would tend to licence a form of trespass." 397 U.S. at 737.
—"We therefore categorically reject the argument that vendor has a right under the Constitution or otherwise to send unwanted material into the home of another." 397 U.S. at 738.

While the *Rowan* decision predated the Supreme Court's decisions in *Central Hudson and Cincinnati v. Discovery Network*, 507 U.S. 410 (1993), the Supreme Court should continue to be receptive to congressional efforts to protect domestic privacy and spare individuals from unwanted communications at home. Moreover, to the extent the homeowner decides what solicitations are offensive, the government is not making content-based distinctions that would more clearly run afoul of the First Amendment.

Protection for Children.

To the extent the pending "anti-spam" legislation seeks to protect the welfare of children, Congress may enjoy additional latitude. The Supreme Court has repeatedly recognized "children deserve special solicitude in the First Amendment balance because they lack the ability to assess and analyze fully the information presented through commercial media." *Anheuser-Busch, Inc. v. Schmoke*, 101 F.3d 325, 329-30 (4th Cir. 1996)(summarizing the additional restriction allowed by the Supreme Court under the Cable Television Consumer Protection and Competition Act, the Public Telecommunications Act, and with respect to pornography). As the Court recognized long ago, "[a] democratic society rests, for its continuance, upon the healthy, well-rounded growth of young people into full maturity as citizens." *Prince v. Massachusetts*, 321 U.S. 158, 168 (1944).

TELEPHONE CONSUMER PROTECTION ACT; A GOOD ANALOGY

In 1991, President Bush signed the Telephone Consumer Protection Act (TCPA), 47 U.S.C § 227. Congress enacted legislation to restrict automated and prerecorded telephone calls as well as unsolicited commercial faxes because it found that "unrestricted telemarketing . . . can be an intrusive invasion of privacy." The TCPA defined "unsolicited advertisement" as "any material advertising the commercial availability of quality of any property, goods, or services which is transmitted to any person without that person's prior express invitation or permission."

The TCPA provides a potential model for the "Anti-Spam" bills pending before this Congress. In the TCPA, Congress was concerned about invasions of privacy and shifting the burden of advertising costs to the consumer. These issues are directly analogous to the concerns over unsolicited commercial e-mail.

Congressional Findings.

In the TCPA, Congress found that:

—"Unrestricted telemarketing . . . can be an intrusive invasion of privacy."
—"Many consumers are outraged over the proliferation of intrusive, nuisance calls to their homes."
—"Evidence compiled by the Congress indicates that residential telephone subscribers consider automated or prerecorded telephone calls . . . to be a nuisance and an invasion of privacy."
—"Individuals' privacy rights . . . and commercial freedoms of speech and trade must be balanced in a way that protects the privacy of individuals and permits legitimate telemarketing practices."

Legislative Prohibitions on Unsolicited Commercial Communications.

The TCPA reined in nuisance telemarketing by, among other things, making it unlawful "to initiate any telephone call to any residential telephone line using an artificial or prerecorded voice to deliver a message without the prior express consent of the called party" and to "use any telephone facsimile machine, computer, or other device to send an unsolicited advertisement to a telephone facsimile machine."

Private Right of Action for Damages and Injunction.

The TCPA granted any person a private right of action to bring suit in state courts to enjoin violations of the Act, and to recover actual monetary losses from such violations or to receive $500 in damages for each violation, whichever is greater. Courts were authorized to award treble damages for willful or knowing violations.

Required Identification.

The TCPA requires fax messages to identify the name and telephone number of the business or other entity sending the message, and the date and time of the transmission.

FCC Rules.

The Federal Communications Commission (FCC) was authorized to prescribe applicable rules and exemptions. The TCPA also authorized the FCC to require the establishment and operation of a single national database of residential telephone subscribers who object to receiving telephone solicitations. The Act did not authorize the FCC to exempt any recorded telephone messages containing any unsolicited commercial advertising.

The FCC has adopted rules implementing the TCPA. See 47 C.F.R. § 64.1200. The FCC has not required the establishment of a national database, but does require telephone solicitors to maintain a "Do Not Call" list of persons who do not wish to receive telephone solicitations, together with a written policy for maintaining such list. "Do Not Call" requests must be honored for 10 years from the time the request is made.

TCPA Has Been Held Constitutional.

The Ninth Circuit has upheld the TCPA's constitutionality in *Destination Ventures, Ltd. v. FCC,* 46 F.3d 54, (9th Cir. 1995), and *Moser v. FCC,* 46 F.3d 970 (9th Cir. 1995), *cert. denied*, 515 U.S. 1161. *See also Kenro, Inc. v. Fax Daily, Inc.*, 962 F. Supp. 1162 (S.D. Indiana 1997).

These decisions found Congress' regulation of commercial speech in the TCPA was justified on grounds of protecting the public from invasions of privacy and preventing the shift of advertising costs to consumers.

—"There was significant evidence before Congress of consumer concerns about telephone solicitation in general and about automated calls in particular.... We conclude that Congress accurately identified automated telemarketing calls as a threat to privacy." 46 F.3d at 974.

—"That some companies prefer the cost and efficiency of automated telemarketing does not prevent Congress from restricting the practice." *Id.* at 975.

—"[U]nsolicited commercial fax solicitations are responsible for the bulk of advertising cost shifting. Thus, banning them is a reasonable means to achieve Congress's goal of reducing cost shifting." 46 F.3d at 56.

The TCPA's jurisdictional provisions, which are largely repeated in H.R. 3113, have been challenged on numerous occasions. To avoid uncertainty, Congress could find that federal legislation regarding "spam" is necessary because Internet operations are inherently interstate. *See, e.g., ErieNet, Inc. v. Velocity Net, Inc.*, 156 F.3d 513, 515 (3rd Cir. 1998); *Nicholson v. Hooters,* 136 F.3d 1287, 1287-88 (11th Cir.1998), modified, 140 F.3d 898 (11th Cir.1998); *Chair King, Inc. v. Houston Cellular Corp.*, 131 F.3d 507, 509 (5th Cir.1997).

Moreover, Congress may wish to address the Tenth Amendment issues inherent in assigning enforcement of a federal cause of action to the State courts. *Cf. International Science & Tech. Inst., Inc. v. Inacom Communications, Inc.*, 106 F.3d 1146 (4th Cir.1997) (holding that the TCPA's provision of exclusive state court jurisdiction did not impermissibly commandeer state courts in violation of Tenth Amendment).

KEY PROVISIONS OF THE "ANTI-SPAM" BILLS

H.R. 2162, the "Can Spam Act," is essentially based on a "property rights" model. Persons are prohibited from using—i.e., trespassing against—the equipment of an electronic service provider in violation of the provider's posted e-mail policies.

The bill would authorize federal and state courts to issue injunctions and award damages for such unauthorized uses of a provider's equipment. Only injured electronic service providers would have private right of action to enforce the bill's civil provisions. The bill's restrictions apply only to "commercial electronic mail," which is defined as e-mails "the principal purpose of which is to promote, directly or indirectly, the sale or other distribution of goods or services to the recipient." Other

than the commercial nature of the message, no other content restriction is implicated by the bill.

The bill would also criminalize the use of another person's Internet domain name in connection with sending e-mail messages. Fraudulent "headers" would thus be banned. This provision is analogous to the TCPA's requirement that telephone solicitations identify the person or entity making the solicitation.

H.R. 3113, the "Unsolicited Electronic Mail Act of 1999," is considerably more complex and "regulatory" in nature. The bill sets forth numerous "findings" that effectively document the substantial governmental interest in regulating unsolicited e-mails, and articulates the fine line that Congress must follow: "In legislating against certain abuses on the Internet, Congress should be very careful to avoid infringing in any way upon constitutionally protected rights, including the rights of assembly, free speech, and privacy."

The bill would require a federal agency (the FCC in the October 20 version of the bill) to maintain a list of individuals who do not wish to receive unsolicited commercial e-mail or unsolicited "pandering" e-mail, or both. No person would be allowed to transmit such unsolicited e-mails to any individual whose name has been on the list for more than 30 days. The federal agency would be empowered to issue an order directing the initiator of unsolicited e-mails to refrain from sending further messages.

These provisions are analogous to the design of the postal statute upheld by the Supreme Court in the *Rowan* decision discussed above. However, H.R. 3113 would depend on the existence of an unwieldy bureaucracy and on potentially problematic exchanges of lists between the federal agency and private parties. Inevitably, H.R. 3113's "pandering" provisions would involve the federal government in making content-based judgments in tension with the First Amendment.

It is worth noting that the FCC has declined to exercise its authority under the TCPA to establish its own "Do Not Call" list.

H.R. 3113 would also prohibit the transmission of unsolicited e-mails unless such messages contain a reply electronic mail address to which the recipient may send a reply indicating a desire not to receive any further messages.

H.R. 3113 authorizes a private right of action by any injured party in state court. The federal agency and injured parties would be authorized to enforce the official cease and desist orders in court.

H.R. 3113 also contains certain provisions based on a "property rights" model. ISPs are authorized to develop usage policies and to decline to transmit unsolicited e-mails to subscribers without compensation from the senders. This principle is sound, but it is not clear why a new federal law would be required to establish the proposition. Reliance on a federal agency to enforce these provisions would be a departure from the current philosophy that looks to self-regulation first for governing Internet activities.

H.R. 1910, the "E-Mail User Protection Act," proscribes a number of activities such as initiating unsolicited e-mails with false sender names, return addresses or headers; failure to comply with the request of recipient not to receive any further unsolicited messages; use or distribution of software designed to create false Internet domain, header, or originating e-mail information, etc.

The bill essentially deems these activities to be unfair or deceptive trade practices, and the FTC is given authority to enforce violations under its existing statutory authority.

Criminal sanctions are provided for intentional misappropriations of the name or e-mail address of another person, of for intentionally transmitting unsolicited e-mail to an individual who has specifically communicated to the violator that individual's desire not to receive such e-mail.

The bill also create a private cause of action for injured ISPs and e-mail recipients.

COMMON LAW "SPAM" LITIGATION

The scale of the spam invasion into the homes of citizens and the servers of ISPs has already generated significant litigation opportunities as ISPs attempt to adapt the common law to their current security and privacy needs.

America On Line has led the pack in this regard, aggressively pursing spammers under a variety of legal theories. *See*, e.g., *America Online v. Greatdeals*, No. 99-62-A (E.D. Va. 1999). Although the business practices of spammers have on numerous occasions subjected them to fraud, deceptive trade practice, or intellectual property-rights liability, suits against legitimate but unsolicited materials have relied upon traditional theories of trespass and trespass to chattels.

In *Cyber Promotions, Inc. v. American Online,* 948 F. Supp. 436 (E.D. PA 1996)(receiving a transfer of, and consolidating, AOL's E.D. Virginia complaint against Cyber Promotions as counterclaims in the E.D. PA action), an ISP was sued for interfering with the delivery of spam e-mails. The court granted AOL's motion for summary judgment holding that bulk transmissions of commercial e-mail are not constitutionally protected activity. The court rejected the argument that AOL's e-mail service constituted a "public function" or "state action" of any kind.

Mr. TAUZIN. Thank you very much, Mr. Raul.

Next will be Mr. Michael Russina, Senior Director of Systems Operations at SBC Communications in San Antonio, Texas.

Mr. Green, would you do the honors of introducing our guest?

Mr. GREEN. Thank you, Mr. Chairman.

I would like to thank Michael Russina from SBC on very short notice for being able to be here when our other witness from Texas couldn't be.

Mr. Russina is the Senior Director of Systems Operations at SBC where he originated SBC's Internet service company and helped establish the necessary infrastructure to provide SBC customers with Internet access, e-mail, and personal web pages. Before that, he was with Microsoft as an systems engineer. He is a graduate of Southwest Missouri State, and I will provide the committee with his bio. But, Mr. Chairman, he came back to Texas as quick as he could from both Microsoft and Southwestern Missouri.

Mr. TAUZIN. I just wanted to welcome you, and I wanted everyone to know that you came on very short notice, and we deeply appreciate your attending the committee hearing today.

STATEMENT OF MICHAEL RUSSINA

Mr. RUSSINA. Thank you.

Mr. Chairman and members the committee, my name is Michael Russina. I am Director of Systems Operations of SBC Internet Services. SBC Internet Services is a subsidiary of SBC Communications. SBC Internet Services is a leading provider of Internet service in 13 States.

My function within SBC Internet is to build and maintain value-added services that the SBC Internet companies offer for our customers. For example, USENET, e-mail, authentication and personal web service are under my supervision. This represents roughly 200 separate distributed systems.

I would like to thank you for this opportunity to present SBC Internet's comments on the activity commonly referred to as spamming or the sending of unsolicited bulk commercial electronic mail.

SBC Internet Services supports State and Federal efforts to reduce or stop spamming. The transport and delivery of bulk electronic mail saddles Internet service providers such as SBC Internet with significant expense. There is also a goodwill cost to ISPs as reflected in customer complaints about receipt of spam.

It is relatively cheap and easy for a telemarketer to send bulk e-mail. All a telemarketer needs is a dial-up connection and a PC. The burden and cost of spamming falls on the ISP and the end user. It is a substantial burden for an ISP to process and store the vast amount of data generated by bulk mail messages. Spamming contributes to many of the access, speed and reliability problems of

ISPs. Indeed, many large ISPs have suffered major system outages as the result of massive junk e-mail campaigns.

Today, roughly 35 percent of all the e-mail transmitted over SBC Internet systems in our Pacific Bell and Southwestern Bell regions is bulk e-mail, and the amount of such traffic is consistently increasing.

SBC Internet has just completed a $1.96 million upgrade on its e-mail infrastructure in each of the regions in order to handle anticipated electronic messaging traffic to and from its subscribers over the next few years. If the volume of unsolicited commercial e-mail is not substantially reduced, we anticipate it may be necessary to accelerate additional infrastructure enhancements at the cost of $686,000 per region—35 percent of $1.96 million is how we derive that—or $1.37 million per year total hardware cost to SBC Internet over those two regions.

Not reflected in the above costs is the additional costs in man hours occasioned by spamming. Our network personnel must continually monitor our system for problems when a spam attack occurs or our systems go from a normal to a busy state, and our personnel must immediately react to determine if there is a system problem or just a spam attack. Once it is verified that it is a spam attack, they must work to ensure that the large volume of messages does not bring the system down.

In California and Texas, SBC Internet operates under a zero tolerance policy for unsolicited bulk e-mail or spam. Therefore, if our network personnel determine that it is a spam attack, then the company must expend man hours to track the source and stop the spam.

Furthermore, many man hours are also expended on responding to customer e-mail and telephone complaints about receipt of spam. Our policy department handlings around 1,000 messages a day. Of those that turn out to be actionable complaints, over 80 percent relate to an unsolicited bulk e-mail, whether the complaints are from our own customers complaining about receiving it or from outside receivers complaining about our customers sending it. The policy department devotes most of its time, therefore, to this problem. The cost is measured not only in dollars for the labor expended to handle these complaints but also in the loss of goodwill with our customers, an immeasurable expense.

Fraud and spam only detract from the Internet user's experience with e-mail, and as a company which seeks to be a high-tech leader we want to make sure our customers always feel comfortable using e-mail to communicate. Unless the growth of unsolicited commercial e-mail is stopped, it could eventually destroy the usefulness and effectiveness of e-mail as a communication tool.

SBC Internet supports legislative efforts that will help put an end to e-mail abuse. To the extent that Congressman Miller's bill, H.R. 2162, will lessen the flow of spamming by prohibiting telemarketers from sending unsolicited commercial e-mail over the system of an ISP in violation of that ISP's policy, SBC Communication supports the legislation.

We also support the efforts of Congressman Green in his legislation, H.R. 1910, to end the fraudulent practices of many telemarketers which are an enormous source of the spam problem.

False addresses and domains can cause mass system overloads and can damage the reputation of individuals and ISPs that are falsely portrayed as the spammer.

Thank you again for letting me testify today. I hope we can work together to find a solution to this growing problem.

[The prepared statement of Michael Russina follows:]

PREPARED STATEMENT OF MICHAEL RUSSINA, DIRECTOR, SYSTEMS OPERATIONS, SBC INTERNET SERVICES

Mr. Chairman and Members of the Committee. My name is Michael Russina. I am Director of Systems Operations at SBC Internet Services.

SBC Internet Services is a subsidiary of SBC Communications, Inc. SBC Internet Services is a leading provider of Internet access in 13 states under the brand names of Pacific Bell Internet operating in California, Nevada Bell Internet, Southwestern Bell Internet operating in Texas, Missouri, Kansas, Arkansas, and Oklahoma, and SNET Internet in Connecticut. We have recently acquired Ameritech and its subsidiary ISP—Ameritech Interactive Media Services, which was rated by PC World Magazine as the best regional ISP in the Nation. SBC Communications has committed itself to providing high-speed Digital Subscriber Line (DSL) technology to more than 80 percent of its customers by the end of 2002. Under this broadband initiative, SBC's local network will be transformed into a next-generation, packet-switched advanced broadband network.

My function within SBC Internet is to build and maintain the value-added services that the SBC Internet Companies offer for our customers. For example, USENET, e-mail, authentication, and personal web servers are all under my supervision. This represents roughly 200 separate, distributed systems.

I would like to thank you for this opportunity to present SBC Internet's comments on the activity commonly referred to as "spamming" or the sending of unsolicited bulk commercial electronic mail.

SBC Internet Services supports state and federal efforts to reduce or stop spamming. The transport and delivery of bulk electronic mail saddles Internet service providers (ISPs), such as SBC Internet, with significant expense. There is also a "goodwill" cost to ISPs as reflected in customer complaints about receipt of spam.

It is relatively cheap and easy for a telemarketer to send bulk e-mail. All a telemarketer needs is a dial-up connection and a PC. The burden and cost of spamming falls on the ISP and the end user. It is a substantial burden for an ISP to process and store the vast amount of data generated by bulk mail messages. Spamming contributes to many of the access, speed, and reliability problems of ISPs. Indeed, many large ISPs have suffered major system outages as the result of massive junk e-mail campaigns.

Today, roughly 35 percent of the all e-mail transmitted over SBC Internet's systems in our Pacific Bell and Southwestern Bell regions is bulk e-mail. And the amount of such traffic is constantly increasing. SBC Internet has just completed a $1.96 million upgrade of its e-mail infrastructure in each of these regions in order to handle anticipated electronic messaging traffic to and from its subscribers over the next few years. If the volume of unsolicited commercial e-mail is not substantially reduced, we estimate that it may be necessary to accelerate additional infrastructure enhancements at the cost of $686,000 per region (35 percent of $1.96 million) or $1,372,000 per year total hardware cost to SBC Internet for those two regions.

Not reflected in the above cost is the additional costs in man hours occasioned by spamming. Our network personnel must continually monitor our systems for problems. When a spam attack occurs our systems go from a normal state to a busy state, and our personnel must immediately react to determine if there is a system problem or just a spam attack. Once it is verified as a spam attack, they must work to ensure that the large volume of messages does not bring the system down.

In California and Texas, SBC Internet operates under a zero tolerance policy for unsolicited bulk e-mail or spam. Therefore if our network personnel determine it is a spam attack, than the company must expend man-hours to track its source and stop the spam.

Furthermore, many man-hours are also expended on responding to customer e-mail and telephone complaints about receipt of spam. Our policy department handles around 1000 messages a day. Of those that turn out to be actionable complaints, over 80% relate to unsolicited bulk e-mail (whether the complaints are from our own customers complaining about receiving it, or from outside users complaining about our customers sending it). The policy department devotes most of its

time, therefore, to this problem. The cost here is measured not only in dollars for the labor expended to handle these complaints, but also in loss of goodwill with our customers—an unmeasurable expense.

Fraud and/or spam only detract from the Internet user's experience with e-mail, and as a company which seeks to be a high-tech leader, we want to make sure our customers always feel comfortable using e-mail to communicate. Unless the growth of unsolicited commercial e-mail is stopped, it could eventually destroy the usefulness and effectiveness of e-mail as a communication tool.

SBC Internet supports legislative efforts that will help put an end to e-mail abuse. To the extent that Congressman Miller's bill, H.R. 2162, will lessen the flow of spamming by prohibiting telemarketers from sending unsolicited commercial e-mail over the system of an ISP in violation of that ISP's policies, SBC Communications supports the legislation.

We also support the efforts of Congressman Green, in his legislation, H.R. 1910, to end the fraudulent practices of many telemarketers—an enormous source of the spam problem. False addresses and domains can cause mass system overloads and can damage the reputation of individuals and ISPs that are falsely portrayed as the spammer.

Thank you again for letting me testify today. I hope we can work together to find a solution to this growing problem.

Mr. TAUZIN. Thank you very much, Mr. Russina.

Next will be Mr. Charles Kennedy, Morrison & Forester here in Washington, DC.

STATEMENT OF CHARLES H. KENNEDY

Mr. KENNEDY. Thank you, Mr. Chairman.

I teach Internet law and computer law at the Catholic University of America here in the District, and I understand that is why I am here today, to talk about law.

When I teach spam, by the way, to my students——

Mr. TAUZIN. Is that Catholic law or regular law?

Mr. KENNEDY. I am not qualified to teach Catholic law. It is the regular stuff.

When I teach spam, by the way, I always teach the Monty Python sketch that was discussed in the first panel. That sketch, to complete the record, is set in a seaside resort in the north of England. Everything on the menu has Spam in it. So the waitress, who is one of the Monty Python guys in a dress, not a pretty sight, recites the menu and says Spam over and over and over. And at some point a Viking longboat beaches itself outside. A bunch of Vikings come in, and they start chanting "Spam", pounding on the table until there is a crescendo of the word "Spam." a comparison with unsolicited commercial e-mail should be obvious.

Mr. TAUZIN. Are you going to suggest this as a way to mete out an appropriate punishment for the spammers?

Mr. KENNEDY. Whatever the Vikings did.

I will turn my attention, Mr. Chairman, to the pending bills.

My written testimony, which I will not repeat, is in two sections.

First, the restrictions on commercial e-mail. As the subcommittee probably knows, restrictions on commercial speech are subject to a more lenient standard of review. I see no reason why an anti-spam statute directed to commercial e-mail should not survive judicial review under the first amendment. I put a few pointers in my testimony as to how that might more successfully be accomplished.

I would draw the subcommittee's attention more particularly, though, to those provisions in the pending bills that appear to reach noncommercial e-mail. H.R. 3113, as Mrs. Wilson said, has a restriction on pandering e-mail, and it appears to make the defi-

nition of pandering within the discretion of the recipient, and it appears, as presently drafted, to cause the initiator of the e-mail to decide at his or her peril as to whether the recipient will regard it as pandering. Now that section is based on a postal statute that was upheld by a Supreme Court decision in 1970; and, as my written testimony suggests, with little tweaking it should be just fine.

H.R. 3024 talks about both commercial and noncommercial e-mail and requires both to have accurate address elements. Now if a commercial spammer uses an incorrect address element it is usually for purposes of evading anti-spam filtering by an ISP, and it might also be a trademark violation or an unfair trade practice within the jurisdiction of the FTC.

But individuals often conceal their identity to avoid embarrassment or retribution, and there is in constitutional law a right to speak anonymously, so I would have some concern about extending that prohibition to noncommercial speech.

In general, Mr. Chairman, I think that restriction of these bills to commercial unsolicited e-mail would achieve predominantly the purpose of this legislation and would not cause to you get involved in a higher standard of scrutiny if the statute is challenged on first amendment grounds.

In conclusion, as an Internet user, I welcome what the subcommittee is doing, and I hope your efforts do result in legislation in this Congress. Thank you.

[The prepared statement of Charles H. Kennedy follows:]

PREPARED STATEMENT OF CHARLES H. KENNEDY, MORRISON & FORESTER LLP

I appreciate the Committee's invitation to offer my views on legislative solutions to the problem of unsolicited commercial email ("UCE"). The purpose of my testimony is to describe briefly the constitutional framework within which the courts will entertain challenges to such legislation. With that framework in mind, it should be possible to draft a statute that will withstand judicial review and accomplish the Congress's purpose of regulating practices that deceive, annoy and burden Internet users and service providers.

My views on this subject were developed in the course of teaching Computer Law and New Technologies and the Law at The Catholic University of America. I also am Of Counsel to Morrison & Foerster LLP, but the opinions expressed in this testimony are mine and not necessarily those of any client of Morrison & Foerster.

As I explain in more detail below, any statute that limits UCE will have stronger prospects upon judicial review if it is confined to *commercial* bulk, unsolicited email and is supported by specific legislative findings that articulate a substantial governmental interest and demonstrate the Congress's careful consideration of both the costs and benefits of the statute's restrictions on speech. In this connection, the most plausible basis for anti-UCE legislation is avoidance of cost-shifting, followed by preservation of the societal benefits of the Internet and protection of Internet users' privacy. As I also point out below, anti-UCE statutes that specify forbidden content, regulate non-commercial email or prohibit concealment of the identity of senders of non-commercial messages will invite closer scrutiny by reviewing courts.

I. THE PENDING BILLS AS REGULATIONS OF COMMERCIAL SPEECH

From a constitutional point of view, the most important fact about H.R. 3113, H.R. 2162 and H.R. 1910 is that they apply primarily to *commercial* email. (I leave aside, for the moment, H.R. 3024 and the restrictions proposed by H.R. 3113 for pandering email, which I address separately below.) Because of this limitation, any claim that a statute based upon one of these bills violates the First Amendment will be assessed under the law of commercial speech. The Supreme Court has made it clear that restrictions on commercial speech will be upheld more readily—that is,

will be scrutinized somewhat more leniently—than content-based restrictions on lawful, non-commercial speech.[1]

Specifically, any court that hears a First Amendment challenge to an anti-UCE statute will ask four questions. First, does the statute regulate lawful, non-misleading speech? Second, has the Government asserted a substantial interest that the legislation is intended to serve? Third, does the statute directly advance the Government's asserted interest? And fourth, are the statute's restrictions no more extensive than necessary to serve the Government's asserted interest?[2]

Although this standard is less exacting than the "strict scrutiny" standard that the Supreme Court applies to most restrictions on the content of lawful non-commercial speech, the commercial speech, standard is much less than a free pass for legislators, as numerous decisions rejecting restrictions on commercial speech show.[3] Accordingly, any anti-UCE statute should be drafted with each of the four elements of the commercial speech standard clearly in mind.[4] I'd like to address each of those elements in turn and apply those elements specifically to the provisions of H.R. 3113, H.R. 2162 and H.R. 1910.

A. Does The Statute Regulate Lawful, Nonmisleading Speech?

So long as the commercial speech that an anti-UCE statute addresses involves lawful activity and is not deceptive, that speech is protected under the First Amendment and the statute must meet all four elements of the commercial speech test. Accordingly, the first step in assessing the pending bills is to determine whether, and to what extent, they regulate lawful and nonmisleading speech.

H.R. 3113, 2162 and 1910 all contain some provisions that are fairly read as regulating lawful, non-misleading speech. Specifically, each bill limits the ability of advertisers to send unsolicited, commercial email regardless of whether the content of those messages is unlawful or deceptive. Because they will sweep lawful, truthful speech within their restrictions, these provisions of the three bills must satisfy all four elements of the commercial speech test.

Two of the bills also prohibit practices that mislead the recipients of email messages as to the origin of those messages. Specifically, H.R. 2162 prohibits the unauthorized use of the domain name of another in connection with an email message where such misuse causes harm to a computer, computer system or network; and H.R. 1910 makes it unlawful to send UCE that contains a false, fictitious or misappropriated sender name, return address, or contact person name and telephone number. To the extent the practices prohibited in these sections of H.R. 2162 and 1910 are misleading and potentially fraudulent, they appear not to be protected as commercial speech under the First Amendment. Accordingly, a reviewing court should uphold these provisions without reviewing them under the last three elements of the commercial speech standard.

B. Does The Statute Assert A Substantial Governmental Interest?

In order to pass constitutional muster, an anti-UCE statute should articulate a substantial, plausible governmental interest that the restrictions contained in the statute are designed to promote. Although a reviewing court will give some deference to the Congress's judgment that an asserted interest is substantial, drafters of commercial speech legislation should be prepared for close judicial scrutiny on this point and should articulate significant interests that can be backed up by factual support if the statute is challenged.[5]

Opponents of unsolicited commercial email have identified a number of adverse effects from UCE that might be proper objects of congressional concern. The broadest of these effects is the possible, overall harm that UCE can cause to the societal

---

[1] *See Central Hudson Gas & Electric Corp. v. Public Service Commission of New York,* 447 U.S. 557 564 (1980) ("Central Hudson:).

[2] *Central Hudson, supra,* 447 U.S. at 566.

[3] *See 44 Liquormart, Inc. v. Rhode Island,* 517 U.S. 484 (1996); *City of Cincinnati v. Discovery Network, Inc.,* 507 U.S. 410 (1993); *Linmark Associates, Inc. v. Citizens' Consumer Council, Inc.* 431 U.S. 85 (1977); *Virginia State Board of Pharmacy v. Virginia Citizens' Consumer Council, Inc.,* 425 U.S. 748 (1976).

[4] Some have suggested that Internet regulation should be subject to a separate, media-specific level of scrutiny such as the one the courts have acknowledged for the broadcast medium. No court has adopted this suggestion, however, and we should assume that the usual standard of review for restrictions on commercial speech will apply.

[5] In *Posadas de Puerto Rico Associates v. Tourism Company of Puerto Rico,* 521 U.S. 844 (1997) ("Posadas"), Chief Justice Rehnquist's opinion for the majority stated that the courts should defer to the governmental body's reasons for finding that its asserted interest is substantial. 478 U.S. 328 (1986). In a later decision, however, the Court stated that the Government must justify a restriction on commercial speech by demonstrating that "the harms it recites are real." *Edenfield v. Fane,* 507 U.S. 761 (1993).

value of the Internet. As courts have recognized, the Internet is a uniquely open and democratic forum that offers unprecedented opportunities for communication by persons who do not happen to own newspapers, magazines, cable companies or broadcast stations.[6] Central to the value of the Internet are the low cost and convenience with which access to, and communication by means of, this medium can be achieved. Anything that raises the cost or difficulty of using the Internet without a corresponding social benefit is, arguably, an impediment to the widest public enjoyment of this medium.

Although no court has had occasion to review this rationale as a basis for regulation of UCE, a U.S. district court in Ohio has accepted the claim that UCE reduces the value of Internet services for users and access providers. In *Cyber Promotions, Inc. v. CompuServe,* the court found that bombardment by UCE burdened CompuServe's equipment and caused so much inconvenience and annoyance to CompuServe's subscribers as to reduce the value of CompuServe's entire network.[7] Multiplied by the number of access providers and subscribers throughout cyberspace, this observation applies with equal force to the Internet generally.

A second, plausible concern is that UCE unfairly shifts the cost of mass advertising to Internet access providers and their customers, rather than the commercial enterprises that cause those costs. Avoidance of such cost-shifting was upheld on judicial review when asserted as the basis for the so-called Junk Fax Act, in which the Congress found that the sending of unsolicited, commercial fax messages unfairly shifted the sender's advertising costs to unwilling recipients.[8] In upholding the Junk Fax Act against a First Amendment challenge, the Ninth Circuit Court of Appeals endorsed prevention of such cost shifting as a substantial governmental interest in commercial speech cases.[9]

A third, plausible concern is protection of the privacy of Internet users. Although claims of this kind have some support in the case law, it is not certain that this asserted interest will support restrictions on UCE. The Supreme Court has rejected the privacy rationale as the basis for restrictions on contraception advertisements and utility company bill inserts, on the ground that recipients of such mail can "avoid further bombardment of their sensibilities simply by averting their eyes."[10] The Court has accepted assertions of the interest in residential privacy, however, as a basis for upholding Post Office regulation of junk mail;[11] and the Ninth Circuit Court of Appeals expressly sustained the State of California's assertion of a residential privacy interest in regulating telemarketing practices.[12] Against this somewhat contradictory background, the privacy interest certainly is worth asserting as a basis for restrictions on UCE, but only in combination with stronger claims such as prevention of cost shifting.

The Findings/Policy provisions of H.R. 3113 include clear statements of all three of the interests I have described. Specifically, the second finding emphasizes the interest in assisting "global commerce on the Internet to reach its full potential" by regulating activities that "prevent other users and Internet service providers from having a reasonably predictable, efficient, and economical online experience." The fourth and fifth findings of H. R. 3113, and the second policy determination recited in that bill, emphasize the substantial interest in preventing unfair cost shifting to Internet users and service providers. Finally, the ninth finding and third policy determination of H.R. 3113 articulate the concern that bulk email, which recipients are unable to avoid receiving through reasonable means, may "invade the privacy of recipients."

By contrast, H.R. 2126 and H.R. 1910 do not appear to include detailed findings and policy determinations. In order to increase the likelihood that the second prong of the commercial speech test is met upon judicial review, any UCE statute should contain such findings and determinations.[13] The provisions of H.R. 3113 are an appropriate model for that language.

---

[6] *American Civil Liberties Union v. Reno,* 521 U.S. 844 (1997).
[7] *CompuServe, Inc. v. Cyber Promotions, Inc.,* 962 F. Supp. 1015 (S.D. Ohio 1997).
[8] 47 U.S.C. § 227.
[9] *Destination Ventures, Ltd. v. FCC,* 46 F.3d 54 (9th Cir. 1995).
[10] *Bolger v. Young Drug Products Corp.,* 463 U.S. 60, 72 (1983); *Consolidated Edison Co. v. Public Service Commission,* 447 U.S. 530 (1980).
[11] *Rowan v. Post Office Department,* 397 U.S. 728 (1970); *see also Frisby v. Schultz,* 487 U.S. 474 (1988) (upholding restrictions on residential picketing based on interest in residential privacy).
[12] *Bland v. Fessler,* 88 F.3d 729 (9th Cir. 1995).
[13] This also appears to be true of H.R. 3024, which is discussed further below.

C. Does The Statute Directly Advance The Government's Asserted Interest?

There is some uncertainty as to the strength of the link the Government must demonstrate between the asserted governmental interest and a challenged statute's tendency to advance that interest. In *Posadas,* the Supreme Court found that a legislature's mere belief that the regulation would serve to advance the asserted interest would satisfy this prong of the commercial speech standard.[14] In a subsequent decision, however, the Court appeared to retreat from *Posadas,* announcing that a challenged regulation must advance the asserted interest in a direct and material way.[15] According to that later decision, "this burden is not satisfied by mere speculation or conjecture; rather, a governmental body seeking to sustain a restriction on commercial speech must demonstrate that the harms it recites are real and that its restriction will in fact alleviate them to a material degree."[16] In drafting a statute regulating UCE, it is prudent to assume that the more stringent formulation of the third prong will be applied.

In applying this third prong of the commercial speech test, the Supreme Court has rejected regulations that achieve only a "paltry" reduction in the problem at which the regulations are aimed. Notably, in *City of Cincinnati v. Discovery Networks,* the Court found that the city's goal of reducing blight and making sidewalks safer was only trivially advanced by a ban that reached the small number of commercial newsracks and left the much larger number of non-commercial newsracks operating.[17] However, satisfaction of the third prong does not require that a statute provide a comprehensive or definitive solution to the problem it addresses. Notably, the Ninth Circuit Court of Appeals, in Destination Ventures, found that a ban on unsolicited commercial faxes reasonably advanced Congress's goal of reducing advertising cost-shifting, in spite of the fact that the statute did not reach all forms of such cost-shifting.[18] As the Court of Appeals pointed out in that case, "[t]he First Amendment does not require Congress to forego addressing the problem at all unless it completely eliminates cost shifting."[19]

H.R. 3113, 2162 and 1910 all advance the asserted interests in Internet protection, avoidance of cost shifting and protection of privacy; but the probable effectiveness of each of the bills is not equivalent. Notably, H.R. 3113 and H.R. 1910 both require UCE transmitters to honor opt-out requests. H.R. 3113, however, by giving end users a global opt-out mechanism that does not have to be exercised separately against individual UCE providers, may advance the asserted interests in privacy and cost shifting more effectively. Similarly, H.R. 2162, which does not provide an opt-out mechanism for end users but only prohibits transmission of UCE in violation of an Internet service provider's posted policy, is potentially less effective than either of the other two statutes. All three statutes, however, will have more than a "paltry" effect on the asserted problem and are likely to satisfy the third prong of the commercial speech test.

D. Are The Statute's Restrictions No More Extensive Than Necessary?

In *Board of Trustees of the State University of New York v. Fox,* the Supreme Court found that a legislature seeking to regulate commercial speech is not required to choose the least restrictive means of protecting the articulated governmental interest. It is sufficient if the regulation is "a not necessarily perfect, but reasonable" fit between the asserted interest and the means chosen to advance that interest.[20]

In assessing whether such a "reasonable fit" has been achieved, a reviewing court will consider whether the legislature has carefully calculated "the costs and benefits associated with the burden on speech imposed by its prohibition."[21] Although the outcome of a reviewing court application of the fourth prong cannot be predicted with confidence, H.R. 3113, 2162 and 1910 all reflect consideration of the costs and benefits associated with their prohibitions. Notably, all three bills seek to regulate UCE through measures that stop short of outright bans on all unsolicited, commercial email messages and leave some scope for email-based advertising of a kind that does not reach unwilling recipients. As such, the restrictions in these bills are no more stringent than needed to prevent transmission of email that violates recipi-

---

[14] 478 U.S. 328 (1986).

[15] *Edenfield v. Fane,* 507 U.S. 761 (1993); *see also United States v. Edge Broadcasting Co.,* 509 U.S. 418 (1993).

[16] *Edenfield v. Fane, supra,* 507 U.S. at 770-771. In *United States v. Edge Broadcasting,* however, the Court appeared to soften this requirement somewhat, causing still more confusion as to the stringency of the third element of the test.

[17] 507 U.S. 410 (1993).

[18] 46 F.3d 54 (1995).

[19] *Id.* at 56.

[20] 492 U.S. 469 (1989).

[21] *City of Cincinnati v. Discovery Networks, supra,* 507 U.S. at 417.

ents' preferences or the policies of Internet service providers. The Government could plausibly argue, on judicial review, that lesser restrictions would fail to prevent the harm to the health of the Internet, the assaults on privacy and the pervasive cost-shifting that UCE causes.

For a reviewing court, the best evidence that the Congress has given full consideration to the costs and benefits of a restriction on UCE will be a clear set of legislative findings that articulate these costs and benefits and account for the balance the statute strikes between them. The findings set out in H.R. 3113 are a useful model for this purpose.

II. PROPOSED REGULATION OF NON-COMMERCIAL ELECTRONIC MAIL MESSAGES

Of the four bills on which I have been asked to testify, two of the bills—H.R. 3113 and H.R. 3024—include provisions that go beyond regulation of commercial speech. Specifically, H.R. 3113 limits the transmission of "pandering" email—a category not confined to commercial messages; and H.R. 3024 includes restrictions on both commercial and non-commercial messages. By extending their reach to non-commercial email transmissions, these bills may invite harsher scrutiny by reviewing courts than restrictions on commercial email will receive. Specifically, if these restrictions are found to be content-based, they will be reviewed under the rigorous "strict scrutiny standard"—an analysis significantly more exacting than the commercial speech test.[22] Accordingly, the Committee should consider whether a statute that regulates only commercial email would serve the legislative purpose with less risk of an adverse decision by a reviewing court.

A. Restrictions on Non-Commercial "Pandering" Speech in H.R. 3113

H.R. 3113 includes a prohibition, apparently based upon a Postal Service regulation upheld in a 1970 decision of the Supreme Court,[23] that prohibits the transmission of unsolicited, pandering electronic mail to any person whose name appears on a list maintained by the Federal Communications Commission ("FCC"); or the transmission of any pandering email unless that message contains an email address to which a recipient may send a reply asking not to receive further messages. The bill's definition of "unsolicited pandering electronic mail message" is not confined to commercial messages but includes any email message "which the recipient, in his or her sole discretion, believes to be arousing or sexually provocative that is sent to a recipient with whom the initiator does not have an existing consensual relationship or has been sent by the initiator without the express consent of the recipient."

Although I have not considered the implications of this provision in depth, it appears to raise troubling constitutional questions. First, the provision's reference to "pandering" communications makes it a content-based restriction subject to strict scrutiny. Second, the provision apparently is violated when a person initiates the transmission of a pandering message to anyone whose name appears on an FCC list of persons who do not wish to receive such messages. That list, however, does not identify specific initiators from whom the listed persons do not wish to receive transmissions. In other words, the provision places on each potential initiator the burden of determining whether the listed addressee will find the transmission erotically arousing or sexually provocative. Such a restriction may violate the protections of both the First and Fifth Amendments, because it may chill lawful speech and fail to give persons adequate notice of the conduct that will result in liability.

This provision of H.R. 3113 also appears to differ from the Post Office statute on which it is based. The Post Office statute established a procedure by which persons could indicate their desire not to receive further mailings from particular, identified senders. Accordingly, a potential mailer consulting the Post Office list was not required to determine, at his peril, whether the mailing he intended to send to a listed person would be regarded by the addressee as a "pandering" message within the statute. Instead, the potential mailer had an unambiguous duty not to send any further materials to that person.

It is entirely possible that H.R. 3113 is intended to work in the same way as the Post Office statute on which it is based. Specifically, the drafter may intend to impose liability only upon initiators who have received specific notice from the FCC, after receipt of a complaint from a recipient, to send no further pandering emails to the complainant. The bill mandates such a procedure, and imposition of liability on that basis would appear to be constitutional under *Rowan v. Post Office Department*. It is not clear to this reader, however, that the statute does not create liability

---

[22] *See Turner Broadcasting System, Inc. v. FCC*, 512 U.S. 622, 642 (1994). If the restrictions are not content-based, they will be reviewed under the less exacting or intermediate scrutiny", standard. Id.

[23] *Rowan v. Post Office Department, supra.*

for the simple act of sending a first, pandering email to a person who has not obtained an FCC order.

In any event, it is likely that most unsolicited email of an erotic nature advertises pornographic materials and therefore can be classified as commercial. Accordingly, H.R. 3113 may prove more robust on judicial review, and still will substantially address the problem of unsolicited erotic email, if the references to pandering messages are removed.

B. Restrictions on Non-commercial Speech in H.R. 3024

H.R. 3024, like the provisions of H.R. 3113 just discussed, extends its reach to both commercial and non-commercial email. That bill also requires any initiator of unsolicited, bulk electronic mail messages to provide an accurate electronic return address and a method by which the recipient can request not to receive further messages.

H.R. 3024 raises an issue that is presented, to some extent, by all anti-UCE legislation that requires covered communications to contain accurate return addresses. To the extent an emailer misappropriates the domain name of another, uses false header information to avoid compliance with Internet service providers' anti-UCE policies, or conceals his or her identify for similarly deceptive purposes, that conduct may readily be found to be outside the protection of the First Amendment. In many cases of non-commercial email, however—and even in some cases of commercial email-the transmitter may use return address information that does not violate trademark, constitute an unfair trade practice or have as its purpose the evasion of an anti-UCE policy, but that conceals the identity of the sender simply to avoid retaliation or embarrassment. Drafters of anti-UCE legislation should consider whether these restrictions infringe upon the First Amendment right of anonymous communication, and whether those restrictions will survive review under the strict scrutiny, intermediate scrutiny or commercial speech standard of review, as appropriate.[24]

In general, it would seem advisable to draft anti-UCE statutes to reach only commercial, mass, unsolicited email, so that prohibitions on the use of false header information are more likely to impinge upon abusive, rather than constitutionally permitted, concealments of the sender's identity.

Mr. TAUZIN. Thank you very much, Mr. Kennedy.

Next will be Mr. Jerry Cerasale, Senior Vice President, Direct Marketing Association. Jerry?

STATEMENT OF JERRY CERASALE

Mr. CERASALE. Thank you very much for putting up with me again, and I appreciate the opportunity to be here.

The Direct Marketing Association is very concerned about unsolicited commercial e-mail. Basically, marketing depends upon trust; and, right now, unsolicited commercial e-mail does not have the consumer trust; and that is a major problem with this form of communication.

We are also very concerned, however, that it is important not to simply shut down a form of communication. And we think that that is an important matter, and I think our witnesses here today have raised that issue, also. We think that solutions are very difficult, but we want to sit down and continually work with you and your fine committee and your staff on looking at these solutions.

But since I last appeared before you there have been some significant changes in the marketplace, I think, some movement that I think I would like to raise with you.

The first is the Direct Marketing Association has finally, and I say that with a smile, launched its e-mail preference service, which

---

[24] *See Lamont v. Postmaster General,* 381 U.S. 301 (1965); *Shelton v. Tucker,* 364 U.S. 479 (1960); *Thomas v. Collins,* 323 U.S. 516 (1945). The right of anonymity also has been applied in commercial speech and Internet contexts. *NLRB v. Midland Daily News,* 151 F.3d 472 (6th Cir. 1998); *ACLU v. Johnson,* 4 F. Supp. 2d 1029 (D.N.M. (1998).

is a service in which individuals will be able to put their e-mail address on this list and companies will then scrub those addresses from their list on any unsolicited commercial e-mail offering that they have.

That service is now up, and we are getting companies signed on. They are required, if they are DMA members, to sign on to this. It is part of our privacy promise. It is fashioned after our mail preference service and our telephone service.

Mr. TAUZIN. Jerry, tell us how it works—specifically how it works for the consumer and the company.

Mr. CERASALE. It will not work for the customer until January 10. We want to make sure that we get everybody's systems lined up so it can work.

It starts this way. We have a web site, E-MPS.org, where companies and consumers can go to. Companies can sign up for this, and it costs $100 a year. They will—a company, if they want to send out an unsolicited commercial e-mail, will send their list of addresses to the DMA. We will then scrub that against the EMPS list and send back a list that has been cleaned for the marketer who then can send out the e-mail preference—excuse me, send out the solicitation without sending it to someone who has put their name on the list.

For a consumer, they would go to E-MPS.org and enter in their e-mail address, send it to us, and they are on the list.

The list works for—right now, the list is set up to work for a year. We find that the average e-mail address is good for about 6 months, with so many people changing it. So we have it work for a year.

But that is the system and how it is going to be set up. We are signing up companies now to make sure that their systems work with our system. And on January 10 they will be required to use this scrub on the list, and individuals can sign up for the list.

That is how it is set up to work. And it is very inexpensive. It is free to the consumer and $100 a year to the marketer.

It is part of our privacy promise that they use this. And our privacy promise requires that people give notice if they distribute information to third parties, give individuals an opportunity to opt out from that situation and also provides that marketers must honor opt-outs even from their customers from receiving any information. And that is required for telephone mail and e-mail.

We also believe that what has happened is that many service providers have established contractual arrangements with their business customers preventing them from sending bulk unsolicited commercial e-mail. And if they get complaints finding that, they are shutting down those sites. So that is an effort that has begun, and we believe it is becoming more and more prevalent on the net.

Finally, we find that Internet service providers appear to have significantly increased their ability to filter bulk unsolicited e-mail. We think the shutdown from certain service providers are forcing unsolicited e-mail providers going to specific ISPs, and it is making it easier to try and shut that down.

Finally, we are very sensitive at the DMA to sending fraudulent electronic messages with fraudulent headers. That practice is basically used to bypass any filtering operation. We believe that, ulti-

mately, it may be a clearly a subject for legislation. However, I do emphasize that right now it is our belief—and you can ask the person on the far end of the table here—that if you do send an e-mail with a fraudulent header that you have violated section 5 of the FTC act.

We do not object to any legislative solution, and it may be that we have to come up with a legislative solution. We do think that technology and business is changing, and we want to make sure that we give some time to see what is happening. And as we start with our EMPS service, as we see Internet service providers taking greater action against unsolicited bulk e-mail, that we think that we want to make sure we target and have a true rifle shot, as opposed to a shotgun blast.

I stand ready to work with you, and we appreciate the time.

[The prepared statement of Jerry Cerasale follows:]

PREPARED STATEMENT OF JERRY CERASALE ON BEHALF OF THE DIRECT MARKETING ASSOCIATION, INC.

I. INTRODUCTION

Good morning, Mr. Chairman, and thank you for the opportunity to appear before your Subcommittee as it considers unsolicited commercial electronic mail and the House bills that have been proposed to address this issue. I am Jerry Cerasale, Senior Vice President of Government Affairs for The Direct Marketing Association, Inc. ("The DMA").

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

The DMA member companies have a major stake in the success of electronic commerce, and are among those most likely to benefit immediately from its growth. The healthy development of electronic commerce depends on consumer trust. It is imperative that the e-mail communications medium earn that trust.

There are two main topics I wish to focus on in my testimony today that I believe are critical to the examination of unsolicited commercial electronic mail ("UCE"). First, I want to discuss The DMA's exciting new electronic mail preference service, known as e-MPS, which will allow greater control of UCE. Second, I want to describe the progress that we believe is being made by industry in combating the abuse of UCE.

The DMA welcomes this congressional inquiry into these important matters.

II. THE E-MPS EMPOWERS CONSUMERS WITH CHOICE CONCERNING RECEIPT OF UNSOLICITED COMMERCIAL E-MAIL

Mr. Chairman, just last week The DMA's e-mail preference service[1] was launched at our annual conference in Toronto. The DMA is very excited about this new service, which will allow individuals to remove their e-mail addresses from Internet marketing lists in a manner similar to The DMA's long-standing telephone and mail preference services. This ambitious undertaking is aimed at empowering consumers to exercise choice regarding receipt of UCE, while creating opportunity for the many exciting new benefits of legitimate marketing in the interactive economy.

As I mentioned, the e-MPS is based on The DMA's very successful Mail Preference Service ("MPS") and Telephone Preference Service ("TPS") self-regulatory initiatives. Both of these initiatives represent The DMA's response to consumers' re-

[1] See attached brochure.

quest for choice in the amount of mail and telephone solicitations they receive. In developing responsible marketing practices for the Internet age, we have adapted this important concept of consumer choice to the Internet medium through the development of e-MPS.

As of January 10, 2000, consumers will be able to register for the e-MPS service at a special DMA web site. At no cost to consumers, they can use this service to place their e-mail addresses on a list indicating that they do not wish to receive UCE. This service affords consumers with flexibility to determine the types of solicitations they receive. Individuals can opt out of business-to-consumer UCE, business-to-business UCE, or all UCE.

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

III. INDUSTRY IS MAKING SIGNIFICANT ADVANCES IN COMBATING THE ABUSE OF UNSOLICITED COMMERCIAL ELECTRONIC MAIL MESSAGES

The DMA commends the Members on their proposed legislation and the Subcommittee for its continued oversight of the development of the Internet. The three bills being discussed today all present thoughtful approaches to addressing some of the problems posed by abusive use of UCE. It is important for our membership and for the successful development of this tremendous new medium that responsible marketing practices be followed in the sending of unsolicited electronic mail messages. Such practices will ultimately provide consumers and business with the numerous potential benefits of a robust electronic commerce marketplace.

It is amazing to think that the widespread use of e-mail began with the commercial inception of the Internet just a few short years ago. Electronic mail has truly become a mainstay of both the personal and professional communications of today. The use of electronic mail is growing at such a significant pace that the GAO estimates that in the coming years the United States Postal Service will lose approximately $17 million annually due to the use of e-mail.

The DMA is encouraged by the significant developments that are beginning to effectively combat abuses of electronic mail. These developments include the termination of service by e-mail providers to individuals that abuse their services, technological developments that allow service providers to detect and block bulk UCE, and successful legal actions against individuals who have abused electronic mail.

Providers of electronic mail services have made significant strides in reducing the problems associated with UCE by terminating the accounts of individuals who abuse the services. In order to be able to terminate service, providers are including prohibitions on the sending of UCE without their express permission in their terms of service agreements. These efforts have drastically reduced the amount of abusive UCE that individuals receive.

There are, of course, situations where ISPs' services are being abused by entities that are not bound by the providers' terms of service agreements. These situations arise when providers' networks are used in the transmission of e-mail by individuals who are not subscribers to their services. The DMA is very sensitive to the burdens on the facilities of providers associated with this type of abuse. Bulk UCE should not be used in a way that results in the interruption of the providers' services. As we understand it, however, such abuses are being successfully addressed through technological processes that allow providers to detect and block such messages. Recent advances in technologies have made such detection and blocking very effective.

In addition to termination of service and technological solutions, legal actions have been an important vehicle through which to reduce abusive UCE. Service providers have been successful in reducing the abusive uses of UCE through a variety of different legal causes of action.

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

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

While The DMA does not object to a legislative solution to UCE, we believe that current efforts of industry and innovations in technology render any immediate legislation unnecessary. Likewise, we believe that the e-MPS will empower consumers with robust choice as to whether to receive unsolicited electronic mail messages.

IV. CONCLUSION

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

The Direct Marketing Association ("The DMA") is the largest trade association for businesses interested in interactive and database marketing, with nearly 4,500 member companies from the United States and 53 other nations.

Founded in 1917, its members include direct marketers from every business segment as well as the non-profit and electronic marketing sectors. Included are catalogers, Internet retailers and service providers, financial services providers, book and magazine publishers, book and music clubs, retail stores, industrial manufacturers and a host of other vertical segments including the service industries that support them.

The DMA's leadership is continuing to expand its presence in the Internet and electronic commerce with its acquisitions of the Internet Alliance and the Association for Interactive Media. Members of The DMA include L.L. Bean, Time Inc., Dell Computer, Gateway 2000, DoubleClick, autobytel.com, BMG Direct, Charles Schwab & Co., Lucent Technologies, eBay, Acxiom, AT&T, America Online, IBM, MCI WorldCom, and others.

According to a DMA-commissioned study conducted by The WEFA Group, direct marketing sales in the United States exceeded $1.3 trillion in 1998. Approximately $759 billion in direct marketing purchases were made by consumers and $612 billion were made by businesses.

Mr. TAUZIN. Thank you, Mr. Cerasale.

Finally, Mr. Ray Everett-Church, Chief Privacy Officer and Vice President for Public Privacy of AllAdvantage.com in Hayward, California. The Chair is pleased to receive your testimony.

STATEMENT OF RAY EVERETT-CHURCH

Mr. EVERETT-CHURCH. Thank you, Mr. Chairman. And thank you to all the members of the committee. I am very grateful to have been given this opportunity.

I am here today representing my firm, AllAdvantage.com, which is a world leader in the emerging infomediary industry. As of this month, PC Data ranks our web site as the 12th largest most trafficked web property on the Internet. That is only after 7 months of operation.

As one of the world's large infomediaries, AllAdvantage.com works as an agent for consumers. We provide consumers with the means to take control of the way information is gathered about their web habits and to benefit from the collection and use of their personal information. Because we strictly maintain the privacy of personal information that our members share with us, we are able to build a relationship of trust with consumers, providing them with relevant content, including advertising that is individually targeted to their interests and preferences.

To become the world's most trusted infomediary, we depend upon not only consumer trust in us but upon consumer trust in the en-

tire electronic commerce marketplace, and the issue of trust is why AllAdvantage is interested in this issue of spamming.

As one of more than 200 corporate members of the Coalition Against Unsolicited Commercial E-mail, a grassroots coalition of businesses and consumers concerned with the problems of spam, and an association I am very pleased to sit on the board of directors for, AllAdvantage takes the issue of spamming very seriously. The reason I am here today is to share with you a sense of why AllAdvantage sees spam as a threat not only to our company but to the future of our industry, and I want to share with you some of the lessons I have learned in dealing with companies who have been on the receiving end of the flood of spam.

Finally, I would like to present some conclusions I have drawn for what we feel is the appropriate role for Congress to play in solving this problem.

Let me be clear about one thing at the outset: AllAdvantage is not eager to see burdensome regulations imposed on electronic commerce. Our first preference is for technology to provide an answer to the abuse that technology has made possible. However, as one who has worked for many years on technological solutions to the spam problem, I can speak with some authority to the fact that technology alone cannot end the scourge of spam.

I worked for many years as a technology consultant and as an attorney in private practice for clients consisting primarily of Internet startups and Internet service providers. On occasions too numerous to count, I received panicked phone calls from companies whose businesses were under assault from spammers. Sometimes their systems would crash under the weight of millions of e-mails, and in other cases they had their domain names appropriated by a spammer to deflect complaints or absorb undeliverable or bounced e-mail messages that were now flooding their server. In still other instances, spammers might have even hijacked their mail server to do the actual delivery of the flood of e-mail.

Such problems are not limited to the private sector. As I understand, the House of Representatives actually had a problem due to an exuberant staffer a couple of weeks ago, so I think the issue was brought very close to home.

When I have been called by folks in the private sector the conversation almost follows the same pattern. After confirming that they have taken necessary steps to solve any security issues that they have and to limit the load of spam into their system, we turn to the issue of the state of the law on spamming and review their legal options. Inevitably, we would each come to the same conclusion, the conclusion that countless other victimized businesses had, that pursuing a legal case is often not worth the trouble or expense. Even if the chances of winning a suit are high, the likelihood of recovery was minuscule.

This fact highlights the double-edged promise of bulk unsolicited commercial e-mail. Sending e-mail in bulk costs the sender a fraction of the cost of postal mail or making telemarketing phone calls, making it an attractive way for an individual to play in the big leagues. However, given the technology that is a great equalizer, one person can generate enough e-mail to take down the systems of a multibillion dollar corporation. This means that on a daily

basis we are faced with situations in which a single person's actions can cause damage and business losses far in excess of their ability to be held responsible for the trouble they cause.

When turned into an advertising medium, the skewed economics of e-mail turns traditional notions of advertising on its head. But in the world of junk e-mail marketing, because it costs no more to send the first e-mail than it does to send the ten millionth, there are very few incentives to limit their activities.

AllAdvantage believes that consumer distrust of the medium is the greatest impediment to the growth of e-commerce, and as recent studies have indicated, spam is a tremendous concern to consumers. A recent Gartner Group survey indicated that 34 percent of respondents saw spam as an invasion of their privacy, and 63 percent of respondents to an Intelliquest survey cited spam as the reason they feared making online purchases. As an advocate for our members, we believe that consumers' online habits as they are shaped by spam severely undermine consumer trust in the medium and are the reason why we support legislation that will address this problem.

I thank the chairman.

[The prepared statement of Ray Everett-Church follows:]

PREPARED STATEMENT OF RAY EVERETT-CHURCH, CHIEF PRIVACY OFFICER & VICE PRESIDENT FOR PUBLIC POLICY, ALLADVANTAGE.COM

Thank you Mr. Chairman and members of the Committee. I am very grateful to have been invited here today to discuss the issue of unsolicited commercial e-mail.

I am here today representing my firm, AllAdvantage.com, a world leader in the emerging Infomediary industry. As one of the world's largest Infomediaries, AllAdvantage.com works as an agent for consumers. We provide consumers with the means to take control of the way information is gathered about their Web habits, and to benefit from the collection and use of their personal information. Because we strictly maintain the privacy of the personal information they share with us, we are able to build a relationship of trust with consumers, providing them with relevant content, including advertising, individually targeted to their interests and preferences. To become the world's most trusted Infomediary; we depend upon not only consumer trust in us, but also upon consumer trust in the entire electronic commerce marketplace.

As one of more than 200 corporate members of the Coalition Against Unsolicited Email (CAUCE, www.cauce.org), a grassroots coalition of businesses and consumers concerned with the problems of spam, and an association for which I sit on the Board of Directors, AllAdvantage takes the issue of spamming very seriously. The reason I am here today is to share with you a sense of why AllAdvantage sees spam as a threat to not just our company, but to the future of our industry. I also want to discuss with you some of the lessons I have learned in dealing with companies who have been on the receiving end of a flood of spam. Finally, I wish to present some conclusions I have drawn about the appropriate role for the Congress to play in solving this problem.

Let me be clear about one thing at the outset: AllAdvantage is not eager to see burdensome regulations imposed on electronic commerce. Our first preference is for technology to provide an answer to an abuse that technology has made possible. However, as one who has worked for many years on technological solutions to the spam problem, I can speak with some authority to the fact that technology alone cannot end the scourge of spam.

I worked for many years as a technology consultant and as an attorney in private practice for clients consisting primarily of Internet "startups" and Internet service providers (ISPs). On occasions too numerous to count, I received panicked phone calls from companies whose businesses were under assault from spammers. Sometimes their systems would crash under the weight of millions of e-mail messages to their service's subscribers. In other cases, their domain name had been appropriated by a spammer, used to deflect complaints or to absorb undeliverable ("bounced") e-mail, messages that were now flooding their server. In still other instances, the spammers might even have hijacked their mail server to deliver a flood

of mail to another site. Recently, the House of Representatives own system crashed due to a spammed message from an exuberant staffer.

Always the conversation would follow the same pattern. After confirming that they had taken an array of technical steps to limit the load of incoming spam and implemented measures to repair any damage done, talk would turn to the question of legal recourse. Explaining to them the state of the law on spamming, and reviewing their legal options, inevitably they would come to the same conclusion that countless other victims had: pursuing a legal case is not worth the trouble or expense. Even if the chances of winning a suit were high, the likelihood of recovery was miniscule.

This fact highlights the double-edged promise of bulk unsolicited commercial e-mail. Sending e-mail in bulk costs the sender a fraction of the cost of sending postal mail or making telemarketing phone calls. One person can generate huge volumes of mail with just a few clicks of a mouse, blanketing millions in a matter of minutes or hours. However, the ability for one individual to generate enough e-mail to take down the systems of a multi-million dollar corporation means that on a daily basis we are faced with situations in which a single person's actions can cause damage and business losses often far in excess of their ability to pay for the trouble they cause.

When turned into an advertising medium, the skewed economics of e-mail 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. Postal Service, 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 e-mail marketing, it costs no more to send the first e-mail than it does to send the ten millionth e-mail. Thus, there is every incentive for the marketers to cast their advertisements as widely and indiscriminately as possible. There isn't even an incentive to remove duplicate addresses from mailing lists. And why not? When advertisers pay nothing more for each additional message, any time spent on editing a mailing list is time wasted.

Nobel Prize-winning economist Ronald Coase wrote eloquently about the damage done when costs are chronically externalized onto an ever-widening base. Coase 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 than to treat it and dispose of it in a more environmentally sensitive manner. By creating such "externalities," as economists call it, the creator can maximize their own profit, even if it comes at another's—or everyone's—expense. Certainly those who are harmed by poisons in a river 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 in this example give incentive to the polluters while making it prohibitive for victims to seek a remedy. Hence, governmental intervention became necessary.

Much is the same when it comes to spam. While some companies have successfully sued junk e-mailers for the damage they have caused, very few ISPs can afford to fight these kinds of cutting edge cyberlaw battles. As a result, the economics favor the abusers and disfavor those victimized. Indeed the mailers are counting on the fact that the incremental costs foisted upon each individual member of the public at large will be ignored, and on the occasions when those costs become aggregated in the crash of an ISP, they know that they present too small of a target to be worth suing.

As Coase pointed out, this is a prescription for economic disaster. When inefficiencies are allowed to continue, the free market no longer functions properly. The "invisible hands" that would normally balance the market and keep it efficient cannot function when the market is carrying dead weight and perpetuating chronic inefficiencies. Unchecked, businesses that are (and should be) 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 e-mail takes 3 hours to

travel from one ISP to another, or when all your e-mail is lost in a server crash. But the costs do not stop there.

With spam, the number one complaint of most Internet users, we see that consumers have deserted many public discussion forums for fear that their e-mail 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 e-mail to communicate with their existing customers for fear of being branded net abusers.

AllAdvantage believes that consumer distrust of the medium is the greatest impediment to the growth of e-commerce—a belief borne out in study after study. A recent Gartner Group survey indicated that 34% of respondents saw spam as an invasion of their privacy, while 63% of respondents to an Intelliquest survey cited spam as the reason they feared making online purchases. Because of its impact on consumers' online habits, we believe spam is a threat to our business and to the entire online industry. As an advocate for our members, we believe that by giving individuals and ISPs the legal tools needed to stop spam, and by avoiding cumbersome and costly procedures, consumers are better served.

In particular, our hope is to see legislation that recognizes the right of individuals and businesses to be free from bearing the costs of unwanted advertising. AllAdvantage supports legislation that will allow the marketplace to determine the value of unsolicited commercial e-mail, with senders clearly able to discern recipients' desires, and recipients given recourse if their rights are violated.

First, we believe that service providers should be permitted to set policies based upon the preferences of their customers, up to and including the unrestricted right to undertake such technical measures as they deem necessary to limit the amount of spam entering their systems. Already, dozens of ISPs cater to the wishes of parents and religious communities who wish to buy Internet access that filters out unwanted and offensive materials. The ability of service providers to respond to consumers' desires for such content-based blocking should not be hindered.

Second, we believe that operators of mail servers, be they service providers, private businesses, or school, should be permitted to publicly post a policy stating whether they accept unsolicited commercial e-mail, and if so, under what terms. For those who do not wish to accept unsolicited commercial e-mail, the notice should be respected and treated under law much like a "No Trespassing" sign on the border of one's private property. For those organizations that agree to accept unsolicited commercial e-mail, such a system could enable senders and recipients to negotiate a fair delivery arrangement, in effect establishing a marketplace for spam.

Providing a server-based "No Trespassing" sign is already possible today, a fact acknowledged in H.R. 2162. The technology is already built into virtually every e-mail server in operation today, and even as I address this committee, hundreds of e-mail servers around the country are already broadcasting their spam preferences to every prospective e-mail sender, if they know what to look for. This technique, called "SMTP Banner Notification," gives advertisers ample opportunity to avoid unintended liability by allowing them to quickly and authoritatively assess the publicly posted policies of service providers. All that is needed in this regard is for Congress to acknowledge that such a notification process is possible and to establish the legal weight of the notice transmitted through it.

Third, and finally, we believe that if a sender of unsolicited commercial e-mail fails to heed the wishes of recipients through such public notices, the law should permit both individuals and businesses harmed by spam to seek recovery by bringing private attorney general (qui tam) actions in court. For those individuals or businesses who cannot afford to bring such actions to enforce their rights, we would like to see them be able to petition the Federal Trade Commission to bring an enforcement action on their behalf. This dual approach is already contained in H.R. 3113 and we believe it is an excellent starting point.

By carefully assembling pieces of both H.R. 2162 and H.R. 3113, we believe it is possible to craft a bill that is stronger than either of the bills taken separately. We believe that combining the complementary portions of both bills will produce a measured approach that gives maximum flexibility to service providers and their customers, while also giving responsible marketers ample opportunities to reach audiences that will be receptive to their information.

AllAdvantage, along with a coalition of business and consumer groups, has been honored to share with Representatives Wilson and Miller new language that we believe draws from the best ideas contained in bills H.R. 2162 and H.R. 3113. Through the leadership of these outstanding Members of Congress, and hopefully with the input from and support of Representatives Goodlatte and Boucher—two of the most respected advocates for strong Internet commerce—we hope to be able to take part in crafting a compromise. We would like to thank the talented staff in the offices

of Representative Wilson, Representative Green and Representative Miller for allowing our coalition to share our concerns and ideas.

It is my hope that we can ultimately reach agreement on language that can win not only bipartisan support in Congress, but can be supported by e-commerce firms, ISPs, advertisers, and advocates for consumers. If we can meld the approaches contained in these two bills, I believe we can reach language that will give ISPs and e-commerce businesses the tools they need to react to the concerns of their customers, without creating unnecessary government involvement in the Internet.

In conclusion, 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. Yet in just a few short years, the outrageous volumes of unsolicited advertisements by e-mail have clearly begun to have a profoundly negative effect upon all Internet commerce. My fear is that the untapped potential of e-mail may be lost if its functionality and utility are destroyed by the unchecked activity of the extreme minority of individuals who send unsolicited commercial e-mail. Unless Congress acts to preserve the viability of the medium and to give businesses and consumers the ability to protect themselves from floods of unsolicited e-mail, 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.

Thank you, Mr. Chairman, for allowing me the opportunity to address the committee. I look forward to answering any questions you might have.

Mr. TAUZIN. Thank you very much.

The Chair thanks you all.

The Chair will go out of order in respect for the authors of the legislation, and the Chair will recognize Mrs. Heather Wilson for a round of questions.

Mrs. WILSON. Thank you, Mr. Chairman.

I have a number of different questions. I would first like to ask probably Mr. Brown and Mr. Church and possibly also Mr. Russina about technology issues. Is there filtering technology that is effective now or could legislation combined with filtering technology—legislation, for example, that required some kind of a header or a tag or something that could—for unsolicited commercial e-mail, could that be a solution to this problem?

Mr. BROWN. I think that filtering is—I guess the easiest answer is filtering is not scalable, either technically or economically. As spam increases or more unsolicited e-mail goes out there, we are going to need to implement more systems, more computers to process that mail to determine whether or not that is a message that we want to take or not to take by examining the messages.

So I would say that, as volume of e-mail goes up, we are going to have to look at every e-mail that comes through to determine whether or not it is a message or not. So we have to touch each one of them. I don't think that is necessarily a scalable solution economically or technically.

Mrs. WILSON. Mr. Church or Mr. Russina? Do you have anything?

Mr. RUSSINA. Some of the things that we do today as far as trying to track where the user is coming from and put some tracking and legitimizing behind the e-mails, we look at the IP address from which the e-mail is coming from, and it has to match the domain name from which the e-mail is coming from, but we cannot check the user. We do not have that capability yet.

So if we have a consumer that is logging in, say, the Southwestern Bell Internet Service and spamming the Pacific Bell Internet Service, if they are coming from an IP address that belongs to Southwestern Bell and they use a bogus name on the front of the

"at" sign, they can do it. There is not any means of tracking that piece down right now.

Mr. EVERETT-CHURCH. If you think about the way a computer processes information, as fast as it operates, it really only processes one thing at a time. It just does it one at a time very, very rapidly.

If you think of each e-mail message coming in, a lot of operations occur. It has got to be passed through a system, sorted, deposited in the correct mailbox, written to the hard disk, et cetera.

If you add filtering to that process, matching the data to a list, to a data base of known spamming addressing or what have you, in some cases you are doubling or tripling the amount of actions that must be taken on any piece of data. And when you try and scale that to a large quantity such as the kind of data traversing systems like America Online and SBC and others, you find that the—as John Brown said, the filtering solutions don't always scale.

Mrs. WILSON. Thank you.

Mrs. Harrington, you may be the best one to ask this question because of the data base that the FTC keeps. Is most pornographic e-mail also commercial e-mail? In other words, if we restricted legislation to unsolicited commercial e-mail, would we capture much of the problem with the pornographic e-mail?

Ms. HARRINGTON. I don't know. We see a good deal of commercial e-mail that is intended to induce people to call or visit sexually explicit chat lines and sites. But we only know what we know. I think that consumers are more inclined to forward to us commercial e-mail than noncommercial e-mail, and so I don't have an answer to your question.

Mrs. WILSON. Do any of you who deal with this or who run ISPs and watch your computers have a sense of this?

Mr. BROWN. Well, I would ask the question, if I am sending a solicitation to come and visit my pornographic web site, some of those web sites recoup their costs by charging you a monthly service fee or subscription rate to visit their site, and some of those places are now taking—advertising on the web site, banner ads, et cetera, to recoup their costs.

So I guess my question is—that would be an indirect form of commercial. Would it be a direct and would that relate to your question? I am not sure. But I think one could get slippery with we are not directly deriving revenue from sending that e-mail; we are getting it indirectly. I would be sort of curious about how slippery that could get.

Mrs. WILSON. Thank you, Mr. Chairman.

Mr. TAUZIN. The gentleman from Texas, Mr. Green, is recognized.

Mr. GREEN. Thank you, Mr. Chairman.

I would like to ask Mr. Cerasale a couple of questions. When—the first bill I introduced was 1910, and it was the one that dealt with fraud on spam. Could you expand a little bit and tell me why you prefer spam legislation that only deals with fraud?

Mr. CERASALE. Why we prefer only legislation that deals with fraud?

Mr. GREEN. Yes, do you think that is more where the Congress should be addressing?

Mr. CERASALE. Well, first, I think that we have State and Federal laws on fraud. The thing—why I discussed fraud was that we think that, right now, that is the means to bypass filtering. The fraudulent headers are the means to bypass filtering. And that fraud I was talking about was in that area, the fraudulent header. A fraudulent get-rich-quick scheme, et cetera, whether it is over the Internet or in the phone or through the mail, they are all the same, people trying to get rich quick. And I think they are clearly covered by section 5 of the FTC Act, and strong enforcement is what is needed.

I think the change here is that the fraudulent header is a meaning to deceive usually—deceive the recipient, but basically to deceive the ISP in their filtering operation.

Mr. GREEN. I know the DMA has taken a positive step from the marketer's perspective on addressing spam through their EMPS service, your opt-out list. And my concern is more with the bad actors, the people who will open a shop for a few hours and send out millions of spam and then move on. In that instance don't you think there should be a legislative solution?

And, further, could you explain what would happen to a member or a company who uses your EMPS service and then sends out spam anyway? And what action would DMA take to stop their own members from doing this?

Mr. CERASALE. The first part of the question is, looking at the bad actors—thank you for thinking that our members are good actors, I appreciate that—but the bad actors who are not members of the DMA, who don't use the service—the service is not limited to just DMA members. Anyone who is willing to pay the $100 can use it.

I think our point is that we would like to see a little bit of time to take a look at it to see if this becomes a norm, if we have an educational process and so forth, that you should have the opportunity to opt out. It may be even looking at an e-mail coming out should give you the opportunity to opt out individually on it. Those kinds of things the DMA is looking at and maybe a little bit of time to see how EMPS works.

We are not standing here opposed to legislation that would say that you have to give people notice and choice, because that is clearly the DMA's privacy promise. That is what we stand for.

What would happen if the e-mail preference—if a DMA member who has to use the e-mail preference service doesn't use it, sends out unsolicited commercial e-mail without scrubbing it against the list?

The first thing, you have to look was there a mistake made would be one. But let's assume it was not a mistake. They did it in violation of the privacy promise. The procedure would be we would do an investigation, but they would be brought before the board of directors and could be kicked out of the DMA, and that would be publicly stated.

So there would be a press release from the DMA that says—let's use my name—the Jerry Cerasale Company has been kicked out of the DMA for not fulfilling its privacy promise and violating it here. That would create some fairly significant negative publicity toward the Jerry Cerasale Company. And we found when we went around

with the privacy promise and we put ads in the trade press to say these are the people who have signed up already prior to July 1 when it started, we have—it was applied to business-to-consumers, so we had some business-to-business members who said we want to be able to sign up because we are not getting the good press from this that we signed up for.

So I think that is where the negative is. Sorry to take so long on the answer.

Mr. GREEN. Thank you, Mr. Chairman.

If I could throw one question out and they could answer it however. Because it is one you brought up earlier concerning the technological blocks that are available maybe now for spam or filters, and both, whether it be the ISP or the individual, and is there new technology that we might be able to use that would do it? And that would be for everyone to answer as quick as you could.

Mr. TAUZIN. Anyone wants to handle it, please. What is the status of filtering technology both from the consumer and to the ISP?

Mr. CERASALE. I don't think there is too much from the consumer standpoint. I do not see any status of technology—I am not the expert here—any technology where the consumer can stop certain e-mail. When it comes in to you it is not bulk at that time. It is individual. And it comes to my station, and you can potentially have a block. I think technology can be made that you only want to receive e-mail from certain places. That is available.

Mr. TAUZIN. I think what the gentleman is asking, though, is if—assuming, as Mrs. Wilson pointed out, that unsolicited bulk e-mail was required by law to be headed in that fashion so that you had a violation of section 5 if you failed to properly head it. Could the consumer conceivably have filtering devices and the ISP similarly have filtering devices that could then either block it going to the consumer or stop it from entering the consumer's PC?

Mr. CERASALE. I think if you had certain words that were required likely there is a technology that could stop it from coming in. That raises the issue of labeling speech, however, and we have to look at that as we talk about——

Mr. TAUZIN. Mr. Brown?

Mr. BROWN. Thank you, Mr. Chairman.

I think the easy answer to that question is I am sitting in Roswell, New Mexico, and for me to get to America Online I have to make a long distance intrastate call to get to Albuquerque, New Mexico. I go to my local computer store. I buy my filtering software. I load it on my PC. I have still spent the money to call Albuquerque, so I download that message and then I use my filtering software to throw away. The cost is shifted to the end user.

That would be my statement, Mr. Chairman.

Mr. TAUZIN. Okay. The gentlewoman from California is recognized.

Ms. ESHOO. Thank you, Mr. Chairman, for holding this hearing. And, first, may I ask, has there been a unanimous consent request that members be able to submit statements?

Mr. TAUZIN. I think we have done it, but I will do it. I ask unanimous consent that all members' written statements be made a part of the record. Without objection, so ordered.

Ms. ESHOO. Thank you very much.

Welcome to the witnesses. I have three questions, one of Ms. Harrington and two of Mr. Everett-Church; and I have 5 minutes, so try to get your answers in. All right?

First to Ms. Harrington, do you believe that by increasing the penalties in the Computer Fraud and Abuse Act and current State law that we could solve many of the ongoing problems that the witnesses identified with regard to spam and spamming?

Ms. HARRINGTON. I think that increased penalties operate as a deterrent, yes. But I think that there is a pervasive problem with deceptive and fraudulent UCE and other deception on the Internet that goes to the difficulty that consumers and enforcers have in authenticating the identity of a site owner or a mail sender.

We have heard talk about false headers and so forth. When a false header is used, which probably is in most instances deceptive and in violation of the FTC act, there is a task of investigating to determine who the sender is, and that may or may not be a difficult task. Likewise, if a URL is falsely registered, it is very difficult to learn who the true owner of the URL is. And so if we are thinking about increased penalties, I think it is very important to increase penalties for falsifying that information, both e-mail header information and URL registration information.

Ms. ESHOO. As a deterrence. How would you characterize it in terms of percentage, one, and the other that you just described? Do you have any idea?

Ms. HARRINGTON. URL versus false e-mail? Well, I think that URL registration—the falsification of URL registration information is a huge problem.

Ms. ESHOO. How huge, though? Give us an idea.

Ms. HARRINGTON. When we go out on the Internet and find web sites that make egregiously false claims it is not uncommon when we check the "who is" and other registration information to find that it is patently and facially false. And what we know is that the registrars take the position that it is not their job to verify the truthfulness or authenticity of that information. So we will find a fraudulent site and see that it is registered to a party who identifies itself as Amanda Hugandkiss living in Here, There, Everywhere. And when we go to the registrar and say how can you allow someone to sign up with this facially false information, and they say, hey, not our job.

Ms. ESHOO. Thank you. That is instructive for the shaping of legislation.

To Mr. Everett-Church, fellow Californian, welcome. It is good to have you here.

Service providers are already bringing lawsuits against spammers. Why would service providers seek action from an agency like the FTC instead of bringing an action themselves? And, also, you are a board member of the Coalition Against Unsolicited Commercial E-mail, which you mentioned just a few moments ago. What does the Coalition membership see as the key elements of legislation to stop spam?

Mr. EVERETT-CHURCH. To address your first question, the problem with bringing an action in court for most service providers is that it is extremely costly and time consuming, both in investigating, trying to track down—as Ms. Harrington mentioned, it

can be very difficult to locate the appropriate defendant to bring a case and then to pursue that only to find that there is no possibility of recovery against an individual. So for small service providers, that kind of cost can make seeking legal redress insurmountable for them and leave that unavailable.

The resources of an agency like the Federal Trade Commission are a little bit larger than that of a small service provider and so the hope is that by turning to the agency they can get the relief that they need.

As to your second question, very briefly, the Coalition, the members of the Coalition Against Unsolicited Commercial E-mail are real eager to see a marketplace solution but one that is grounded in legal recognition of the rights of service providers and consumers to be free from the harm imposed by senders of unsolicited commercial e-mail.

So we are hoping to see legislative solution that addresses itself to the specific issues of service providers' rights of action, ability for consumers to protect themselves and to make their preferences known and to seek recovery in the event that those wishes are violated.

Ms. ESHOO. I hope you move to my district.

Mr. EVERETT-CHURCH. Can you help us find office space?

Ms. ESHOO. It is at a premium, I know.

Mr. TAUZIN. The gentleman from Illinois is recognized.

Mr. SHIMKUS. Thank you, Mr. Chairman.

I think Ms. Eshoo asked a couple of questions I wanted to, especially with the ISPs and, actually, with Ms. Harrington on the FTC. Let me just follow up just on my own since I was out. Catching the end of the question, do you feel the FTC has tools necessary right now to prevent the fraudulent and deceptive e-mail?

Ms. HARRINGTON. Yes, I think that section 5 of the FTC act is sufficiently broad and expansive, that it gives the Commission the authority to take action to prohibit deceptive practices.

There are some challenges involved in investigating deceptive marketers who use false header information. The investigative challenge there is great. And the cost of doing that kind of investigation is significant and so I would be remiss—and I want to make clear that I am speaking for myself and not necessarily the Commission or the Chairman, but I would be remiss in failing to say that the more resources that we can have in terms of people and computers to do these kinds of investigations, the better job we will do. This is a whole new area of marketing that we are I think working hard to stay on top of. And all of the other areas of marketing that we have been policing for years are still vibrant and active, so it has really expanded our work.

Mr. SHIMKUS. Thank you, Mr. Chairman. And appreciating the time and the vote, I think I will yield back. I thank the folks for their testimony.

Mr. TAUZIN. The Chair recognizes himself briefly.

In the time we have remaining, let me try to follow up on some of the things that have been suggested and that we have heard.

Mr. Kennedy, first of all, if a law was passed—part of the laws we passed required unsolicited bulk e-mail to be properly identified by the sender. Do you see any constitutional problems with such

a provision in terms of inhibiting free speech? After all, we have similar laws regarding bulk mail at the post office. Is this similar and could it be sustained on a similar basis or is there a problem?

Mr. KENNEDY. No, I believe it would be sustained if it applies to commercial e-mail only. You get a more lenient standard of review for restrictions on commercial speech. And, after all, in the commercial context what we are dealing with are people who falsify header information to defeat anti-spam software. Sometimes they violate trademark by doing this. Often they violate section 5 of the FTC act. That is not protected speech.

Mr. TAUZIN. Assuming we could do that then, the next question I want to ask all of you, if you had in place some or parts of all the laws that have been discussed here today as possible remedies, if you had in place rights of action by the ISP to go against someone who is defrauding them by stealing their mailers and their servers or hijacking their systems to flood someone with e-mail, if you had indeed a requirement that bulk commercial e-mailers had to properly identify on the header exactly what it is, that bulk unsolicited e-mail, so that filtering systems could eventually be more effective both for the ISP who might filter them out at the request of the customers or to the customers themselves who might filter them out at the PC end, and if you had systems like Mr. Cerasale has talked about where at least the better players would be signing up to literally take themselves out of the play of sending e-mail to people who don't want it, is there a possibility that combinations of that sort could work to effectively lower the scale, if you will, of unsolicited bulk e-mail so that Mr. Everett-Church's and Mr. Brown's filtering systems would not be overwhelmed so that the FTC would not necessarily be overwhelmed in terms of the work, so that the consumers would the least see a lowering of the level, the tempo of this stuff? Anyone want to hit it?

Ms. HARRINGTON. Mr. Chairman, I am not a technologist, but I just read in a Salon Magazine online magazine article the other day about an entrepreneur who made his fortune developing the software that is used for push technology, that is, that sends much of this out. He has taken that fortune and invested it in a new enterprise that is going to filter it all out.

Mr. TAUZIN. Like the radars and the radar detectors?

Ms. HARRINGTON. I think that gives me hope. That is, if there is someone who is a technologist who made his first fortune figuring out how to cause this problem and he now has invested his fortune in a company that is purportedly going to solve the problem, that gives me hope.

Mr. TAUZIN. It's like Dillinger joining the FBI.

Ms. HARRINGTON. That is right. So I think it is worth—certainly worth trying to pull together the components that you just mentioned.

Mr. TAUZIN. If those components were pulled together, there is no question that section 5 would give you authority to deal with anyone who consistently was failing to correctly identify their commercial bulk e-mail as commercial bulk e-mail.

Ms. HARRINGTON. It might be helpful to, if there is going to be a labeling requirement, to give us some specific authority to enforce that.

Mr. TAUZIN. Mr. Brown.

Mr. BROWN. Mr. Chairman, I want to go back to my example a moment ago about the consumer level filtering. One of the things that I would like to try to make very clear is that, regardless of whether we label this, et cetera, the message has to still be delivered. There is a cost to that delivery. And who bears that cost? And so the question I would have is, are we attempting to try to minimize that cost or are we trying to get rid of that cost?

Mr. TAUZIN. Well, Mr. Brown, assuming that filtering systems could be developed both for the ISP to filter them at the server——

Mr. BROWN. I still have to receive that from the upstream link that I am paying for.

Mr. TAUZIN. But in fact if consumers knew, if you had to post your policy that we are not going to send you unsolicited e-mail, and you have the equipment, how to filter it out, because of the requirements that it be properly labelled and the FTC is there to help you enforce that policy, the opportunities for people to use your system to flood people with e-mail would be decreased dramatically, don't you think?

Mr. BROWN. Yes, I would agree. I would think that it would be decreased dramatically.

I guess where my stance is coming from is that I don't want to spend even a penny on having to deal with it.

Mr. TAUZIN. Well, I know you don't, but if I am a customer of yours and I can choose from among ISPs who are not willing to spend that penny to protect me from this e-mail that I don't want or to choose a company like yours that is willing to spend the penny, I might choose you over the other company. I mean, that is the premise at least of the Miller approach, that consumers would make choices in the marketplace among ISPs depending on which one better protects them. And if we provided you with better capabilities to protect them by a labeling requirement, enforceable through the FTC, would you not be encouraged then to be one of those companies who wants to attract customers who want that protection? I think you might.

I know you would rather not spend the penny, but I am saying if the customers say they are going to choose you if you spend that penny and are maybe even willing to pay a little more if you do that for them, you might be encouraged to do that.

Ms. HARRINGTON. Mr. Chairman, I would add to this package the importance of opt-out and consumer empowerment to opt out. And on the opt-out matter, something that is tricky is defining the prior business relationship. And the caution we would sound is that the exception not be so broad that it swallows the rule.

Mr. EVERETT-CHURCH. I wanted to add briefly, as I mentioned in my remarks, technology alone cannot solve the problem, but the legal component is important. And by addressing both the technology and the legal issues and pulling them together and, in fact, even combining the approaches contained in the various bills that we have talked about today, I think we can reach a solution that is very carefully targeted and crafted to address the most significant of the problems.

Mr. TAUZIN. That is what I am learning today, too. I think it is possible to take the best of all of these approaches and maybe add

this labeling. With the FTC clearly in charge of enforcement on the labeling end we might be able to put something together. We are going to try.

Let me thank you then. You have contributed mightily.

And as I said, Mr. Church, if we have come to the conclusion about one of the best parts of all these bills we have done a lot of good today.

Thank you very much. The hearing stands adjourned.

[Whereupon, at 12:25 p.m., the subcommittee was adjourned.]