LEGISLATIVE EFFORTS TO COMBAT SPAM

JOINT HEARING

BEFORE THE

SUBCOMMITTEE ON
COMMERCE, TRADE, AND CONSUMER PROTECTION

AND THE

SUBCOMMITTEE ON TELECOMMUNICATIONS AND
THE INTERNET

OF THE

COMMITTEE ON ENERGY AND
COMMERCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS

FIRST SESSION

JULY 9, 2003

Serial No. 108–35

Printed for the use of the Committee on Energy and Commerce

Available via the World Wide Web: http://www.access.gpo.gov/congress/house

U.S. GOVERNMENT PRINTING OFFICE

88–428PDF WASHINGTON : 2003

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

COMMITTEE ON ENERGY AND COMMERCE

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

MICHAEL BILIRAKIS, Florida
JOE BARTON, Texas
FRED UPTON, Michigan
CLIFF STEARNS, Florida
PAUL E. GILLMOR, Ohio
JAMES C. GREENWOOD, Pennsylvania
CHRISTOPHER COX, California
NATHAN DEAL, Georgia
RICHARD BURR, North Carolina
Vice Chairman
ED WHITFIELD, Kentucky
CHARLIE NORWOOD, Georgia
BARBARA CUBIN, Wyoming
JOHN SHIMKUS, Illinois
HEATHER WILSON, New Mexico
JOHN B. SHADEGG, Arizona
CHARLES W. "CHIP" PICKERING, Mississippi
VITO FOSSELLA, New York
ROY BLUNT, Missouri
STEVE BUYER, Indiana
GEORGE RADANOVICH, California
CHARLES F. BASS, New Hampshire
JOSEPH R. PITTS, Pennsylvania
MARY BONO, California
GREG WALDEN, Oregon
LEE TERRY, Nebraska
ERNIE FLETCHER, Kentucky
MIKE FERGUSON, New Jersey
MIKE ROGERS, Michigan
DARRELL E. ISSA, California
C.L. "BUTCH" OTTER, Idaho

JOHN D. DINGELL, Michigan
Ranking Member
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
BART STUPAK, Michigan
ELIOT L. ENGEL, New York
ALBERT R. WYNN, Maryland
GENE GREEN, Texas
KAREN MCCARTHY, Missouri
TED STRICKLAND, Ohio
DIANA DEGETTE, Colorado
LOIS CAPPS, California
MICHAEL F. DOYLE, Pennsylvania
CHRISTOPHER JOHN, Louisiana
TOM ALLEN, Maine
JIM DAVIS, Florida
JAN SCHAKOWSKY, Illinois
HILDA L. SOLIS, California

DAN R. BROUILLETTE, *Staff Director*
JAMES D. BARNETTE, *General Counsel*
REID P.F. STUNTZ, *Minority Staff Director and Chief Counsel*

SUBCOMMITTEE ON COMMERCE, TRADE, AND CONSUMER PROTECTION

CLIFF STEARNS, Florida, *Chairman*

FRED UPTON, Michigan
BARBARA CUBIN, Wyoming
JOHN SHIMKUS, Illinois
JOHN B. SHADEGG, Arizona
Vice Chairman
GEORGE RADANOVICH, California
CHARLES F. BASS, New Hampshire
JOSEPH R. PITTS, Pennsylvania
MARY BONO, California
LEE TERRY, Nebraska
ERNIE FLETCHER, Kentucky
MIKE FERGUSON, New Jersey
DARRELL E. ISSA, California
C.L. "BUTCH" OTTER, Idaho
W.J. "BILLY" TAUZIN, Louisiana
(Ex Officio)

JAN SCHAKOWSKY, Illinois
Ranking Member
HILDA L. SOLIS, California
EDWARD J. MARKEY, Massachusetts
EDOLPHUS TOWNS, New York
SHERROD BROWN, Ohio
JIM DAVIS, Florida
PETER DEUTSCH, Florida
BART STUPAK, Michigan
GENE GREEN, Texas
KAREN MCCARTHY, Missouri
TED STRICKLAND, Ohio
DIANA DEGETTE, Colorado
JOHN D. DINGELL, Michigan,
(Ex Officio)

SUBCOMMITTEE ON TELECOMMUNICATIONS AND THE INTERNET

FRED UPTON, Michigan, *Chairman*

MICHAEL BILIRAKIS, Florida
JOE BARTON, Texas
CLIFF STEARNS, Florida
Vice Chairman
PAUL E. GILLMOR, Ohio
CHRISTOPHER COX, California
NATHAN DEAL, Georgia
ED WHITFIELD, Kentucky
BARBARA CUBIN, Wyoming
JOHN SHIMKUS, Illinois
HEATHER WILSON, New Mexico
CHARLES W. "CHIP" PICKERING, Mississippi
VITO FOSSELLA, New York
CHARLES F. BASS, New Hampshire
MARY BONO, California
GREG WALDEN, Oregon
LEE TERRY, Nebraska
W.J. "BILLY" TAUZIN, Louisiana
(Ex Officio)

EDWARD J. MARKEY, Massachusetts
Ranking Member
BOBBY L. RUSH, Illinois
KAREN McCARTHY, Missouri
MICHAEL F. DOYLE, Pennsylvania
JIM DAVIS, Florida
RICK BOUCHER, Virginia
EDOLPHUS TOWNS, New York
BART GORDON, Tennessee
PETER DEUTSCH, Florida
ANNA G. ESHOO, California
BART STUPAK, Michigan
ELIOT L. ENGEL, New York
ALBERT R. WYNN, Maryland
GENE GREEN, Texas
JOHN D. DINGELL, Michigan,
(Ex Officio)

CONTENTS

LEGISLATIVE EFFORTS TO COMBAT SPAM

WEDNESDAY, JULY 9, 2003

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ENERGY AND COMMERCE,
SUBCOMMITTEE ON COMMERCE, TRADE, AND
CONSUMER PROTECTION JOINT WITH THE SUBCOMMITTEE
ON TELECOMMUNICATIONS AND THE INTERNET
Washington, DC.

The subcommittees met, pursuant to notice, at 1:03 p.m., in room 2123, Rayburn House Office Building, Hon. Cliff Stearns (chairman, Subcommittee on Commerce, Trade, and Consumer Protection) and Hon. Fred Upton (chairman, Subcommittee on Telecommunications and the Internet), presiding.

Members present, Subcommittee on Commerce, Trade, and Consumer Protection: Representatives Stearns, Upton, Cubin, Shimkus, Shadegg, Bass, Ferguson, Issa, Tauzin (ex officio), Schakowsky, Solis, Markey, Davis, Stupak, Green, McCarthy, Strickland, and Dingell (ex officio).

Members present, Subcommittee on Telecommunications and the Internet: Representatives Upton, Stearns, Cox, Cubin, Shimkus, Wilson, Bass, Walden, Tauzin (ex officio), Markey, McCarthy, Davis, Boucher, Eshoo, Stupak, Engel, Wynn, Green, and Dingell (ex officio).

Also present: Representatives Burr and Holt.

Staff present: David Cavicke, majority counsel; Ramsen Betfarhad, majority counsel; Shannon Vildostegui, majority counsel; Will Nordwind, majority counsel; William Carty, legislative clerk; Gregg Rothschild, minority counsel; Jonathan J. Cordone, minority counsel; Peter Filon, minority counsel; and Nicole Kenner, minority research assistant.

Mr. UPTON. Good afternoon. Pleased to hold this joint subcommittee hearing today with my good friend Cliff Stearns, Ed Markey and Jan Schakowsky. Today's hearing is entitled, "Legislative Proposals to Combat Spam."

I would note that when I returned from our July 4 break, I found dozens of spam e-mails on my system last night, 3 or 4 times the normal for not cleaning it up for a couple of weeks. This is a watershed moment for the Congress, and if we work together as a Congress, I am confident that after many years of fits and starts we may finally be in a position to respond to our constituents' plea for help in protecting their in-boxes from a flood of annoying junk e-mail and, more disturbingly, the offensive smut.

Efforts in the last couple of Congresses have fallen short, particularly because of squabbles between committees of jurisdiction. At

the end of the day, we have had some terrific debates about combating spam but the bills have just died. Meanwhile, spam has proliferated, consumers patience has worn thin, and the volume of spam threatens to clog the arteries of the Internet.

I know every member of this committee and these subcommittees wants to combat spam. Vice chairman of this full committee, Mr. Burr, has introduced legislation, H.R. 2214, which would, at its core, empower consumers to opt out of receiving commercial e-mail. I would note that Mr. Burr's bill not only has the support of Chairman Tauzin, Mr. Stearns, myself and others but even more—well, maybe not more significantly but certainly important, the Judiciary Chairman, Jim Sensenbrenner. This is indeed a major development and bodes well for our efforts to once and for all move beyond the dead bills and committee squabbles of the past, get legislation to combat spam signed into law.

I also want to commend Mr. Green and Mrs. Wilson for introducing their legislation, H.R. 2515. I was pleased to see that when this bill was unveiled it contained so much common ground between it and the Burr-Sensenbrenner-Tauzin bill. Indeed, both bills apply opt-out to all commercial e-mail. Both bills rely upon the FTC, the DOJ, State AGs and ISP private rights of action for enforcement. These bills are not that far apart, and I am convinced that the gaps can be bridged. Both bills got sequential referrals to the Judiciary Committee, so it is imperative that we avoid the inner committee pitfalls of the past if we are going to deliver for the American people. Based on the fine spadework of Mr. Burr, Tauzin and Sensenbrenner to reach significant accommodation between the two committees prior to the introduction of the bill, I believe to their credit we are much closer to the goal line than ever before. Mr. Green and Mrs. Wilson's proposal are very similar in many respects, which I view as a further good sign that Mr. Burr, Chairman Tauzin and Sensenbrenner came pretty close to hitting the sweet spot.

Of course, like every other bill, H.R. 2214 was introduced with the expectation that it likely would be perfected along the way through the legislative process. That is what hearings, markups, and house floor consideration—not to mention the conference with the Senate—are for. Mr. Green and Mrs. Wilson's bill provides some suggestions on where we can improve our product, and I suspect that we will hear about some of those today. For instance, we can tighten definitions to ensure that we close down any potential and unintended loopholes.

I also support expanding AG enforcement to cover not only the fraud provisions of the bill but also instances where marketers fail to put required inclusions in their e-mails and where marketers fail to honor consumer opt-out requests. I also think that we can beef up the monetary caps and aggregate caps on State AG recoveries, and I pledge to continue working with all members of this committee in a bipartisan manner to make these and other productive improvements upon the final product as we continue to work in a cooperative fashion with the Judiciary Committee.

To paraphrase my old boss, Ronald Reagan, it is amazing what we can done if you don't worry so much about who gets the credit. When it comes to combating spam there is plenty of credit to go

around in this committee on both sides of the aisle as well as in the Judiciary Committee too. Mr. Burr, Mr. Green, Mrs. Wilson, so many others deserve such credit. So if we can just learn from the past, work together, avoid the pitfalls, I am confident we will succeed in delivering anti-spam legislation to the American people before too long. At this point I yield to my friend from Massachusetts—maybe I don't yield to him—Mr. Markey, for 5 minutes for an opening statement.

Mr. MARKEY. I thank the chairman very much. This is the second round for me in a battle against spam, and the last round was very bitter, it was a multi-year fight, but, ultimately, I was successful. Because spam is to the Internet what Spam has been to culinary critics for years. For years, millions of little kids, and that was my brothers and I in our house in the 1950's, my mother was constantly serving unsolicited Spam to my brothers and I.

And telling us it was good for us and telling us just because she had a monopoly and just because she controlled the capacity to Spam my brothers and I sometimes 3, 4 times a week, always unsolicited. And we as consumers had very little ability to protect ourselves successfully when we were 8 or 9, but by the time we were 11 or 12 and we were able to organize better, we ultimately were able to just stop the scourge of Spam. Now, once again, spam raises its ugly head and consumers out there are looking for relief from unsolicited invasions, especially in the privacy of their home where they should have more control over what it is that has allowed entry into that sacred domain.

I want to salute the principal sponsors of the spam legislation that I have cosponsored which has been offered by Mrs. Wilson and by Mr. Green. I think it is important for us to work with the other members who are working on other approaches on this legislation, the chairman and others. This committee approved spam legislation authored by our two colleagues in the previous Congress, and I believe the bill they have introduced in this Congress is an improvement over previous versions. It is sensible regulation of certain Internet-based conduct and includes realistic but tough enforcement measures. It will help to preserve the best of what the Internet offers consumers and to businesses while helping consumers and industry stem the tide against the daily deluge of unsolicited commercial e-mails.

One issue I want to highlight that I believe the Committee ought to tackle as well is wireless spam. As wireless technology advances and becomes like the traditional phone networks and network for sending data, text and images in addition to voice services, it is predictable that spam will migrate to wireless services. When a computer user logs on in the morning and finds 150 spam e-mails and has to spend time deleting all of these items, it is a clear nuisance. Think about the prospect of driving home and having your wireless phone ring and buzz as all of these spam e-mails arrive. It will be spam that follows you wherever you bring your phone. It will be even more of a nuisance and more burdensome to consumers to the extent to which they may pay their wireless phone company based upon the number of text messages received or sent. This is a future that is right around the corner unless we act. It also has become the plague of millions of wireless users in Asia and

other parts of the world. Our colleague, Rush Holt, has also introduced legislation that aims to address this issue. I believe that we can tailor a remedy for wireless spam that recognizes that spam to a wireless phone is even more intrusive than it is to a desktop computer.

I look forward to working with all of my committee colleagues on addressing this issue as we attempt to reach a consensus committee position on the underlying issue. Again, I want to commend you, Mr. Chairman, Chairman Stearns, and I look forward to working with Chairman Tauzin and Mr. Dingell and the other members on this very important legislation.

Mr. UPTON. Okay. I now yield to the chairman of the Subcommittee on Commerce, Trade, and Consumer Protection of which we have having a joint hearing, Mr. Cliff Stearns from Florida.

Mr. STEARNS. I thank my colleague from Michigan and I welcome the witnesses and I am pleased to co-chair this with my colleague, Mr. Upton.

I think no one disputes the great value of e-mail. It has brought efficiency and productivity to all of us and helped us in a short period of time, and it has become critical, ubiquitous, inexpensive and a very effective medium of communication. It is a communication medium that at least according to one survey 75 percent of us are not willing to forgo for even telephone service. The evidence that e-mail is indeed the killer application of the information and knowledge age can be found simply in our routines, our daily routines at work or play, where routinely, like Mr. Upton indicated, is going through our e-mails and deleting what we have to do.

But, of course, a lot of this is filled, our e-mails are filled with unwanted e-mails asking us to buy certain products ranging from the real products to the absurd. I guess I personally don't have a problem with the marketing per say. After all, a consumer-based economy is highly dependent on marketing to differentiate the array of goods that we have and services to the consumers. But I think the problem is twofold after you look at it from there.

First, the marginal cost of sending the additional e-mail is just about zero. Senders of commercial e-mail have no incentive to target their marketing. Thus, the networks and systems that support e-mail are flooded with these e-mails. Recent estimates suggest that as much as half of all e-mails are composed of such commercial solicitations. Now, someone bears the cost of this voluminous unwanted solicitations, and of course that someone, ultimately, is the consumer, the user of e-mail. We will pay, as the e-mail service providers buy more equipment. They will pass it on to us. We will also pay, all of us, in lost time and productivity—the time we have to go through and delete those all these e-mails.

The second problem that I see is that e-mail communications make accountability a lot more difficult. Unscrupulous people use it to advance fraudulent and deceptive acts, and even good commercial actors are tempted to take advantage of this lack of accountability.

So I think targeted legislation that can bring about a greater level of accountability to e-mail communications is good. I think H.R. 2214 is that bill. It enjoys the support of a lot of members, including the chairman of this committee as well as the chairman

of the Judiciary Committee, which is very important. This type of cross-committee cooperation is very important. It is necessary in order for us to enact finally this legislation on spam. I am also pleased that some of the leading voices for anti-spam legislation, indeed pioneers in this effort, colleagues on my committee, are also interested in trying to work through and pass legislation finally. I am particularly talking about the gentlelady from New Mexico, Ms. Wilson, and my colleague, Mr. Green and Mr. Boucher. So we have an opportunity for a bipartisan bill.

I believe that effective Federal legislation should bring about greater accountability as a bottom line. That greater accountability can be achieved by strengthening existing laws—making sure that fraud and deception is prosecuted and subjected to severe penalties. In addition, I think that legislation should encourage accountability through adoption of certain best practices by e-mail marketers. I know a number of witnesses today have their own thoughts on this issue. I have a proposal that I think would advance best practices in the market and in turn inject greater accountability. So I hope to discuss this proposal later.

In conclusion, with an observation I think that our witness will probably confirm, legislation is only one part of the solution. I think many of you on the witnesses out there could propose a technical solution. Technology, consumer education, industry cooperation, in my view, are the key tools in combating spam and injecting real and effective accountability. We must also consider the transnational dimensions of spam. It is an international problem that will require increased international cooperation to combat. So I hope to introduce bipartisan legislation before August recess that would strengthen the Federal Trade Commission's ability to address the growing problem of transnational fraud, including spam that is not home grown. Thank you.

Mr. UPTON. At this point, I would recognize the vice chair of the Subcommittee on Commerce, Trade and Consumer Protection, the gentlelady from Illinois, Ms. Schakowsky.

Ms. SCHAKOWSKY. Ranking, actually, but that is good.

Mr. UPTON. I am sorry.

Ms. SCHAKOWSKY. No, that is all right.

Mr. UPTON. I am sorry, the ranking member.

Ms. SCHAKOWSKY. No. I thank——

Mr. UPTON. We thank you all on this side of the aisle. We will get that voter registration changed in Illinois.

Ms. SCHAKOWSKY. I thank Chairman Upton and Chairman Stearns for holding this hearing today on spam. I wanted to ask unanimous consent to place in the record a statement by Congressman Rush Holt, which focuses on wireless spam.

Mr. UPTON. Without objection.

[The prepared statement of Hon. Rush Holt follows:]

PREPARED STATEMENT OF STATEMENT OF HON. RUSH HOLT, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEW JERSEY

I am pleased that the Subcommittees have convened this joint hearing to explore ways to address the mounting problem of unsolicited e-mail advertising, or spam, which has become perhaps the biggest nuisance of the Information Age.

I urge the committee to include in their legislation provisions to combat a related problem that has gotten out of hand in some countries and is growing ever worse in the U.S.—spam sent to wireless phones through text messaging.

The Japanese are already fighting off a tsunami of cell phone spam. On one recent day, the 38 million customers of the largest Japanese wireless company, NTT DoCoMo, received 150 million pieces of spam. Even today, after passage of anti-spam laws in Japan, DoCoMo's subscribers still receive up to 30 million wireless spam messages each day. This has caused millions of Japanese wireless phone users to simply stop using their cell phone service.

So far, U.S. cell phone users have been largely spared this torrent of annoying, unwanted messages. I presume this is because a lot of telemarketers don't believe there are enough text-capable cell phones in the country. Most new phones are text capable, however, and the number of text messages sent in this country has been rising rapidly, quadrupling from 250 million messages sent in December 2001 to 1 billion messages sent in December 2002. 17% of cellular customers, about 23 million people, currently use text messaging—including 45% of cell phone users in the lucrative 18-to-25-year-old category. Direct marketers are already beginning to salivate.

I have introduced the Wireless Telephone Spam Protection Act as H.R. 122. This bill is intended to launch what could be called a preemptive attack against wireless spam before it spins out of control in the United States. Congress too often acts once the fire is already lit. This time, we should put the fire out before it gets out of control.

I want to emphasize that not only should anti-spam legislation incorporate wireless spam, it should also set stronger penalties and consumer protections. Under most wireless plans, consumers pay for each message they receive—they're paying to be spammed. That is why consumers should not have to opt out of text message spam after they've already received it, but instead should only receive those messages they choose to get.

Mr. Markey has recognized the importance of addressing the wireless spam problem, and he has informed me that he intends to address it during markup. I want to express my appreciation to Mr. Markey for his efforts and for all of his leadership on telecommunications issues.

I hope we can stop the wireless spam tsunami before it floods us all.

Ms. SCHAKOWSKY. My constituents have contacted me about how much they hate spam, and it is important to note that spam is more, however, than just a time-consuming nuisance to people. A great deal of spam is fraudulent and obscene. According to the Wall Street Journal and Reuters, 50 percent with children with e-mail accounts receive e-mail with pornography. Under the current law, parents are virtually powerless to stop their children from receiving inappropriate and disturbing solicitations. We need to give parents the tools to protect their children. First Amendment rights need to be protected, but predators that target our children and grandchildren must be prevented from contacting them in the first place.

Spam has also provided enormous opportunities for scam artists. Shamefully, many spammers take advantage of senior citizens and children. This past April the FTC released a report analyzing false claims made in spam. The FTC analyzed 1,000 pieces of spam and found that 66 percent contained deceptive information. The FTC and State law enforcement agencies need broader enforcement authority to go after all bad actors regardless of where they make their pitch—from the Internet, on television or in the newspaper. Cyber criminals need to be held accountable.

It is important to note that spam is a problem that extends far beyond fraudulent and obscene. We are all overwhelmed with solicitations for loans and various products and Viagra. Consumers do not want to receive e-mails from these businesses. Maybe some do but those who don't should be able to opt out of receiving future solicitations if they wish. Unwanted spam also hurts our economy.

It clogs networks and it causes entire networks to crash. Experts estimate spam will cost U.S. businesses over $10 billion this year. The problem will only get worse over time. According to industry experts, the volume of spam rose from 8 percent of all e-mail in January 2001 to 45 percent in 2003. Spam is likely to exceed 50 percent of all e-mail by 2004. It is clear it is a major problem. The question is what can we do to help our constituents and stop spammers from sending unwanted solicitations while at the same time ensuring that e-commerce remain vibrant.

Spam is a very difficult problem to solve partly because it is hard to track down many of the culprits. A great deal of spam is sent from abroad, and many spammers do not have fixed addresses, are difficult to track down. But I am glad that we are taking action. I am a co-sponsor of 2515, the Anti-Spam Act of 2003, and I support the bipartisan bill because it gives the FTC and State attorneys generals strong enforcement powers, has a comprehensive opt-out provision and has a clear definition of what types of commercial e-mail should be regulated. I want to just list a couple of concerns, though, that I have about 2214 in its current form and hope that they can be worked out.

One, it limits the amount of damages that an attorney general can pursue from the spammer that violates the law. Second, it prevents from States from enforcing the opt-out list. Third, it forces the FTC to establish a knowledge standard before issuing an injunction. Fourth, it applies only to e-mails that have a solicitation as a primary purpose, and I am afraid companies will be able to bury solicitations in their e-mail, that people will find the loopholes.

So I look forward to working with all my colleagues on both sides of the aisle on this problem. We were able to do the do not call list and that helped the FTC and passed legislation that helped the FTC to implement it. We have gotten an overwhelming positive response and now it is time to tackle spam. It is clear that we need to take action before the problem gets worse. Thank you, both chairman.

Mr. UPTON. I recognize the chairman of the full committee, Mr. Tauzin from Louisiana.

Chairman TAUZIN. Thank you, Chairman Upton, and thank you, Chairman Stearns, for holding this important joint hearing today. I wish that Mr. Markey was still here because once again today I have to defend—oh, you are here, you are back—I have to defend someone against another unfair, unwarranted, unreasonable political attack, this time the mystery meat known as spam. I heard you, Mr. Markey, talk about how growing up you and your brothers were subjected to unwarranted and unwelcomed and unsolicited adventures with the mystery meat known as Spam. That never troubled me as a young man. Before there was trail mix, before there was power bars, as a young hunter and fisherman there was Spam, and we loved it and enjoyed it and still do. What upset us the most was powdered meat. Now, that really—I never could understand—I mean if you want meat, you should get meat, you should not get powder. I never understood that when I was a child.

Mr. MARKEY. Yes. Well, we didn't have those cajun spices that kills the taste, you see. I mean in an Irish home you eat it straight. There is no extra——

Chairman TAUZIN. Yes, meat and potatoes, I know. And then the other thing that really got us was Vienna sausage, I mean unsolicited Vienna sausage. Why Vienna? I mean we had Aunt Doolie sausage, we had great venison sausage, we had every kind of sausage you can imagine.

Mr. UPTON. Did you have a cat or something?

Chairman TAUZIN. Huh?

Mr. UPTON. Didn't you have a cat or something that could eat some of that?

Chairman TAUZIN. I thought you were saying something else.

Bottom line is we had other things to object to besides the mystery meat, Spam, and I want to defend it; it is still a good product. But when it comes to unsolicited e-mails spam is obviously a scourge.

If our house is our castle, our castle is under siege right now, it really is. I mean we have gone after some who have put it under siege. We helped pass the telemarketing do not call list and Americans are calling like crazy to get on that list and to stop unwarranted, unsolicited telemarketing calls. We have allowed every citizen in the country to call the post office and stop the junk mail from hitting my mail box. We can say no to unwanted visitors, to unwanted telemarketing calls. We can say no to unwanted postal mailings into our mailbox. It is time we give Americans a chance to say no to unwanted e-mails. It is that simple. And the bills we are working on are going to do that and give Americans a new right.

And we have finally got concurrence with the Judiciary Committee, we are working on a common product. I really want to thank Mr. Burr and Mr. Upton and Mr. Stearns and all the members who worked to negotiate that product with the Judiciary. I want to thank Mr. Dingell, and I particularly want to thank Ms. Wilson for their assistance in these negotiations. They are still going on, we are still getting concessions. I think we are getting closer and closer to a final product that is going to join the Wilson-Green effort with the effort our two committees are making, and instead of having a product that is blocked at another committee from getting to the floor, now we will have a joint committee product. We will have a product on the floor, and the Senate is likely to pass the product. We are likely to get some real action on this issue this year, and I want to thank you all for it. I particularly want to commend Ms. Wilson for again being an outstanding leader on this issue as she was last year, last Congress, and to commend all of you for recognizing that this is not going to happen if we fight committee battles over it. It is going to happen when we all come together.

I particularly want to point out the three features of this bill quickly. It creates consumer choice for the first time in this area, it has got huge new anti-fraud provisions. And by the way, we have been improving them in these negotiations, including new rights for the AGs of our State, strong enforcement provisions, and as Mr. Markey pointed out, it begins to do something now about a problem

that has already hit Europe, already hit Asia, it is really big in the common market already, and that is the problem of wireless spam, which we expect is going to be a huge problem in this country if we don't cut it off in its tracks. And we have begun that process in this bill.

So when you think about the fact that this bill is now coming together in such a great bipartisan way and more importantly between our two great committees of Judiciary and Commerce, we have got a real chance to give consumers a real chance to defend their Internet castle from this siege that so many are under.

I have been asked is this an attack on the First Amendment, the free speech amendment? It is not. This is about the right to listen or not listen. Husbands understand that. We call that selective hearing, and wives get real angry with us when we do it. But Americans have always enjoyed the right to turn it off, not to hear, not to listen. That doesn't affect people's right to speak. They can speak all they want. You don't have to listen if you don't want. What we are talking about in this case is—on the Internet—your right not to receive information you don't want, particularly when it is egregious and offensive information, in many cases, into your home, the same way you can say no to those kind of products when people sought to deliver them over the mail or in a telephone conversation.

So this is a great effort, and I want to thank our two subcommittees for working as closely as they have and for so many of you, Mr. Green, and for so many of you coming together and trying to find a common product. We are going to have one next week, and we will deliver a great victory to the floor, and eventually we will have the signature of the White House and Americans will be better off for it. God bless you. Thank you.

Mr. UPTON. Recognize the ranking member of the full committee, the gentleman from the great State of Michigan, Mr. Dingell, for an opening statement.

Mr. DINGELL. Mr. Chairman, I thank you, and I commend you and Chairman Stearns for holding this hearing today. Spamming, cramming, slamming, they are all unacceptable practices, and I want to say to my colleagues, the chairman of the committee, to the gentleman—rather to the gentlewoman from New Mexico, Ms. Wilson, to my two friends, the chairmen of the subcommittees, Mr. Green, and to the others, including my dear friend Mr. Burr who have worked on this matter. I commend them and I am appreciative of what it is they have done.

I want to observe that this committee has made a significant effort to combat spam. During the past two Congresses we have reported legislation to protect consumers from the increasing amounts of commercial e-mail that fill in their in-boxes. Unfortunately, the legislation has yet to make it to the President's desk. I hope this year will be different. I would note that we are engaged in a discussion with members of the Judiciary Committee because of a rather unfortunate shared jurisdiction on this matter. I would note that the position of the other committee is one which strongly favors a much weaker and much less protective bill of the rights and the concerns of American consumers.

As all of us are aware, the amount of spam clogging the information networks of this Nation has risen several fold since we last considered legislation on this matter. In fact, the volume has increased to such levels that it is degrading the usefulness of e-mail as a quick means of communication. For this reason, the call for action has constantly grown. Indeed, spam legislation now enjoys broad support across the political spectrum, even from industry groups that once opposed it. I am confident that the resolve of this House to pass strong legislation has increased and will grow as the people make their wishes and their concerns known.

Today we find ourselves examining two bills. The first, H.R. 2515, is a strong bill put forward by two of the leaders on this issue: Mr. Green and Ms. Wilson. I am pleased to join with them and a bipartisan majority of the committee who are co-sponsors of the bill on which they are so well leading. The second, H.R. 2214, was introduced by my dear friend, Mr. Burr, along with Chairman Tauzin and Chairman Sensenbrenner. This bill has several unfortunate weaknesses. I remain hopeful that the competing bills can be reconciled into one strong bill. And I want to make clear my affection and respect for the sponsors of all of the legislation I discussed.

Four criteria will tell us whether a compromise bill would provide immediate protection for consumers and would prevent network congestion. First, it must afford State attorneys general and the Federal Trade Commission, FTC, full enforcement authority over each provision in the bill. Lack of enforcement is simply to assure that we pass out nothing but a sham and a fraud. The Burr-Tauzin bill, and I say this with respect for its authors, fails to do this. It is unnecessary and wholly unprecedented to place arbitrary caps on the damages that State attorney generals may seek from serial spammers.

And I have a couple of words to say about serial spammers and folk like that. We have a number of different things in this world for which we have no great affection. One is cockroaches and another is spammers. The Bible doesn't say what we can do about cockroaches, so we regard them as pernicious pests and step on them at every occasion. And it does tell us that we have to be kind to our fellow man. It doesn't say that we have to tolerate them clogging our in-boxes in our different electronic devices with the kind of nonsense and sometimes pernicious stuff that they dispense to their fellow citizens. And so we can step on them at least figuratively by bringing to a halt some of the more outrageous of their practices. I believe that the legislation that we are going to confront today has to address this fact.

Second, the legislation should apply to all commercial e-mail, and it should not contain limiting purposes or limiting primary purpose language that is found in the Burr-Tauzin bill. From a consumer's perspective, spam is spam, and in my experience, consumers find no distinction between good spam and bad spam. They call it all bad spam. The Burr-Tauzin bill would create a new category of legalized spam that would be exempt from the opt-out provision and from State regulation. I don't know anybody except those who would benefit from this that want this kind of arrangement. Smart

marketers would seize this loophole to create spam that fits within this definition and is exempt from law.

Third, the bill should also contain strong language protecting consumers, particularly children, from unwanted sexually oriented e-mail. Only the Wilson-Green bill ensures that consumers will not be required to view offensive material before opting out. This language is then critical and is crucial to a successful piece of legislation.

Fourth, the bill must contain a sufficiently broad definition of affiliates so that consumers are not required to opt out of each affiliates' operation within a giant corporation. Let me take one for example: Citigroup has hundreds of affiliates, and Burr-Tauzin bill would require a consumer to individually opt out of each affiliate. These affiliates are functioning oft-times out of common mailing centers, are functioning together with coordinated operations, but the consumer will be propelled to submit to serial annoyances from each of them and to be like a fellow swatting flies to try and get a little bit of peace.

In contrast, the Wilson-Green bill takes a much more sensible and consumer-friendly approach, one that the American people want. Simply stated, if affiliates can share a consumer's e-mail address, then they can also share that consumer's request to opt out of future spam. Very simple. If they can share it, they have to share two things: One, the address, and, two, the demand of a citizen which must be respected that they stop this nonsense.

In crafting a compromise, we must remember that the twin purposes of this bill are to protect consumers from unwanted e-mail and to help unclog our communications network. A bill that does not provide for strong enforcement or that creates a category of government-sanctioned spam will not achieve either of these important purposes which I strongly support. I would note that it will not stop the flood of filth on the Internet also. I, therefore, look forward to the witnesses' testimony on the two bills, and I urge my colleagues to make ready for a fight. Let us win this and let us stop this nonsense now. Thank you, Mr. Chairman.

Mr. UPTON. The gentleman's time has expired. I would note that we have three votes on the floor, which we will go for 1 or 2 more speakers if we can. But I also remind members that if they defer their opening statement, they will get an extra 3 minutes bonus for their first round of questioning. So let me just start that procedure. Mr. Shimkus?

Mr. SHIMKUS. Thank you, Mr. Chairman. I am going to keep this short and I will take my opening statement. Two things are wrong. Spam delegitimizes the Internet as a viable marketing took, one. And worst of all, it exposes children to content that may be harmful for them to view or see, and that is one of the provisions in my colleague and good friend, Congressman Wilson and Congressman Green's bill that I would like to see become part of the law is that the Centers of Sexually Explicit Material include a warning label that lets the recipient know he or she will be going to a sexually explicit web site. This will help stop the brazen spammers who embed sexual material in the actual content of their e-mails.

This gives me also an opportunity to talk about the dot-kids-dot-us, which Congressman Markey and I and Congress Upton, which

will come online we believe in September, which is a tool to help parents make sure that there is age-appropriate material for their kids when they are going through the web sites. So this is my opportunity to encourage all of you that don't know about dot-kids-dot-us or you companies in industry and interest groups, that is going to be a good opportunity to make sure your material is—if you want access to kids, that it is going to be suitable for children. So with that, Mr. Chairman, thank you for the time. I yield back.

Mr. UPTON. Okay. Mr. Boucher.

Mr. BOUCHER. Thank you very much, Mr. Chairman. Spam is no longer just a nuisance to consumers. It has truly become an epidemic that carries a large economic cost. Today more than 40 percent of all traffic on the Internet in terms of electronic mail is spam, and it is anticipated that very soon that number will exceed 50 percent. For example, AOL and Microsoft intercept each day more than 2 billion spam messages just between those companies.

A solution is needed that will protect consumers and businesses and punish the abusers. Such a solution must include at a minimum three important factors: Vigorous enforcement, a workable definition of spam and strong consumer protections. First, spammers will not be deterred unless there is strong enforcement. I was recently pleased to join with 29 of our committee colleagues, a bipartisan majority, including Representatives Wilson, Green, Dingell, Markey and others, in introducing the Anti-Spam Act of 2003. Our legislation ensures that Internet service providers, State attorneys general and the Federal Trade Commission are given full authority to enforce vigorously all aspects of the Anti-Spam Act. Legislation without such enforcement is a tiger without teeth and will not stop spam abuse. Any legislation with strong preemption, which this bill, in fact both of these bills contain, must be matched by strong enforcement. Otherwise the States would lose their current authority to act in the consumer interest.

Second, any legislation to reduce spam must define spam broadly enough to include what consumers normally considered to be junk mail. Common sense dictates that spam is commercial e-mail that consumers do not want in their in-boxes. Accordingly, spam legislation must provide consumers with an ability to opt out of any e-mail with commercial content that they do not want. Alternative legislation takes a very narrow approach to the meaning of spam by defining spam as e-mail whose primary purpose is commercial, which, in effect, becomes a legal charter for companies to continue to flood in-boxes and burden ISPs.

Third, the consumer opt-out must be simple and it must be effective. Out legislation does not require a consumer to opt out of each affiliate of a company in order to stop receiving unwanted e-mail. If a consumer does not want to receive a e-mail from a company of all 100 of its affiliates, a single opt out should be effective. The alternative legislation would require the 100 opt outs.

These three factors, vigorous enforcement, a common sense definition of spam and strong consumer protections, are essential as elements of legislation that will be effective in fighting spam. It is my hope that prior to committee markup we will be able to achieve consensus on these matters so that a broadly supported and truly effective measure can be presented to the House, and I look for-

ward to working with our colleagues who are authoring both of these measures in order to achieve that goal. Thank you, Mr. Chairman. I yield back.

Mr. UPTON. Thank you. I would note that we have three votes that are pending. We have 9 minutes left in the first vote. Immediately when the three votes are done we will resume, which I would guess will be about 2:10. So we will stand adjourned.

[Brief recess.]

Mr. STEARNS. The joint hearing of the Subcommittee on Telecommunications and the Internet and the Subcommittee on Commerce, Trade, and Consumer Protection will reconvene, and we will continue with the opening statements. The gentleman from California, Mr. Cox.

Mr. COX. Thank you, Mr. Chairman. I want to welcome back our panel and thank you for your forbearance during our floor votes. It is a very distinguished panel and we look forward to hearing from you. I want to thank you, Mr. Chairman, thank Chairman Upton as well for holding this important hearing on a maddening problem for all of us.

Anyone who uses the Internet appreciates the time that our esteemed panel has devoted to studying this issue. Thank you also to Chairmen Tauzin and Sensenbrenner and of course Mr. Burr, the author of H.R. 2214, for your hard work in seeking to stem the rising tide of spam.

I think Mr. Burr and his cohorts in this effort were very wise in choosing not to create a national do-not-spam list. I say that because while I favor such lists in the context of unwanted telephone calls and faxes, the nature of the Internet and more importantly the nature of most egregious spammers strongly suggest that offshore operators, criminal organizations frequently running fraudulent enterprises, would simply use the do-not-spam list as a useful list of new e-mail addresses, a fresh set of victims for their unwanted and often repulsive communications.

Speaking of repulsive communications, I would also like to commend the sponsors of H.R. 2214 for creating tough civil and criminal penalties for pornographers who falsify header information. When someone presents a false identity or disguises the content of their e-mail by failing to include a warning label, we should throw the book at them. There are people who like pornography and there are people who abhor it, but no consumer should be misled or tricked by it. For that reason, I intend to work with the sponsors of the bill to go a bit further and apply to e-mail the same standard the law currently applies to physical mail. Congress should outlaw the sending of unsolicited pornography.

The authors of H.R. 2214 also deserve great credit for ensuring that the cure to spam isn't worse than the disease. Specifically, the authors deserve credit for limiting the ability of class action lawyers to profit from spam. We have already seen how unscrupulous trial lawyers have profited handsomely from unwanted faxes thanks to a loophole in the 1991 law that was intended to prevent them. Despite the lawyers getting rich, my constituents still write to me asking for relief from unwanted faxes. The Burr-Tauzin-Sensenbrenner bill wisely focuses its attention on helping consumers rather than simply authorizing lawyers to collect a new litigation

tax. The great strength of H.R. 2214 is that it empowers consumers and Internet service providers, the people bearing the costs of spam in time and in hassle. It will create harsh penalties for those who inflict these costs.

Finally, Mr. Chairman, I would note that spam doesn't have to be commercial to be annoying, to be costly or to be burdensome. Last week, I am sad to report the California Supreme Court in my home State issued a most peculiar ruling that needs legislative correction. The court held that the owner of a private computer network cannot use the law of trespass to prevent an intruder from sending 200,000 e-mails into that network. In this case, the network made repeated requests to the spammer to cease and desist, but the court said it could not find economic harm. I will soon introduce legislation to correct this injustice and ensure that trespassing is trespassing, whether the property is a piece of land or a computer server. I hope that the authors of H.R. 2214 will consider this provision for inclusion in the final mark. I yield back, Mr. Chairman.

Mr. STEARNS. Thank the gentleman. Mr. Stupak?

Mr. STUPAK. Thank you, Mr. Chairman, and I would like to thank both chairmen for holding this hearing today, and I want to welcome our distinguished witnesses. Unfortunately, I will be in and out so I want to make this opening statement now, as I have a number of matters up in my office I have to attend to.

I am concerned that this is now the third Congress in a row that this committee has addressed this issue, held hearings, markups and expressed commitment to combating spam. Yet while the flood of unsolicited e-mails is only growing, ISPs becoming more and more overwhelmed and consumers more aggravated, this committee seems to be moving in the wrong direction.

I commend the chairman of the full committee and Mr. Burr for working on legislation to combat spam, but I am concerned that this bill is weaker than the legislation that has come through this committee in the past. I believe that the bill falls short due to insufficient enforcement and inadequate protection to consumers. Furthermore, we must do all that we can to protect parents and children from harmful pornographic e-mails, and this bill does not provide such protection. This is not the direction in which we should be going. This problem of spam is too big and too expensive to provide piece meal enforcement and inadequate remedies.

Last, I remain concerned that unlike the bills in previous Congresses, this bill, or the bills pending before the committee today, do not contain a private right of action. I co-sponsored the legislation introduced by Representatives Wilson and Green. This bill has a number of—a good number of Democrats and Republicans on this committee in support of this legislation, and I am pleased that efforts were made to strengthen enforcement and provide protection from harmful pornographic e-mail in this legislation. However, unlike the last speaker, I would like to note that I think we should go even farther and provide for a private right of action and in fact for class actions. We must equip all injured parties with the tools they need to take action and ensure that we do not leave consumers out in the cold without an individual remedy. I look forward to hearing from the witnesses today about these bills and

other measures that may be necessary in order to address this growing problem. Thank you, Mr. Chairman.

Mr. STEARNS. I thank the gentleman. I believe the gentlelady from New Mexico, Ms. Wilson. I remind all members that the opening statement is about 3 minutes, and we urge all of you, so we can move forward here because we got a late start because of the full committee markup and we are trying to get to our witnesses who have patiently waited through votes, and so I urge all of you to put it in part of the record if you can. Thank you.

Ms. WILSON. Thank you, Mr. Chairman. I will submit a more complete statement for the record, but I do want to set a little bit the context in which we are meeting here today. Five years ago, Mr. Green from Texas and I started working on then what was a pretty obscure but annoying problem: spam or junk e-mail. In the 106th Congress, we were able to pass the Wilson-Green bill by 427 votes to 1, but the Senate did not take it up. And in the 107th Congress, our bill, H.R. 718, passed this committee by a unanimous voice vote and was scheduled for the floor the week of September 11. In this 108th Congress, we have now introduced H.R. 2515. It now has 56 co-sponsors, including 30 of the 57 members of this committee—10 Republicans and 20 Democrat co-sponsors. A majority of this committee is a co-sponsor of the bill.

What was an obscure issue in 1998-1999 by 2001 started to become a serious problem when it was estimated that 7 percent of all e-mail was junk e-mail or spam and is now overwhelming consumers on the Internet with estimates being 40 to 50 percent of e-mail being spam on the Internet at a cost of some $10 billion per year, all of that cost paid for by the recipients and not by those doing the advertising. Fifty percent of children between 7 and 18 years of age report getting pornographic spam in their e-mail boxes, and we have seen in the last couple of years that the promise of technological solutions have failed. Even if you are blocking 80 percent of the spam with your filtering technology, the 20 percent that is getting through is still overwhelming people's in-boxes. We are now at the tipping point, I believe, where we are actually discouraging use of e-mail, impeding commerce, and e-mail is now becoming not a reliable or useful communications tool.

So what must good policy do? I think it has to have a strong civil and criminal penalties for fraudulent e-mail. We have to make sure that we protect consumers and children particularly from sexually oriented messages. We have to have clear definitions without loopholes on what spam is. If the technical loopholes are the joy of spammers today, we certainly don't want to create legal loopholes for them to be exploited by spammers tomorrow. Consumers have to have a right to say, "No. Take me off your list." And that right has to be respected and enforceable. We have to have strong enforcement mechanisms, particularly if there is no private right of action in the bill.

I think we are at a tipping point. If we don't get strong antispam legislation this year, the problem may rapidly be getting to such a point that only an outright ban or an opt-in approach will be enough. You know, it might be reasonable to ask people for one or two opt-outs a day to protect their rights and protect the rights of free speech, but is it reasonable to ask a consumer to have to

do that 100 times a day? Possibly not, and I think we are rapidly getting to that point where we may have to take more extreme action analogous to the junk fax law if we are unable to get meaningful legislation passed in this Congress.

Spam has become a significant problem that threatens to cripple the Internet and the worldwide e-mail system and it is about time we address it.

Mr. STEARNS. I thank the gentlelady.

Mr. Davis from Florida. The gentleman passes.

Mr. Green? Mr. Green is not here.

Mr. Wynn.

Mr. WYNN. Thank you, Mr. Chairman. I really appreciate you calling this hearing today. Let me just make the observation that combined with our efforts on the do not call list, this effort against spam could make us a truly pro-consumer committee. Spam e-mails are unsolicited advertisements that flood the Internet in an attempt to advertise an issue or product to people who may not otherwise choose to receive it, and cost a tremendous amount of money. It accounts for about 50 percent of e-mail traffic, and this number is only expected to rise. Just today, a staffer said she had received over 78 spam e-mails before lunchtime.

Spam e-mails, as opposed to junk mail, costs the sender very little to distribute, with most of the costs paid for by the recipient through increased Internet access, cost and time. According to the Fight Spam! web site, AOL was receiving 1.8 million spam e-mails from a single company each day until AOL got a court injunction to stop it. Just this one example cost AOL consumers 5,000 hours of connect time daily to discard this spam.

Additionally, fighting spam has emerged as a leading business issue. One reported estimate found that spam cost businesses up to $10 million each year primarily due to the implementation of anti-spam technology and lost productivity. The issue of spam is not simply limited to annoying advertisements. It may also be a catalyst for fraud. An article in the Jefferson City, Missouri News Tribune recently outlined a national spam scam. The sender sent an e-mail to many consumers stating concern over a credit card purchase at Best Buy. The e-mail instructed the individuals to visit a special web site to resolve the situation by entering their credit card and social security numbers. As a result, Best Buy fielded thousands of calls from consumers regarding the fraudulent e-mail and needed to tell them to disregard the message or, if they had already entered their personal information, to notify their banks, credit card companies and the FTC's identify theft program. The scheme cost Best Buy and consumers time and money. Luckily, authorities were able to shut down the web site within 2 hours, however much damage had already been done. The Tribune equated the scam to an electronic hit and run.

I am very pleased to be a co-sponsor of the Wilson-Green anti-spam measure to protect consumers against spammers. This is a measure that would provide effective spam counter measures and enforcement measures against those individuals who fraudulently e-mail consumers. The bill would allow consumers a real opt-out solution and afford the Federal Trade Commission and, importantly, State attorneys general and the Internet service providers

full enforcement authority over the bill's civil provisions, providing a much needed enforcement mechanism.

I look forward to hearing from our panelists and learning more about how we may fight spam and continue our tradition of being true consumer advocates. I relinquish the balance of my time.

Mr. STEARNS. Thank the gentleman. The gentleman from Arizona.

Mr. SHADEGG. I thank the chairman and commend him for holding this hearing. I also commend the chairman of the Subcommittee on Telecommunications and the Internet. I think this is a critically important topic, and I believe it is important that we move legislation as quickly as possible. I will insert my full statement in the record, however, before doing so I want to thank our witnesses for appearing today. I look forward to their testimony, and I want to associate my remarks with those of the gentleman from California, Mr. Cox. I believe in fact we can go a little further in this legislation, and I share his concern about unsolicited pornographic material. And with that I yield back the balance of my time.

Mr. STEARNS. I thank the gentleman.

The gentleman from Texas.

Mr. GREEN. Thank you, Mr. Chairman, and I understand we have reduced our opening statements to 3 minutes, and I will be brief as I can and ask permission to have the full statement put in the record.

Mr. STEARNS. By unanimous consent, so ordered.

Mr. GREEN. My colleague, Congresswoman Wilson and I have been working on this. This is our third term on this, and I want to thank her for the cooperation we have done, and it looks like we are going to be able to pass strong legislation, and that is what I would hope to see. I know that our hearing will talk about the two differences between the Wilson-Green legislation and the H.R. 2214, the Burr bill, and at last count we have at least 25 members of our committee, 10 Republicans and 19 Democrats which I believe is the majority that has co-sponsored our bill, and I hope that after publicly defining clear differences, that the negotiations will continue. We have had some very successful negotiations to reach a consensus committee position.

The Wilson-Green bill is about closing loopholes and putting real teeth in anti-spam policy. We all know the urgency of the problem. It is all over our front pages; in fact, in the latest Consumer Reports talked about how to stop spam. Three sessions ago when we started on this, we thought the—I actually thought maybe technology could deal with it, but we now know that technology can't do it. Otherwise we wouldn't have all the ISPs here interested in passing as strong a bill as possible.

Many of my constituents are lower income and minority folks who draw on these new technologies for communication and information benefits. If people new to the Internet continue to meet these online scams that we have, offensive material and the burden of overwhelming spam, they will be turned off and not take advantage of these new technologies. That is why it is so important.

I would hope to have our principles, one, I think we need to empower the States. The States are doing some really innovative ef-

forts, but at the same time provide Federal solution to the problem of spam. And, ultimately, as the chairman said, do something internationally with our neighbors who also have the same problem. With that, I will yield back my time and will place my statement in the record.

Mr. STEARNS. I thank the gentleman.

The gentleman from California, Mr. Issa.

Mr. ISSA. Thank you, Mr. Chairman. I will be brief. I am pleased to have this opportunity today to discuss the growing problem, the epidemic growing problem of electronic junk mail, or spam. In the years that I spent in the electronics industry and running a small business, I watched the Internet and e-mail grow, but it was only toward the end of my time in the private sector that spam began to become a real and ongoing problem. Today, an entire industry is trying to deal with this problem and doing it without government assistance. The absence of action by this body, both here in this committee and the Judiciary, has led to a problem that can only be resolved by action.

There are products today which through great effort and expense deal with spam somewhat, but they are not available to the common user nor are they likely to be. Products with anti-spam agents, such as surf control, do a very effective job of getting rid of 97, 98, perhaps even 99 percent both of sites that would be offensive and of unwanted e-mail. However, to do this they have to add digital signatures on a daily basis to each and every spam site. This, of course, means that the spammers are working ever harder to try to get ahead of organizations like this, and the cost of doing this continues to rise.

There is no question that this body has the ability to enact digital signatures. We certainly took a lead when we put in the V-chip technology some years ago in order to categorize information. Other suggestions to help deal with this problem include, if you will, sort of a Good Housekeeping seal or a positive enforcement of somebody who in fact agrees not to be a spammer and is checked on that basis.

Many of the pieces of legislation that we will be considering in the days to come attempt to deal with a portion of this product. I am convinced that no one bill has all the answers, that in fact both here at this hearing today and in working with industry and in combining the best features of multiple bills will be the only way that we will succeed in providing the leadership that the government has in harmony with commerce in the private sector. With that, I yield back the balance of my time.

Mr. STEARNS. Thank the gentleman. Mr. Davis? Oh, that is right, you passed. She is not here, Ms. McCarthy. Ms. Eshoo, yes.

Ms. ESHOO. Thank you, Mr. Chairman, and to Chairman Upton and Chairman Tauzin for holding what I think is really one of the more important hearings that we could be having on an issue that is affecting far too many people in this country. And I know that this is going to be a worthwhile hearing given the distinguished panel that is here, including Mr. Hirschman of Digital Impact. The company is in the city of San Mateo which is just outside my congressional district, but I think many of your employees are my constituents, so a special welcome to you here today.

We have to get this right. If we don't, the American people are going to come right back to us. This is not something that is fuzzy or blurred. This is an interruption in their lives every single day. They pay for a service and someone else plays with it and jams their in-boxes. And so we have the responsibility to be very clear in terms of legislation that what we do will be effective and it will be effective because it will be enforced. And most frankly, if we miss the mark on this, I know that we will be asked to come back to square one, because there are too many that are being affected by this.

And the numbers are really staggering. According to E-Marketer, 76 billion spam e-mails will be delivered this year. Fifty percent of kids have received e-mails containing pornographic or sexually explicit information. That is a lot. I mean 50 percent is a lot. And U.S. businesses will spend close to $10 billion to fight spam this year. And marketers are brazenly claiming, and they did this just last week, that the success of the do not call list will drive them to send even more spam, costing U.S. business and consumers even more. So, clearly, it is an issue that we have to address. And why would they do that? Because, obviously, they have been chased away from using one medium, and it is far cheaper, by the way, to do e-mails, to do spam. It is just pennies per thousand.

So I am pleased to be a co-sponsor of the Wilson-Green bill. I think, No. 1, it is important to have many ideas introduced in the Congress, but I think that this is the bill that really comes the closest to resolving things in an effective and very clear way for the people that we represent. I think if the House had passed their bills in either of the previous two Congresses, we wouldn't be facing the spam epidemic that we have today.

So I look forward to questioning the witnesses on the differences between the bills that are under consideration and by my friends, Mr. Burr and Mr. Tauzin. What I am confident of is that I think we can work to iron out the differences. We need your considered opinions today, and that is why hearings are so important here. And I also think that obviously that strong enforcement language is ultimately going to have to carry the day, because if something doesn't have teeth in it, then most frankly it is pretty language but not really worth much than the paper that it is written on.

So welcome to all the witnesses, and thank you to all of the chairmen for having this hearing today. I think it is one of the more important ones that we can have, because I think that this year, not next year but this year, in this Congress we should pass stringent spam legislation. Thank you, Mr. Chairman.

Mr. STEARNS. Mr. Ferguson is recognized.

Mr. FERGUSON. Thank you, Mr. Chairman. I want to thank you, Mr. Chairman for holding this hearing. It is about a matter that faces all of us who use the Internet and all of us who rely on e-mail as an important and a viable form of communication.

Spam isn't only a nuisance, it is a serious threat to the feasibility of the Internet and to children who potentially can be bombarded by graphic images that their parents or anyone in a responsible position would not them to see. The prolific emergence of spam on the Internet is alarming. The estimates range up to 60 percent of all e-mail traffic is unsolicited commercial e-mail, or spam. Forms of

this unsolicited e-mail can vary from advertisements for products to fraudulent scams to pornography. Now, my wife and I have three young kids. They are not Internet users yet, but I hope that they will be someday soon. But I will tell you, I have real serious concerns about them using the Internet and using e-mail if they are going to be subjected to the same sort of bombardment of messages that I know I am and others like me are subjected to.

We have to protect e-mail users against the proliferation of fraud over spam. We have to punish those who invade our e-mail use and people who use misleading header and routing information and those who want to falsify their identify. In short, I believe that we have to do everything we can to curb the overwhelming bombardment that spam has unleased on our in-boxes.

Mr. Chairman, again, I want to thank you for having this hearing, and I look forward to the testimony of our panelists and to hear their suggestions how we can come up with a solution to this growing problem. I yield back.

Mr. STEARNS. The gentlelady, Ms. McCarthy?

Ms. MCCARTHY. Mr. Chairman, thank you very much for this important hearing, and I thank the witnesses too for taking time to come before us and share their wisdom on this important issue. I served in the Missouri State legislature for 18 years before coming to Congress and was very active in the National Conference of State Legislatures, and so I want to assure the panelists and the experts here today and you, Mr. Chairman, that, yes, there is a Federal rule and it is very important nationally and internationally for us to become wise to do what we can to help consumers with this problem, but also have to be in partnership with the State attorney generals who are out there struggling State by State right now trying to put in place something that will work at the State level. And so as we go forward with our legislation, let us also hear from those who have been working with the States so that we are in tandem with what State attorney generals are attempting.

We almost passed a bill successfully in the Missouri legislature this past session, but Microsoft came in and killed it because we will find out why perhaps later today or in the course of our journey, but in any event, Mr. Chairman, this is a very, very important issue, and I am so very grateful to you for having this hearing, and I am grateful to each and every one of you for coming and enlightening us and making us wiser so that we can act in the best interest of the people. Thank you.

Mr. STEARNS. Thank the gentlelady.

Ms. MCCARTHY. Yield back.

Mr. STEARNS. And author of the bill, 2214, Mr. Burr.

Mr. BURR. Thank you, Mr. Chairman. I would like to thank all of my colleagues on the committee for what I think has been a very thoughtful opening statement process so far. Mr. Chairman, we have a very difficult balance to reach. The difficult balance is to make sure we produce a piece of legislation that makes it through the House of Representatives and to accomplish that we have to work with our colleagues in the Judiciary Committee who have not been in the past as open to move legislation, legislation that potentially went too far. I am proud to say that we have worked with them very closely. They have been tremendous partners, as have

Mr. Dingell and many on the minority side as we have tried to negotiate closer on some issues. I am not sure if we can get to closure on all of them, but we are 98 percent of the way there, and I think it explains just how difficult some of the things that we are trying to accomplish are. We don't want this to face a constitutional test down the road on this issue or that issue.

I think there is one thing that we can all agree on. One, we would all like to get the discount airfare offers, we would like to get the discount hotel offers. We never know when they are going to be advantageous to us. We would all like to get rid of the pornography that comes in. And the fact is that those that want to get around what we designed will do it. They are going to find a way to do it. So don't one of us walk away from here and believe that we can create a trap that eliminates all of it, because the only way to do that is to flip the power switch on the back of the computer.

The industry has spent a tremendous amount of money, and they deserve a lot of credit for what they have done to try to filter, but when you have got individuals that intend on getting from point A to point B regardless of how they get there, trust me, at some point they are going to get there. So I think that there is a certain amount that we have to accept that we can't stop. And there is a certain amount that we want to protect that can get there. That is the difficult balance.

I don't perfect to be an expert on this. That is why you folks are here today, and I commend for your willingness. By the same standpoint, I agree with Ms. Eshoo. She has been a good friend, and we have a big responsibility, and we have to get it as close to right as we possibly can. I have worked on a lot of legislation in 9 years. I can't say that I have ever done anything here that is perfect. This will not be perfect. But I also want to make sure that when we complete this process that the House passes a bill this time. And I would urge all of my colleagues to understand that we have other partners, many in the Judiciary Committee, ultimately on the House floor that we have to pass the test with if in fact we want this bill to have a chance to become law. What the American people want is legislation that is signed into law and not something that is just moved through committee and then dies a quick death.

Mr. Chairman, I thank you, Chairman Upton, Chairman Tauzin, Mr. Dingell, and I encourage all of the members of the committee to listen extremely carefully to the answers by these witnesses today. I thank you, Mr. Chairman.

Mr. STEARNS. Thank the gentleman. The gentlelady from California, Ms. Solis.

Ms. SOLIS. Thank you, Chairman Upton. I would like to also thank the witnesses for being here, and I would like to request unanimous consent to submit my statement for the record.

Mr. STEARNS. And by unanimous consent, so ordered.

Ms. SOLIS. And just like to briefly raise a point. In our State of California, we have been very aggressive on this issue of spam, and our Attorney General Lockeer there set up some different provisions and actually went out and filed a first lawsuit in L.A. County. He has also been criticized because we haven't gone far enough. So, certainly, the State solutions that are being offered I think in 30 States probably isn't enough, and we do need to find a Federal so-

lution, so I hope today in listening to the comments that we hear from all of you that we will come up with some genuine ability to start looking at how we can address this issue. So thank you, Mr. Chairman.

Mr. STEARNS. I thank the gentlelady.

Ms. Cubin?

Ms. CUBIN. Thank you, Mr. Chairman. I don't have much to say about the subject that hasn't been said by other members, but I would like to share an excerpt of an e-mail that I received from a constituent that I think typifies the problem that people are facing all across the country. Jeannie Wright from Douglas, Wyoming wrote to me, "Dear Representative Cubin, I am writing in support of the idea to stop the ocean of pornographic e-mail. At my work address, I receive approximately 30 such messages per week. Having never been a viewer of pornography, you can imagine my disgust at receiving messages in which explicit photos automatically appear. You don't have to click on anything, they just appear on the screen. For instance, last week, my daughter and a client were in my office when a photo of a sexual act appeared on my screen as I was searching for a work-related message I had been expecting. How very embarrassing for me and the client and what a lot to try to explain to my 8-year-old daughter, not to mention my boss. These messages make me feel like a victim.

Nasty people I do not know and to which I cannot respond are sending me sexually explicit garbage at the place of my work. Many of the messages offer you a link to unsubscribe. Only about 5 percent of those links are legitimate. The rest do not exist. When I try responding to the e-mail messages, those addresses cannot be found, and the e-mail comes back to me. There is no identifying information on these messages, so I can't even call a phone number and demand that it be stopped. I am afraid to log onto the web sites suggested by the e-mails for fear I will appear on another spam list and receive even more. For now, my only answer is to continue receiving these messages."

This is clearly a troubling situation, and the Congress has been called upon to act. Making hardworking, taxpaying, law abiding moms and dads explain the smut that appears on their computers to their children and their colleagues should not and cannot be tolerated. Mrs. Wright, like many who have contacted their representatives, ought not feel like they are victims. Instead we need to empower Americans to stop the madness. Giving folks the tools to stop the onslaught on the in-boxes is the right thing to do. We already have enacted a national do not call registry, and the same principles of consumer empowerment are incorporated into these antispam bills.

Additionally, I intent to extend these principles to unsolicited faxes by introducing legislation to update the law to require more information and clear opt-out instructions for recipients of junk faxes. I look forward to hearing our witnesses, and I thank you for your patience and your time waiting for us today. I yield back.

Mr. STEARNS. Thank the gentlelady. Mr. Engel, the gentleman from New York.

Mr. ENGEL. Well, thank you, Mr. Chairman. I want to start by expressing a bit of frustration that we find ourselves here again.

Obviously, this is not a new issue; in fact, as Ms. Wilson pointed out, in the 106th Congress the House passed a version of the Wilson-Green bill of which I am proud to be a co-sponsor, and this committee passed the Wilson-Green bill in the 107th. The only difference today is the sheer volume of unsolicited commercial e-mail, or spam, that exists. It is a staggering 9.3 billion messages per day.

I just wanted to point out three parts of the Wilson-Green bill that make it a better bill than the others. First are the enforcement provisions for State attorneys general. Simply put, the Wilson-Green bill allows them to do their jobs. Provisions of the Rid Spam Act basically mean the attorney general of New York, my home State, would never pursue such a case. Why? Because of the $1 million cap. The fact is New York is a much more expensive place to live and work. Such a restriction especially in these difficult financial times with the States would make pursuing such litigation a poor use of taxpayer dollars.

The Wilson-Green bill also gives the ISPs greater power to pursue the culprits who are degrading their networks. We all know this is not like the U.S. postal system where direct marketers pay for the use of the system. This is in fact the opposite. A spammer can send thousands of messages for pennies. The true cost is borne by the companies that maintain the network infrastructure, from the telephone and cable lines the data travels on, to the computers that the e-mails land in. The ISPs are being hurt, and we have an obligation to update our Nation's laws to provide them with tools to protect their investment.

A second issue is one of fairness to the consumer. When a consumer opens a bank account at Citibank, Citibank can share that person's information with its affiliates, such as its credit card system, to market to that person. It is not too much that if that person, one of our constituents and a client at that bank, indicates to Citibank a desire not to receive unsolicited commercial e-mails, that Citibank puts that into the information it shares with its affiliates. And thus the do no spam request follows through.

Finally, the last thing I will mention, and it is not a small issue, as my colleagues have also mentioned, is the sexually explicit e-mails. They are obviously disgusting and my constituents are fed up with them. Wilson-Green adopts the tried and tested and proven approach of the postal system, a blank e-mail with just a link similar to how it goes through the postal system. The Rid Spam Act only requires an indication that sexually explicit material is part of the e-mail, but the e-mail could include sexually graphic pictures. That is simply not good enough.

I regret that we still find ourselves debating this issue. I deeply regret that instead of easily passing such an important bill we are now devolving into two camps. This is a very troubling development. It is my fervent hope that we will work—the chairman will work with Mrs. Wilson, Mr. Green and Mr. Dingell to find common ground and move a bill expeditiously. And I yield back and I thank you.

Mr. STEARNS. I thank the gentleman, and I believe the gentleman from New Hampshire is going to forego his opening statement, so with great expectation we bring up the panel. Mr. Howard Beales, Director, Bureau of Consumer Protection, the Federal

Trade Commission; Mr. Charles Betty, president and CEO of Earthlink; Mr. Charles Curran, assistant general counsel, America Online; Mr. Ira Rubinstein, associate general counsel, Microsoft Corporation; Mr. Paul Misener, vice president for Global Policy, Public Policy, Amazon.com; Mr. Kenneth Hirschman, vice president and general counsel, Digital Impact; Ms. Paula Selis, senior counsel, Washington State Attorney General; and Mr. Christopher Murray, legislative counsel, Consumer Union. Welcome, all of you, and we will just start with Mr. Beales, from my left to my right.

STATEMENTS OF J. HOWARD BEALES III, DIRECTOR, BUREAU OF CONSUMER PROTECTION, FEDERAL TRADE COMMISSION; CHARLES GARRY BETTY, PRESIDENT AND CEO, EARTHLINK; CHARLES CURRAN, ASSISTANT GENERAL COUNSEL, AMERICA ONLINE; IRA RUBINSTEIN, ASSOCIATE GENERAL COUNSEL, MICROSOFT CORPORATION; PAUL MISENER, VICE PRESIDENT FOR GLOBAL POLICY, PUBLIC POLICY, AMAZON.COM; KENNETH HIRSCHMAN, VICE PRESIDENT AND GENERAL COUNSEL, DIGITAL IMPACT; PAULA SELIS, SENIOR COUNSEL, WASHINGTON STATE ATTORNEY GENERAL; AND CHRISTOPHER MURRAY, LEGISLATIVE COUNSEL, CONSUMER UNION

Mr. BEALES. Thank you, Mr. Chairman and members of the subcommittee. I am pleased to be here today to discuss the challenges presented by bulk, unsolicited commercial e-mail, better known as spam. Protecting consumers' privacy has become a principal focus of the FTC. Consumers are concerned about their privacy, including unwanted intrusions into their daily lives. Spam is one of the biggest such intrusions. Everyone enjoys reading the e-mail they want, whether messages are from friends or news about a sale at your favorite store. Today, though, our in-boxes are clogged with unwanted, objectionable and fraudulent messages. Spam is threatening to destroy the benefits of e-mail.

Two factors make spam different from other forms of marketing. One is that unlike telemarketing or direct mail with e-mail it is very easy to hide one's identity or to cross international borders. E-mail can be sent from anywhere to anyone in the world without the recipient knowing who sent it. The cost structure of e-mail is another difference between spam and other forms of marketing. Sending additional spam costs the spammer little or nothing. Instead, recipients and Internet service providers bear most of the costs.

The problems caused by spam go well beyond the annoyance it causes to the public. These problems include the fraudulent and deceptive content of most spam messages, the sheer volume of spam being sent across the Internet and the security issues raised because spam can be used to disrupt service or as a vehicle for spreading viruses. In February of 2002, we announced the FTC's first systematic crackdown on deceptive spam. Since then we have tackled spam on three fronts: Law enforcement, education and research. To date, we have announced 54 law enforcement actions targeting deceptive spam, and the staff continues to investigate and prepare new cases. Among other unfair and deceptive practices, we have challenged spoofing, the practice of forging the from

line in an e-mail to make it appear that the e-mail was sent from an innocent third party. We challenged that as an unfair practice. We have also challenged deceptive subject line information, false remove-me representations, false representations that a service could stop spam from other sources, false claims that buying a spamming business opportunity could make you rich.

The Commission has also been active in business and consumer education efforts and with its research efforts. As you know, we recently conducted a 3-day spam forum to explore and encourage progress toward potential solutions to the detrimental effects of spam. The consensus of all participants in the workshop was that a solution to the spam problem is critically important but cannot be found overnight. There is no quick or simple silver bullet; rather, solutions must be pursued from many different directions: Technological, legal and consumer action.

Right before the forum we announced the FTC spam study. Only 16.5 percent of the spam we analyzed advertised a legitimate product in a legitimate manner; that is, without clear indicia of falsity. We also conducted the remove-me surf to examine removal representations in spam. Contrary to the belief that responding to spam guaranteed that you would receive more of it, 63 percent of the removal links and addresses in our sample simply did not function. Additionally, in our spam harvest, we examined how computer harvesting programs pick up consumers' publicly posted e-mail addresses leading to, you guessed it, more spam.

We have used our research findings to develop informative, high impact materials to educate consumers and businesses on spam. Our spam web site has a wealth of information about how to avoid spam in the first instance and what to do if you receive it. There is no single cure for spam. Instead, a balanced blend of technological fixes, business and consumer education, legislation and enforcement will be required.

Today's focus, obviously, is on legislation. There are three issues that any spam legislation must confront to effectively deal with the spam problem. First, legislation must address how to find the person sending the spam messages. Although technological changes will most effectively deal with this issue, we have proposed several procedural legislative changes that can provide some assistance in our law enforcement investigations. Second, legislation must deal with how to punish the person sending the spam messages. Civil penalties and possibly criminal sanctions would help address this issue. Finally, legislation must determine what standards will govern non-deceptive, unsolicited commercial e-mail. These standards should include clear identification of the sender of a message and empower consumers to end the flow of messages that they do not wish to receive.

Our written testimony and our earlier reauthorization testimony set forth specific legislative changes that we would welcome along with several important principles that potential spam legislation should consider. E-mail provides enormous benefits to consumers and businesses as a communication tool. The increasing volume of spam coupled with its widespread use as a means to perpetrate fraud and deception put these benefits at serious risk. We look forward to continuing our research, education and law enforcement ef-

forts to protect consumers and businesses from the onslaught of unwanted messages. We appreciate the opportunity to describe our efforts, and I look forward to your questions.

[The prepared statement of J. Howard Beales III follows:]

PREPARED STATEMENT OF J. HOWARD BEALES III, DIRECTOR, BUREAU OF CONSUMER PROTECTION, FEDERAL TRADE COMMISSION

Mr. Chairman, the Federal Trade Commission appreciates this opportunity to provide information to the Committee on the agency's efforts to address the problems that result from bulk unsolicited commercial email ("spam"). This statement discusses the Commission's law enforcement efforts against spam, describes our efforts to educate consumers and businesses about the problem of spam, and focuses particularly on the Commission's recent Spam Forum and several studies on the subject that the Commission's staff has undertaken in recent months. It also discusses legislative ideas to enhance the Commission's effectiveness in fighting spam.[1]

As the federal government's principal consumer protection agency, the FTC's mission is to promote the efficient functioning of the marketplace by acting against unfair or deceptive acts or practices and increasing consumer choice by promoting vigorous competition. To fulfill this mission, the Commission enforces the Federal Trade Commission Act, which prohibits unfair methods of competition and unfair or deceptive acts or practices in or affecting commerce.[2] Online commerce, including unsolicited commercial email, falls within the scope of this statutory mandate.

The problems caused by unsolicited commercial email go well beyond the annoyance spam causes to the public. Indeed, these problems include the fraudulent and deceptive content of most spam messages, the offensive content of many spam messages, the sheer volume of spam being sent across the Internet, and the security issues raised because spam can be used to disrupt service or as a vehicle for sending viruses.

FTC SPAM FORUM

Building upon our research, education, and law enforcement efforts, the FTC held a three-day public forum from April 30 to May 2, 2003 on spam email. This was a wide-ranging public examination of spam from all viewpoints. The Commission convened this event for two principal reasons. First, spam is frequently discussed, but facts about how it works, its origins, what incentives drive it, and so on, are not widely known. The Commission anticipated that the Forum would generate an exchange of useful information about spam to help inform the public policy debate. This could help the Commission determine what it might do to more effectively fulfill our consumer protection mission in this area. Second, the Commission sought to act as a potential catalyst for solutions to the spam problem. Through the Forum, the Commission brought to the table representatives from as many sides of the issue as possible to explore and encourage progress toward potential solutions to the detrimental effects of spam.

Virtually all of the panelists at the Commission's recent Spam Forum opined that the volume of unsolicited email is increasing exponentially and that we are at a "tipping point," requiring some action to avert deep erosion of public confidence that could hinder, or even destroy, email as a tool for communication and online commerce. In other words, as some have expressed it, spam is "killing the killer app." The consensus of all participants in the workshop was that a solution to the spam problem is critically important, but cannot be found overnight. There is no quick or simple "silver bullet." Rather, solutions must be pursued from many directions—technological, legal, and consumer action. The Forum explored and helped to suggest paths to follow toward solving the spam problems. Such solutions will depend on cooperative efforts between government and the private sector.

---

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

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

The Forum is only the most recent example of the FTC's role as convener, facilitator, and catalyst to encourage that activity. But the Commission also plays another important role—that of law enforcer. For example, the Commission has pursued a vigorous law enforcement program against deceptive spam, and to date has brought 54 cases in which spam was an integral element of the alleged overall deceptive or unfair practice. Most of those cases focused on the deceptive content of the spam message, alleging that the various defendants violated Section 5 of the FTC Act through misrepresentations in the body of the message.[3] More recently, the Commission has expanded the scope of its allegations to encompass not just the content of the spam but also the manner in which the spam is sent. Thus, *FTC v. G. M. Funding*[4] and *FTC v. Brian Westby*[5] allege (1) that email "spoofing" is an unfair practice,[6] and (2) that failure to honor a "remove me" representation is a deceptive practice. In each of these cases, the defendants' email removal mechanisms did not work and consumers' emailed attempts to remove themselves from defendants' distribution lists were returned as undeliverable.

Westby is also the first FTC case to allege that a misleading subject line is deceptive because it tricks consumers into opening messages they otherwise would not open. In other cases, the Commission has alleged that the defendants falsely represented that subscribing to defendants' service could stop spam from other sources[7] or that purchasers of a spamming business opportunity could make substantial profits.[8] Accordingly, these law enforcement actions demonstrate that the Commission has attacked and will continue to attack deception and unfairness in every aspect of spam.

In May 2003, the FTC joined the Securities and Exchange Commission, United States Postal Inspection Service, three United States Attorneys, four state attorneys general, and two state regulatory agencies to file 45 criminal and civil law enforcement actions against Internet scams.[9] As part of this sweep, the FTC brought five federal court actions alleging the deceptive use of spam. In one case, the defendants allegedly used spam with deceptive representations that the email came from well-known entities, such as Hotmail or MSN, to market a "100% Legal and Legitimate" work-at-home opportunity. Although the spam promised consumers they could earn as much as $1,500 a week stuffing envelopes supplied by the defendants, consumers ended up paying $50 for a set of instructions on how to market a deceptive credit-repair manual.[10] In another case, the defendant allegedly used spam to make false and deceptive income claims for a chain-letter scheme dubbed "Instant Internet Empire."[11] A third complaint alleged that defendants used deceptive spam to market an advance-fee credit card scam.[12] In each of these cases, the FTC was able to obtain preliminary injunctive relief and to shut down the operations.[13]

In addition to the law enforcement actions, in this sweep, the FTC and 17 other federal and state consumer protection and law enforcement agencies initiated an effort to reduce deceptive spam by urging organizations to close "open relays."[14] Fifty

---

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

[4] No. SACV 02-1026 DOC (C.D. Cal. filed Nov. 2002)

[5] No. 032-3030 (N.D. Ill. filed Apr. 15, 2003).

[6] "Spoofing" involves forging the "from" or "reply to" lines in an email to make it appear that the email was sent from an innocent third-party. The third party then receives bounced-back undeliverable messages and angry "do not spam me" complaints.

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

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

[9] FTC Press Release, *Law Enforcement Posse Tackles Internet Scammers, Deceptive Spammers* (May 15, 2003), *available at* <http://www.ftc.gov/opa/2003/05/swnetforce.htm>.

[10] *FTC v. Patrick Cella et al.,* No. CV-03-3202 (C.D. Cal.) (complaint filed May 7, 2003), *available at* <http://www.ftc.gov/os/2003/05/patrickcellacmp.pdf>.

[11] *FTC v. K4 Global Publishing, Inc. et al.,* No. 5:03-CV0140-3 (M.D. Ga.) (complaint filed May 7, 2003), *available at* <http://www.ftc.gov/os/2003/05/k4globalcmp.pdf>.

[12] *FTC v. Clickformail.com, Inc.,* No. 03-C-3033 (N.D. Ill.) (complaint filed May 7, 2003), *available at* <http://www.ftc.gov/os/2003/05/clickformailcmp.pdf>.

[13] In the other two cases, the FTC filed stipulated final orders prohibiting future participation in email chain letters. *FTC v. Evans,* No. 4:03CV178 (E.D. Tex.) (complaint and stipulated final judgment filed May 9, 2003); *FTC v. Benson,* No. 03CV0951 (N.D. Tex.) (complaint and stipulated final judgment filed May 6, 2003). Both are available at <http://www.ftc.gov/opa/2003/05/swnetforce.htm>.

[14] An open relay is an email server that is configured to accept and transfer email on behalf of any user anywhere, including unrelated third parties, which allows spammers to route their email through servers of other organizations, disguising the origin of the email. An open proxy is a mis-configured proxy server through which an unauthorized user can connect to the Inter-

Continued

law enforcers from 17 agencies identified 1,000 potential open relays, 90 percent of which were in 16 countries: U.S., China, Korea, Japan, Italy, Poland, Brazil, Germany, Taiwan, Mexico, Great Britain, Chile, France, Argentina, India, Spain, and Canada. The agencies drafted a letter, translated into 11 languages and signed by 14 different U.S. and international agencies, urging the organizations to close their open relays to help reduce spam.

APPROACHES TO SOLVING THE SPAM PROBLEM

Solutions to the problems posed by spam will not be quick or easy; nor is one single approach likely to provide a cure. Instead, a balanced blend of technological fixes, business and consumer education, legislation, and enforcement will be required. Technology that empowers consumers in an easy-to-use manner is essential to getting immediate results for a number of frustrated end-users. Any solution to the problems caused by spam should contain the following elements:

1. Enhanced enforcement tools to combat fraud and deception;
2. Support for the development and deployment of technological tools to fight spam;
3. Enhanced business and consumer education; and
4. The study of business methods to reduce the volume of spam.

The Commission's legislative recommendations, discussed below, would enhance the agency's enforcement tools for fighting spam. In addition, the FTC will continue vigorous law enforcement and reach out to key law enforcement partners through the creation of a Federal/State Spam Task Force to strengthen cooperation with criminal authorities. The Task Force can help to overcome some of the obstacles that spam prosecutions present to law enforcement authorities.

The Commission's experience shows that the primary law enforcement challenges are to identify and locate the targeted spammer. Of course, finding the wrongdoers is an important aspect of all law enforcement actions, but in spam cases it is a particularly daunting task. Spammers can easily hide their identity, forge the electronic path of their email messages, or send their messages from anywhere in the world to anyone in the world. Tracking down a targeted spammer typically requires an unusually large commitment of staff time and resources, and rarely can it be known in advance whether the target's operation is large enough or injurious enough to consumers to justify the resource commitment. For example, in some instances, state agencies spent considerable front-end investigative resources to find a spammer, only to discover at the back end that the spammer was located outside the state's jurisdiction. State and federal agencies recognize the need to share the information obtained in investigations, so that the agency best placed to pursue the spammer can do so more efficiently and quickly. The Task Force should facilitate this process. Further, it can serve as a forum to apprise participating agencies of the latest spamming technology, spammer ploys, and investigational techniques.

Through the Task Force, the FTC will reach out not only to its civil law enforcement counterparts on the state level, but also to federal and state criminal authorities. Although few criminal prosecutions involving spam have occurred to date,[15] criminal prosecution may well be appropriate for the most egregious conduct. The FTC and its partners in criminal law enforcement agencies continue to work to assess existing barriers to successful criminal prosecutions. The FTC will explore whether increased coordination and cooperation with criminal authorities would be helpful in stopping the worst actors.

Improved technological tools will be an essential part of any solution as well. A great deal of spam is virtually untraceable, and an increasing amount crosses international boundaries. Panelists estimated that from 50 percent to 90 percent of email is untraceable, either because it contains falsified routing information or because it comes through open relays or open proxies.[16] Because so much spam is untraceable,

---

net. Spammers use open proxies to send spam from the computer network's ISP or to find an open relay. *See* FTC Facts for Business, *Open Relays—Close the Door on Spam* (May 2003), *available at* <http://www.ftc.gov/bcp/con

[15] *See, e.g., United States v. Barrero,* Crim. No. 03-30102-01 DRH (S.D. Ill. 2003) (guilty plea entered May 12, 2003). Like the related case, *FTC v. Stuffingforcash.com Corp.,* Civ. Action No. 02 C 5022 (N.D. Ill. Jan. 30, 2003), the allegations in this criminal prosecution were based on fraud in the seller's underlying business transaction.

[16] Brightmail recently estimated that 90% of the email that it analyzed was untraceable. Two panelists at the Commission's Spam Forum estimated that 40% to 50% of the email it analyzed came through open relays or open proxies, making it virtually impossible to trace. Even when spam cannot be traced technologically, however, enforcement is possible. In some cases, the FTC has followed the money trail to pursue sellers who use spam. The process is resource intensive, frequently requiring a series of ten or more CIDs to identify and locate the seller in the real world. Moreover, the seller and the spammer often are different entities. In numerous instances, FTC staff cannot initially identify or locate the spammer and can only identify and locate the

technological development will be an important element in solving spam problems. To this end, the FTC will continue to encourage industry to meet this challenge.

Action by consumers and businesses who may receive spam will be a crucial part of any solution to the problems caused by spam. A key component of the FTC's efforts against spam is educating consumers and businesses about the steps they can take to decrease the amount of spam they receive. The FTC's educational materials provide guidance on how to decrease the chances of having an email address harvested and used for spam, and suggest several other steps to decrease the amount of spam an address may receive. The FTC's educational materials on spam are available on the FTC website.[17]

Finally, several initiatives for reducing the overwhelming volume of spam were discussed at the FTC's Spam Forum. At this point, questions remain about the feasibility and likely effectiveness of these initiatives. The FTC intends to continue its active role as catalyst and monitor of technological innovation and business approaches to addressing spam.

LEGISLATION TO ENHANCE THE FTC'S EFFECTIVENESS TO FIGHT FRAUDULENT SPAM

Effective spam legislation must address the following three issues: First, legislation must address how to find the person sending the spam messages. Although we believe that technological changes will most effectively resolve this issue, we have proposed several procedural legislative changes that can provide some assistance in our law enforcement investigations. Second, legislation must deal with how to deter the person sending the spam messages. As discussed below, the Commission believes that civil penalties, and possibly criminal sanctions, would help address this issue. Finally, legislation must determine what standards will govern non-deceptive, unsolicited commercial email. The Commission believes that the appropriate standards would include clear identification of the sender of a message and by empowering consumers to end the flow of messages that they do not wish to receive.

It would be useful to have additional legislative authority, addressing both procedural and substantive issues, that would enhance the agency's effectiveness in fighting fraud and deception. The procedural legislative proposals would improve the FTC's ability to investigate possible spam targets, and the substantive legislative proposals would improve the agency's ability to sue these targets successfully, including increased penalties for violations.

Procedural Proposals

The FTC's law enforcement experience shows that the path from a fraudulent spammer to a consumer's in-box frequently crosses at least one international border and often several. Thus, fraudulent spam exemplifies the growing problem of cross-border fraud. Two of the provisions in the Commission's proposed cross-border fraud legislation, discussed at the recent reauthorization testimony, would be particularly helpful to enable the FTC to investigate deceptive spammers more effectively and work better with international law enforcement partners.

First, the Commission has asked Congress to amend the FTC Act to allow FTC attorneys to seek a court order requiring a recipient of a Civil Investigative Demand ("CID") to maintain the confidentiality of the CID for a limited period of time. Several third parties have told us that they will provide notice to the target before they will share information with us, sometimes because they believe notice may be required and sometimes even if such notice clearly is not required by law.

Second, the Commission asked Congress to amend the FTC Act so that FTC attorneys may seek a court order temporarily delaying notice to an investigative target of a CID issued to a third party in specified circumstances. Currently, the Right to Financial Privacy Act ("RFPA") and the Electronic Communications Privacy Act ("ECPA") require such notice.

The FTC's experience is that fraud targets often destroy documents or hide assets when they receive notice of FTC investigations. Although the RFPA and ECPA provide a mechanism for delaying notice, the FTC's ability to investigate would be improved by tailoring the bases for a court-ordered delay more specifically to the types of difficulties the FTC encounters, such as transfers of assets offshore. In addition, it is unclear whether FTC attorneys can file such applications, or whether the Commission must seek the assistance of the Department of Justice. Explicit authority for the FTC, by its own attorneys, to file such applications would streamline the

---

seller. In many of those cases, in the course of prosecuting the seller, staff has, through discovery, sought information about the spammer who actually sent the messages. This, too, involves resource-intensive discovery efforts.

[17] *See* <http://www.ftc.gov/spam>

agency's investigations of purveyors of fraud on the Internet, ensuring that the agency can rapidly pursue investigative leads.

Other legislative proposals would enhance the FTC's ability to track deceptive spammers. First, we request that the ECPA be clarified to allow the FTC to obtain complaints received by an ISP regarding a subscriber. Frequently, spam recipients complain first to their ISPs, and access to the information in those complaints would help the agency to determine the nature and scope of the spammer's potential law violations, as well as lead the agency to potential witnesses.

Second, we request that the scope of the ECPA be clarified so that a hacker or a spammer who has hijacked a bona fide customer's email account is deemed a mere unauthorized user of the account, not a "customer" entitled to the protections afforded by the statute. Because of the lack of a statutory definition for the term "customer," the current statutory language may cover hackers or spammers. Such a reading of the ECPA would permit the FTC to obtain only limited information about a hacker or spammer targeted in an investigation. Clarification to eliminate such a reading would be very helpful.

Third, we request that the ECPA be amended to include the term "discovery subpoena" in the language of 18 U.S.C. § 2703. This change is particularly important because a district court has ruled that the FTC staff cannot obtain information under the ECPA from ISPs during the discovery phase of a case, which limits the agency's ability to investigate spammers.[18]

Substantive Proposals

Substantive legislative changes also could aid in the FTC's law enforcement efforts against spam. Although Section 5 of the FTC Act provides a firm footing for spam prosecutions, additional law enforcement tools could make more explicit the boundaries of legal and illegal conduct, and they could enhance the sanctions that the agency can impose on violators. As the Commission recently testified at its Reauthorization hearing before this Committee, the Telemarketing and Consumer Fraud and Abuse Prevention Act ("TCFAPA"), 15 U.S.C. §§6101-6108, provides a model for addressing unsolicited commercial e-mail. Amendments to the TCFAPA would authorize the FTC to adopt rules addressing deceptive and abusive[19] practices with respect to the sending of unsolicited commercial e-mail. Approaching spam through this statutory model would provide the market with direction, but would do so within a framework that could change as the problems evolve. Regardless of the statutory approach taken, however, the Commission believes that the following elements are important.

First, any legislation should give the FTC some authority via rulemaking to address deceptive practices relating to spam. Agency rules could be adapted to new changes in technology without hindering technological innovation, thus providing the market with direction, but doing so within a framework that could change as the problems evolve. Whether addressed through the legislation itself or through rulemaking, unlawful practices that should be prohibited include: using false header or routing information; using false representations in the "subject" line; using false claims that an unsolicited commercial email message was solicited; using false representations that an opt-out request will be honored; sending any recipient a commercial email message after such recipient has requested not to receive such commercial email messages; failing to provide a reasonable means to "opt out" of receiving future email messages; and sending commercial email to an address obtained through harvesting or a dictionary attack. Morever, any statute also should prohibit assisting and facilitating any of the above, i.e., providing substantial assistance to another party engaged in any violation knowing or consciously avoiding knowing that such party is engaged in such violation.

Second, any legislation should embody the same standard of liability that is embodied in Section 5 of the FTC Act, without a general requirement to show intent or knowledge. Imposition of intent or knowledge requirements as a precondition of liability would actually make the FTC's ability to enforce the specific anti-spam statute more restrictive than the agency's existing authority under Section 5 to attack spam and would unnecessarily complicate enforcement.

Third, any statute or rule issued under the statute should be enforceable by the FTC like other FTC rules. This entails actions in federal district court, authority to seek preliminary and permanent injunctions and other equitable relief, and liability for civil penalties of up to $11,000 per violation. (The amount of civil penalties

---

[18] *See FTC v. Netscape Comm. Corp.,* 196 F.R.D. 559 (N.D. Cal. 2000).

[19] The FTC has determined, in the Statement of Basis and Purpose for the Amended TSR, that the undefined term "abusive" used in the legislation authorizing that Rule will be interpreted to encompass "unfairness." 68 Fed. Reg. 4580, 4614 (2003).

is governed by statutory factors, such as ability to pay, previous history of such conduct, egregiousness of the conduct, etc.).

Fourth, any legislation should authorize states to enforce the statute or FTC rule in federal court. A state enforcement mechanism has proven successful in other areas of consumer protection, such as telemarketing, and would make the states more capable law enforcement partners with the Commission.

Finally, any statute should seek to assure consistency between state and federal laws. The scope of the Internet and of email communication is global, transcending national boundaries. Congress should seek to minimize artificial barriers that would break up this market.

Additionally, the criminalization of false header and routing information should be explored. The FTC staff has been discussing with criminal authorities the likely effect of a specific statute that criminalized this conduct. At this time, the FTC has no recommendations on whether changes in the criminal code are necessary or appropriate.[20]

Admittedly, we recognize that these legal steps alone will not solve the growing spam problem. Nor is it clear what impact these steps will have on some of the other problems associated with spam (e.g., volume and security). These issues may need to be addressed separately. Nevertheless, the FTC believes that legislation, such as that described above, would provide more effective investigative and enforcement tools and would enhance the FTC's continuing law enforcement efforts.

CONCLUSION

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

The Commission appreciates this opportunity to describe its efforts to address the problem of spam.

Mr. STEARNS. Thank you. I would again note that, all members, your testimony is made full and part of the record, so we are going to try to insist the 5-minute rule knowing that we are a little later than we originally thought we would be when this hearing started. Mr. Betty, welcome.

STATEMENT OF CHARLES GARRY BETTY

Mr. BETTY. Thank you, Mr. Chairman, ladies and gentlemen of the committee, and thank you for inviting me to testify before you today. My name is Garry Betty and I am the CEO of EarthLink. EarthLink is the Nation's third largest ISP, serving 5 million customers nationwide with dial-up, broadband, web hosting and wireless Internet services. As such, we are on the front lines every day in the fight against this unsolicited commercial mail that we have been hearing about for the last hour or so, known as spam.

Spam is a problem and a growing problem. At EarthLink, have seen over a 500 percent increase in receipt of spam in the last 18 months. And what originally began as an occasional inconvenience has now grown as quite an annoyance. Spam creates inefficiency, but, more importantly, for our customers spam is the No. 1 thing that they least like about the Internet. Like other statistics we have heard, 50 percent of all of our incoming mail is spam. Our existing technology, filtering technology does successfully eliminate 70 to 80 percent of those messages from ever getting to our cus-

[20] Any legislation that criminalizes certain types of spam activities should not negatively impact the FTC's existing Section 5 authority or impose new standards of proof, scienter, or evidence for civil enforcement cases.

tomers, but with this rapid increase even 20 to 30 percent of a lot of spam is a lot of unwanted mail getting to our users' in-boxes.

Many of the members of this panel have commented on cost. Spam does cost Internet providers real money. Excess server capacity, an abuse team working full time to ferret out and close down sources of spam, internal and external legal fees are costs that we incur trying to shut down the most egregious of spammers. Spam is a pernicious problem. Get rich quick schemes, effortless weight loss programs aren't anything new, but the cost burden imposed by spam is. Unlike, as we have heard, telemarketing or direct mail pieces, which require the sender to pay for these messages, spam adds insult to injury by shifting this cost burden to people like Earthlink and of course the customers who have to delete that from their in-boxes.

In order to combat spam, I think we must attack it on several fronts. Legislation, litigation, enforcement, customer education and technology solutions are all fronts in this fight, and I will try to briefly address some of these efforts.

EarthLink supports legislation to help ISPs and consumers fight spam. Congress is clearly engaged in this issue, as we have heard today. We count no fewer than eight bills pending in the House and Senate, and rather than speak to just any one bill, we would like to note provisions in various bills which we think will be helpful to ISPs like Earthlink and our consumers.

Legislative provisions Earthlink supports include no restrictions on an ISP's current ability to block spam on behalf of its customers. ISPs are consumers' first line of defense against spam. Recognition of ISPs rights of action against spammers. As I will discuss, ISPs' lawsuits against spammers are an effective tool to fight spam. Allowing recovery of actual damages greater than the capital and statutory damages, requirements for accurate sender, subject line and IP address information, prohibitions on using harvested e-mail addresses to send spam, and criminal penalties for non-compliance.

Another important front in the fight against spam is litigation. Earthlink was one of the first ISPs to sue spammers. We filed over 100 lawsuits against spammers in the last 5 years and most recently won a judgment in May of 2003 against Howard Carmack, known as the Buffalo Spammer, who was estimated to send out over almost a billion spam messages through Earthlink alone in an 18-month period. Earthlink's case against Carmack is illustrative. Not only did we win a monetary damage but more importantly we obtained permanent injunctive relief against him. Furthermore, we make all ISPs third party beneficiaries of such judgments. This bars the defendant, Carmack, from sending spam to Earthlink customers or to customers of any other ISPs, and we would urge other ISPs to do likewise.

Obviously, this case was successful even without specific anti-spam legislation. Rather we relied on a combination of laws including Federal statutes, State statutes, new laws, such as the Computer Fraud and Abuse Act, and time-tested notions of common law, such as trespass and conversion. This is not to say Federal anti-spam legislation is unneeded; rather, it should supplement and strengthen the legal recourse available today to ISPs and other parties.

Perhaps the most promising front in the fight against spam is the implementation of technology solutions. Earthlink and ISPs have generally relied on filtering software to limit the amount of spam customers receive. Earthlink's filtering system, known as spaminator, successfully filters 70 to 75 percent of all junk mail before it ever gets to a customer's computer. It also gives users customizable tools to further reduce unwanted e-mails in their in-box. Filtering technology worked well until recently, but the volume of spam has increased and this is just not enough. Most recently, Earthlink introduced a new challenge response e-mail system, called SpamBlocker. This is a new way to give customers control over their in-boxes. Unlike filters which deliver all messages except for the ones they filter out, SpamBlocker keeps messages outside of the gate of a user's in-box letting in only those messages recognized by the senders.

Mr. STEARNS. Mr. Betty, you are a minute beyond the 5. In summary——

Mr. BETTY. In summary, I think we have implemented technology with SpamBlocker that in my own case I used to get over 200 a day. I now have not received one unwanted e-mail in my personal mailbox in over 6 weeks.

[The prepared statement of Charles Garry Betty follows:]

PREPARED STATEMENT OF CHARLES GARRY BETTY, CEO, EARTHLINK, INC.

Mr. Chairman, ladies and gentlemen of the Committee, thank you for inviting me to testify before you today. My name is Garry Betty and I am the CEO of EarthLink. EarthLink is the nation's 3rd largest Internet Service Provider (ISP) serving 5 million customers nationwide with dial-up, broadband (DSL, cable and satellite), web hosting and wireless Internet services. As such, we are on the front lines every day in the fight against unsolicited commercial e-mail, commonly known as spam.

As you well know, spam is a growing problem. There are over 70 million American households and businesses online today and almost every one of them has first-hand experience with spam. We at EarthLink have seen a 500% increase in spam over the past 18 months. What was at first an occasional inconvenience grew to be an annoyance and now threatens to overwhelm online communications. E-mail is often described as the Internet's "killer app." Left unchecked, spam threatens to kill the killer app.

Spam creates inefficiency. By some estimates, spam is responsible for $10 billion a year in lost productivity to American businesses. As an ISP, approximately 50% of all e-mail coming into our servers is spam. AOL estimates this figure as high as 80% on their network. We are able to filter out 70-80% of these messages before they ever get to our customers, but the increasing volume means that lots of unwanted electronic junk mail still gets to user's in-boxes. Spam costs Internet providers real money. Excess server capacity, an "abuse team" working full time to ferret out and close down sources of spam on the internet, internal and external legal fees are all costs we incur because of spam. While we don't publish exact figures on this, it is fair to say that they are in excess of $10 million a year for EarthLink alone.

Spam is a pernicious problem. While get rich quick schemes, effortless weight loss programs and pills that promise to enlarge body parts are nothing new, the cost burden imposed by spam is. Newspaper and magazines ads, telemarketing calls, direct mail pieces and signs tacked to telephone poles all require the sender to pay for their messages. Spam adds insult to injury by shifting this cost burden. Spam costs virtually nothing to send. (One recent widely circulated spam message for spammers advertises 20 million email addresses for $149.00.) Instead, the costs of spam are borne by ISPs which must handle this junk e-mail and by consumers who get their in-boxes filled with it.

In order to win the fight against spam, we must engage it on several fronts. In addition to legislation, we must also use litigation, enforcement, customer education and technology solutions to combat spam. I would like to briefly address each of these in turn:

Legislation

EarthLink supports legislation to help ISPs and consumers in the fight against spam. And Congress is clearly engaged in this issue. We count no fewer than seven bills currently being actively discussed in the House and Senate. Rather than speak just to any one bill, we would like to note several provisions in various bills which we think will be helpful to ISPs and consumers, based upon the experience Earthlink has had in suing some of the nation's most egregious spammers.

First, we support the provision in several bills which note that they place no restrictions on an ISP's current ability to block spam on behalf of its customers. ISPs are truly the first line of defense against spam for consumers. ISPs that deploy effective filtering and blocking techniques can spare their customers a good deal of the aggravation that spam creates. However, since spammers are constantly looking for new ways to defeat ISP blocking protections, it is important to ensure that legislation does not limit the ability of ISPs to adjust and refine their filtering and blocking techniques to maximize their effectiveness.

Similarly, we support the provision in various bills that note that ISPs have a right of action to pursue legal action against spammers. As I will discuss in the next section, ISP lawsuits against spammers are an effective tool in the fight against spam.

Next, we would urge caution in placing a cap on monetary damages. Based on our own litigation experience, we believe that large monetary damage awards against the most egregious spammers send a strong signal about the seriousness of spamming and have a stronger deterrent effect against other spammers. We would urge Congress not to impose a damages cap on ISP legal actions against spammers.

Finally, we support requirements for accurate sender, subject line and IP address information. Consumers must have accurate sender, subject line and IP address information, and we applaud the legislative efforts to confirm these basic requirements. For too long spammers have deceived innocent victims with fraudulent and deceptive "come-ons" in the subject lines, confusing consumers into thinking that they are receiving e-mails from a trustworthy entity or friend. These deceptions must be stopped and legislative efforts to address this are well directed.

Litigation

Another important front in the fight against spam is litigation. EarthLink was one of the first ISPs in the country to go after spammers in court. Earthlink's successful 1997 case against Sanford Wallace and Cyberpromotions stopped what was then one of the most prolific spammers on the Internet. Since that time, EarthLink has filed lawsuits against over 100 spammers. Most recently, EarthLink won a judgment in May 2003 against Howard Carmack the "Buffalo Spammer." It is estimated that Carmack sent out some 850 million spam messages over an 18-month period, or an average of about 2 million messages a day.

EarthLink's case against Carmack is illustrative of our lawsuits against spammers. While we were able to obtain a $16.4 million judgment against Carmack, we just as importantly obtained permanent injunctive relief, barring him from spamming again. Furthermore, when EarthLink gets judgments against spammers, it asks the court to make all other ISPs 3rd party beneficiaries of those judgments. This bars the defendant spammer not only from sending spam to EarthLink customers, but also from sending spam to the customers of any other ISP. We urge other ISPs to do likewise in their suits against spammers.

Obviously, this case was brought successfully without specific anti-spam legislation. Rather, we relied on a combination of laws including federal statutes such as RICO and the ECPA, state statutes such as the Georgia Computer Systems Protection Act, fairly new laws such as the Computer Fraud and Abuse Act and time-tested notions of common law such as trespass and conversion. In all, our complaint against Carmack included 14 counts. This is not to say that federal anti-spam legislation is unneeded, rather that it should supplement and strengthen the legal recourse available today to ISPs and other parties.

A postscript: Based on information developed in EarthLink's civil case against Carmack, the New York Attorney General subsequently filed criminal charges against him for identity theft, landing him in jail. We believe this to be the first time that anti-spam litigation has also led to a criminal arrest of a spammer.

Technology Solutions

Perhaps the most promising front in the fight against spam is the implementation of technology solutions. EarthLink and other ISPs have until now generally relied on filtering software to limit the amount of spam their customers receive. EarthLink's filtering systems, known as spaminator, filters out 70-80% of all junk e-mail before it ever gets to a customer's computer. Spaminator also provides users

with customizable tools they can use to further reduce unwanted emails in their inboxes. It is possible to increase the sensitivity of filters such as spaminator, but you then begin to run the risk of filtering out messages from legitimate senders which an e-mail user wants to receive.

Filtering technology has worked well until recently. Eighty percent (80%) effectiveness was fine in filtering through a few dozen spam messages a day. But as the volume of spam has increased 5-fold in the past 18 months, Internet users are now bombarded with sometimes hundreds of messages a day. An 80% effectiveness filter therefore lets through an increasingly unacceptable number of spam messages.

Enter SpamBlocker, EarthLink's new challenge-response e-mail system. Developed at EarthLink, spamBlocker presents a new way to give customers control over their inboxes. Unlike filters, which default to letting through email except for the messages they filter out, spamBlocker keeps all messages "outside the gate" of a user's inbox, letting in only those messages from recognized senders. SpamBlocker allows a user to import their address book of valid senders and to quickly and easily add names to that list. Rather than only eliminating email from unknown sources it holds these messages in a Suspect E-mail folder allowing the recipient to review and accept the messages they wish to receive. SpamBlocker also sends the sender a one-time easy to complete Allowed Sender Request Form. Able to be completed in several seconds by an actual person, it will not be usable by an automated email program or be able to be filled out at all where, as is often the case, a spammer fakes the IP address which is the source of his spam. SpamBlocker will virtually eliminate spam in a user's in-box and is available free to all EarthLink subscribers.

Thank you for giving me the opportunity to testify today.

Mr. STEARNS. Terrific. I wish we all could say that.

Mr. BETTY. If you were an Earthlink customer, you could.

Mr. STEARNS. I am going to check with my brother who has it. Mr. Curran.

STATEMENT OF CHARLES CURRAN

Mr. CURRAN. Chairman Stearns——

Mr. STEARNS. You have got to hit that button. Try again.

Mr. CURRAN. Chairman Stearns——

Mr. STEARNS. No.

Mr. CURRAN. There we go. Chairman Stearns, Chairman Upton, Congressman Markey and Congresswoman Schakowsky, I would like to thank you, along with Chairman Tauzin and Congressman Dingell, for the opportunity to testify today before your subcommittees about the crisis in the growth of junk e-mail. I work in AOL's Legal Department battling spam, and I have overseen AOL's significant litigation efforts against spam senders. I would like to share a perspective from the front lines of the anti-spam war.

Spam has increased at an alarming rate because it is simple and very inexpensive for spammers to send large quantities of e-mail and because the open nature of Internet e-mail technology makes it quite easy for spammers to conceal their identities and the scope of their spamming activities. Consumers, businesses and ISPs face an ever-increasing deluge of spam, and unfortunately these recipients bear the cost of processing all these messages that flood their in-boxes every day.

Consumers and ISPs use filters to try to stop this type of junk e-mail, but spammers constantly adapt. To make sure their e-mail gets through to recipients and to hide their identities, spammers resort to technologies of falsification and evasion. The evasive techniques include falsifying header and routing information, commandeering innocent parties' Internet servers to send spam, hacking into e-mail accounts belonging to innocent users and registering for

multiple e-mail accounts or domain names that are then used to establish false identities for transmitting spam.

Recent studies by the spam filtering company, Brightmail, estimate that up to 90 percent of spam involves these kinds of outlaw techniques of evasion. More recently, many spammers are now adopting computer hacker techniques, such as computer viruses to hijack innocent consumer's computers and use them to send spam untraceably.

This isn't an easy battle, and AOL believes it must be fought on many fronts simultaneously in order to be truly effective. That is why we fight the spam war using a combination of technology, legal counter measures, member education and empowerment and collaboration with others in our industry. We are also working with legislatures such as members of your subcommittees on more effective legislation to bring accountability to spammers.

On the technology front, AOL uses strong filtering technologies to limit the tide of spam entering AOL's e-mail system, blocking up to 2.4 billion messages per day. We are also deploying spam-fighting tools later this summer that will allow our members to divert unwanted e-mail to a separate spam folder and adapt spam filtering to their individual preferences. We provide parents with strong tools, our parental controls, to help keep offensive and objectionable e-mail out of children's in-boxes, and we empower our members to report spam, helping AOL to improve its technological counter measures as well as to identify candidates for enforcement action. The fact that AOL members report up to 10 million spam complaints daily demonstrates the critical importance of spam fighting to our members.

On the legal front, we have served well over 100 defendants in 25 lawsuits, winning court injunctions and damages awards to help deter spam senders. The defendants in these suits have advertised pornographic web sites, get-rich-quick schemes and other dubious products. AOL continually investigates this spamming activity and cooperates with Federal and State authorities in their enforcement actions. We believe that enhanced enforcement is vital to curtailing the growth of spam. The anti-spam litigation brought by ISPs, like AOL, Earthlink and Microsoft, parallel the increasingly aggressive enforcement actions brought by the Federal Trade Commission and State attorneys general. Bringing anti-spam cases is often complex and resource intensive because large-scale spammers try every bit as hard to mask the profits from their activities as they try to hide how they send their e-mails. To give one example, in a recent Federal court case, it took AOL 2 years to expose the complex web of shell and offshore companies used by large scale pornography spammers.

Despite these obstacles, ISPs have strong incentives to bring enforcement actions. First, such actions help improve the experience of our subscribers by attacking the sources that the spam our members complain about most. And, second, it helps to reduce the overall volume of spam on the Internet. We believe that even stronger enforcement tools are necessary to establish the kind of criminal penalties and civil damages necessary, and we thank the subcommittees for making spam a priority issue this year. We are particularly grateful to Chairman Tauzin and Congressman Burr, as

well as Congresswoman Wilson, Dingell and Green for introducing legislation that sets a solid foundation to address this problem.

AOL believes that legislation should do three things to be an effective tool, most importantly because of the seriousness of the outlaw spam problem. Legislation must provide for strong criminal and civil penalties against spammers who use deceptive or fraudulent tactics to hide their identities. For large-scale spammers who use these outlaw tactics, felony-level penalties are needed to deter them for engaging in this crime.

Second, legislation should provide clear baseline rules of the road for commercial e-mail sent by marketers who do not engage in outlaw e-mail transmission techniques. These rules should provide consumers with meaningful choices about the commercial e-mail messages they receive from a particular sender and should prevent end runs around consumers' preferences by the use of sham corporate successors or affiliates.

Finally, it is also critically important that legislation provide for ISP civil enforcement of its prohibitions. ISPs such as a AOL have a unique role to play in anti-spam enforcements because of our firsthand knowledge of the problem obtained through the complaints of our members and our experience fighting the latest technologies used by spammers. We applaud the efforts of this committee in tackling the spam problem at this critical juncture and look forward to working with you and other lawmakers to develop legislative solutions that can help consumers and their ISPs prevail in the anti-spam war. Thank you for the opportunity to testify, and I am happy to answer any questions you may have.

[The prepared statement of Charles Curran follows:]

PREPARED STATEMENT OF CHARLES CURRAN, ASSISTANT GENERAL COUNSEL, AMERICA ONLINE, INC.

Chairman Stearns, Chairman Upton, and Members of the Subcommittees, on behalf of America Online, Inc., I would like to thank you for the opportunity to testify before the Subcommittees on the issue of junk e-mail—or "spam." My name is Charles Curran, and I am an Assistant General Counsel in the Legal Department at America Online, Inc., where much of my time is spent battling spam. I have overseen AOL's extensive litigation efforts against spam senders, and appreciate this opportunity to share with the Subcommittees a perspective from the front lines of the anti-spam war.

I would like to describe the nature of the spam problem, its effect on ISPs and Internet users, and some of the things that AOL is doing to help reduce spam, and to explain the role that ISP enforcement and litigation play in fighting the spam problem. But first, I would like to thank the full Committee for making the spam problem a priority issue this year, and Chairman Tauzin, Rep. Burr, and others for introducing a strong legislative vehicle that we believe sets a solid foundation to address this problem. We believe that spam has grown to present a critical threat to the Internet, and that the spam battle must be fought on many fronts simultaneously in order to be truly effective—including policy initiatives, ISP litigation, government enforcement, spam filtering technologies, member tools and education, and industry collaboration. While technology holds many of the answers to this problem, we cannot succeed in the fight against spam without government working with ISPs to play a strong and important enforcement role. We are anxious to work with you to find a solution to this crisis for e-mail on the Internet.

1. THE REASONS FOR THE SPAM CRISIS

The principal drivers of the explosive growth in the spam problem are the ease with which senders can transmit large quantities of e-mail, and the similar ease with which spammers can conceal their identities as the source of this junk e-mail.

First, the e-mail medium makes it possible for senders to transmit virtually unlimited quantities of advertising messages at very low costs. Spammers do not bear

the costs of processing, sorting and delivering all these e-mails: instead, it is the recipients and their ISPs who must absorb the costs of managing the huge volume of unwanted mail. Spammers are limited in e-mail transmission volume only by the low costs of Internet connectivity. And because e-mail is a nearly costless medium for senders, spammers have every incentive to send out as many e-mails as possible, even if virtually no recipients want or respond to the promotions, and despite heavy costs to ISPs who have to process these huge quantities of mail. These underlying economics are the principal cause of the rapidly expanding volume of spam, and the reason that ISPs and businesses everywhere are experiencing such a tremendous surge in junk e-mail—as spammers send out even greater numbers of junk mail messages to which fewer and fewer recipients will ever respond. AOL estimates that spam accounts for a staggering 60-80% of e-mail traffic that hits our e-mail filters from the Internet, and external studies predict similar alarming trends in Internet e-mail as whole.

The second essential feature of the e-mail medium that contributes to the spam problem is the fact that the technical protocols used to send e-mails on the Internet can be manipulated by spammers, both to conceal their identities as spam senders and to conceal the volume and scope of their e-mailing activities. The "open" nature of the Internet and its underlying e-mail transmission protocols lend themselves to abuse by spammers looking to evade accountability for their activities, and undermine and evade the attempts of consumers and ISPs to filter out or block their junk mail transmissions. In AOL's experience, most spam is sent using such evasive, "outlaw" transmission techniques.

A technical struggle is now taking place on the spam front, one which pits consumers and ISPs using defensive spam filtering technologies against spammers who seek to exploit any technical loophole that will allow them to get their mail through to a recipient's e-mail box. A new and even more pernicious feature of this technological war is the increasing adoption by spam senders of computer hackers' tools—such as viruses and "Trojan horses"—to find ever more untraceable ways to use innocent parties' computers to cover their tracks.

The combination of low sender costs and lack of sender authentication is irresistible to unscrupulous junk mailers. As a result, Internet e-mail users now find themselves being bombarded with an ever-increasing volume of spam in their mailboxes, much of it containing objectionable or misleading content. Indeed, the Federal Trade Commission's May 2003 spam survey indicated that at least two-thirds (66%) of junk e-mail contains falsified header or subject line information, and spam filtering companies like Brightmail estimate that as many as 90% of spam messages contain falsified header or routing information that make them untraceable to a specific source. And so the spam problem is not just a problem in terms of the increasing volume of spam that businesses must process and deliver, but also a challenge for all consumers whose confidence in Internet e-mail is being steadily eroded by incessant waves of spam in their email in-boxes.

2. WHAT AOL IS DOING TO FIGHT SPAM

AOL fights the ongoing spam war using a combination of technological and legal countermeasures, as well as policy initiatives and collaboration with others in industry. In lawsuits involving well over a hundred defendants, AOL has used the legal process to penetrate the secret world of spam senders, not only to help ensure that spammers face accountability for their actions, but also to better understand and combat the techniques of concealment used by the spammers. AOL's goal is to improve the experience of our more than 35 million account holders, and to deter would-be spammers from sending huge quantities of junk e-mail in the first place.

On the technology front, AOL uses a comprehensive set of filtering technologies at the network level to limit the tide of spam entering AOL's e-mail system and our members' mailboxes. In recent months, these anti-spam filters have blocked as much as 2.4 billion pieces of unwanted e-mail in a single day, which amounts to stopping almost 70 spam e-mails per account per day from reaching our members. To counter the flood of spam, AOL dedicates not only significant computer resources to filtering junk mail, but also a large staff of technologists, who give AOL the ability to respond on a 24-hour basis to the ever-changing tactics used by spam senders to attempt to penetrate the AOL network.

AOL also empowers its members to fight spam through a combination of robust e-mail controls and a "Report Spam" tool that lets them report and delete unwanted junk e-mail directly from their mailboxes. Using the "Report Spam" button, members have reported more than 10 million spam complaints to AOL in a single day. AOL uses these member complaints not only to help identify and filter in real-time

the spam being sent to the AOL network, but also to identify large-scale abusers for law enforcement purposes.

Starting later this summer, AOL 9.0, the latest version of AOL's online service software, will provide AOL members with a completely revamped suite of spam-fighting tools. These tools include a new "Spam" folder that is separate from a member's mailbox for incoming e-mail, and to which suspected spam is automatically routed. Not only will spam filtering be enhanced at the network level; members also will be provided personalized and adaptive spam filtering tools that adjust to the individual preferences of each user, as well as word-specific and URL filters that a member can use to route potentially objectionable mail to their "Spam" folder. AOL's overall mail controls and Parental Controls will offer additional features to help protect users of all ages from objectionable spam and the content it contains, such as blocks on the display of embedded images. And AOL will continue to provide our members with other important consumer safety tips and tools that can help them reduce spam and improve the security of their online experience—particularly in the broadband environment, where it is critical that consumers know how to protect themselves in the world of "always-on" high-speed connections that spammers sometimes attempt to abuse.

On the legal front, AOL has been active in suing spammers since 1997. AOL has filed 25 lawsuits against more than 100 companies and individuals responsible for the transmission of spam advertising pornographic Web sites, get-rich-quick schemes, and other dubious products. These lawsuits have demonstrated the ever-greater lengths to which spammers go to conceal their activities and continue their theft of resources from the Internet community. The suits have resulted in court decisions that not only prohibit further spamming by the defendants, but also awarded significant financial damages that have bankrupted many spam senders. AOL's most recent suits, announced earlier this year, targeted more than a dozen companies and individuals responsible for sending more than a billion spam messages to our consumers. AOL continues to investigate other spam senders, sending hundreds of cease-and-desist letters to suspected spam senders and even the vendors of spamming software, so as to deter others from entering the spamming business. And we have cooperated with federal and state enforcement authorities in separate enforcement proceedings, sharing our technical expertise to help widen the overall scope of deterrence.

We're also building alliances with others in our industry to think creatively and constructively about how to curb the overall spam problem. We've joined with Microsoft, Yahoo! and Earthlink to drive a dialogue with other industry stakeholders necessary to the development of open technical standards and industry guidelines that will help fight spam. We also welcome the actions that Earthlink, Microsoft, and other ISPs have taken to fight spam on the legal front, and look forward to finding new ways that industry can work together to collect the technical evidence necessary to bring spammers to justice.

Finally, AOL works with federal and state policymakers to support efforts to reduce spam by enacting laws that specifically target the deceptive, "outlaw" tactics used by spam senders, and that deter the sending of spam by establishing appropriate financial and criminal penalties. For example, we worked with Virginia legislators, the Attorney General, and the Governor to get a tough new law enacted in Virginia earlier this year that provides felony-level penalties for spammers who send significant quantities of spam by fraudulent means. AOL is grateful to the Members of the Subcommittees for their willingness to consider similar tough remedies in federal legislation.

3. THE CRITICAL ROLE OF ISP ENFORCEMENT

Currently, the anti-spam litigation campaigns of ISPs like AOL, Earthlink and Microsoft complement the vigorous efforts of the Federal Trade Commission and State Attorneys General in this regard. ISPs have a critical role to play in anti-spam enforcement efforts, not only because we have a wealth of member complaints and evidence to support effective legal action, but also knowledge from the front lines of the spam battle of the complex and rapidly changing technologies used by most spam senders to evade detection.

It is very important that federal anti-spam legislation provide for ISP civil enforcement of both civil and criminal anti-spam prohibitions. The spam problem has reached a sufficient magnitude that government enforcement alone cannot stem the tide, and must be complemented by sustained, industry-wide enforcement by ISPs. In many cases, ISP assistance not only helps provide an important source of evidence for criminal and other government enforcement—including uncovering the

identities of "king pin" spammers: it also is critical to unmasking "state-of-the-art" technological exploits used by spammers to avoid any kind of accountability.

ISPs like AOL aim to litigate against large-scale spammers, but the spammers making the greatest profits from their activities naturally expend significant efforts to conceal not only how they transmit their spam, but also how they receive revenue from their activity. Consequently, tracking down such spammers through litigation is often highly complex, resource intensive, and time consuming. To provide one example, some large-scale pornography spammers against whom AOL had originally obtained a federal injunction tried to circumvent that prohibition by transferring ownership of their pornography domains through shell companies and offshore entities. A sustained, two-year investigative process was needed to demonstrate the "vast . . . cyber-oriented, multi-state and multi-national conspiracy" that a federal court concluded warranted a $6.9 million damages award against the defendants.[1]

Similarly, large-scale sponsors of spam often use complex business structures to attempt to distance themselves from the actual transmission of spam. For example, AOL engaged in extensive litigation against pornographic Web site operators who used a so-called "Webmaster" business model.— Under this model, the Webmasters obtained a share of the revenue derived at the pornography operator's Web sites, based upon traffic driven to these sites by spam.— The site operators claimed, unsuccessfully, that the spam senders were "independent contractors" for whose actions they were not responsible.

Most spammers also conceal or dissipate the profits of their activity and, as a consequence, legal judgments against them often are difficult to collect. The difficulty in holding such spammers accountable financially, combined with the complexity and expense necessary to even identify their activities, mean that spam enforcement is far from a source of profits for ISPs.

But despite these obstacles, ISPs still have very strong incentives to bring enforcement actions. First, such actions help to improve the online experience of our individual members. Our members help us identify the most objectionable forms of spam through their spam complaints, and rightly expect us to take action to stop it. Second, spam forces ISPs to make significant network and personnel expenditures to process truly gigantic volumes of unwanted mail. ISP enforcement thus not only serves to improve the member experience, but to create deterrence to spam senders whose large-scale e-mail transmissions pose the biggest burden to the Internet as a whole.

In short, ISP civil enforcement serves the interests of Internet users and the entire Internet community by helping identify the most appropriate targets for enforcement, illuminating the technologies and subterfuges used by spammers to evade detection, and complementing and supporting the actions taken by federal and state law enforcement. Consequently, the ability of ISPs to sue for spam-related activity is vital, in conjunction with government enforcement, to controlling the spam problem.

4. THE NEED FOR STRONG CRIMINAL AND CIVIL PENALTIES AGAINST "OUTLAW" SPAMMERS

While ISPs have used existing law to attempt to stem the tide of spam, stronger legislative enforcement tools are needed not only to keep up with the ever-evolving techniques of transmission evasion used by spammers, but also to establish the kinds of criminal penalties and civil damages necessary to deter spammers from engaging in such activities. Additionally, strong penalties prohibiting such "outlaw" techniques are essential to ensuring that future technologies promoting "trusted" e-mail can be used to help improve consumers' e-mail experience.

The "outlaw" techniques that spammers typically have used to conceal their activities include: (1) the falsification of e-mail transmission information and misappropriation of innocent third parties' domain names in such e-mails; (2) the transmission of e-mail from hacked e-mail accounts belonging to innocent users; and (3) registration for multiple e-mail accounts or domain names that are then used to establish false identities for transmitting spam.

More recently, spammers have resorted to hijacking vast blocks of Internet addresses—so-called "zombie netblocks"—from which spammers attempt to hide the scope of their activities by sending their e-mail in small quantities from literally thousands of different places. Additionally, there has been a sharp upsurge in spammers' surreptitious use of innocent parties' Internet servers—the so-called "open proxies"—by which spammers convert computer servers to e-mail processing

[1] *AOL v. CN Productions,* Court Order and Memorandum Opinion (10/25/02) at pp. 24-25, available at http://legal.web.aol.com.

facilities for their spam, once again concealing both the true source and scope of their e-mail activities. The most alarming recent development is spammers' increasing use of computer viruses to turn the computers of consumers with residential broadband connections into an unwitting "stealth" network for spam transmission.

"Outlaw" spam has increased alarmingly in the past year, and we believe that this dramatic growth underlies the astonishing increase in overall spam volume. These spammers are hijacking the computer resources and bandwidth of private consumers and businesses large and small, threatening to overwhelm the entire online medium.

We are particularly pleased that both H.R. 2214 and H.R. 2515 contain criminal prohibitions addressing these abuses, as well as ISP civil remedies that set statutory damage penalties. We look forward to working with the Subcommittees, this Committee and the Judiciary Committee on several refinements to make these prohibitions even more effective.

Federal legislation also can serve an additional important purpose by establishing baseline rules of the road for those advertisers who use the e-mail medium to reach consumers, but who do not use "outlaw" transmission tactics. Such rules, combined with industry standards and new spam-fighting technologies developed by relevant stakeholders, will help ensure that marketers use e-mail responsibly, and also will enhance the ability of consumers to make choices, through the use of technology filters, about the kinds of email they wish to receive.

We are pleased that Members of the Subcommittees and the full Committee have taken an interest in addressing the spam problem and are working to advance legislative solutions.

In the meantime, AOL is committed to maintaining a leadership role in the fight against spam. The goodwill and trust of our members depends on our continued focus on developing solutions to this problem. Spam continues to be the number one issue that we hear about from our members, and is AOL's number one customer satisfaction priority. AOL will continue to pursue strong enforcement actions and innovate our spam fighting tools—giving our members even greater control. But ultimately, we believe the spam battle must be fought on many fronts simultaneously in order to be successful. From technology to education, from legislation to enforcement, industry and government can work together to reduce spam significantly and give consumers control over their e-mail inboxes.

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

Mr. STEARNS. Thank you very much.

Mr. Rubinstein.

STATEMENT OF IRA RUBINSTEIN

Mr. RUBINSTEIN. Chairman Upton and members of the subcommittee, my name is Ira Rubinstein, and I am an associate general counsel at Microsoft Corporation. Thank you for this opportunity to share Microsoft's views on an issue that needs the attention of Congress and the work of your subcommittees: The adoption of effective anti-spam legislation that complements technological and industry-based measures and strengthen existing enforcement tools. We commend you for taking on an issue that harms millions of American consumers and businesses every day.

Microsoft supports the legislation introduced by Chairman Tauzin and Representative Burr as well as legislation introduced by Representatives Wilson and Green, both of which are co-sponsored by several members of the subcommittees. These proposals will help strengthen existing enforcement mechanisms, including the abilities of ISPs to prosecute spammers on behalf of their customers and give law enforcement and the FTC additional means to penalize spammers. They also include important civil and criminal penalties that will help make fraudulent spammers more accountable and deter would be spammers from sending fraudulent e-mail to consumers. We commend the sponsors of these bills for their

leadership and are grateful that these proposals contain these important elements.

In my written testimony, I discuss Microsoft's technological advancements to help fight spam and our cooperation with law enforcement around the world to prosecute fraudulent spammers. Today, however, I want to address how Congress can enable technology to win the battle against spam. To date, the fight against spam has been largely devoted to filtering, which automatically screens e-mail messages and blocks those determined to be spam. Filtering has proven to be a critical mechanism to reduce the volume of spam. Microsoft filters block over 2.4 million spam messages a day from reaching our customers, but filters are in an arms race with the ever-growing volume of spam. Today, because filters do not have detailed information about senders, they sometimes capture wanted e-mail and let spam through. However, there a number of ways to improve filtering. By providing filters with more information about senders of commercial e-mail, we can reduce spam volume with minimal impact on accuracy of filters, thereby improving consumers' confidence in the e-mail messages they receive and their willingness to opt out from unwanted e-mail.

Both industry and government have important roles to play in helping filters work better. Industry can help by creating organizations that will establish commercial e-mail guidelines and certify senders who follow such guidelines through seals that can be identified by filters and seen by customers. Similar organizations already help in protecting consumers' privacy online. For example, think of TRUSTe and BBBOnline. Backed by sufficient industry support, e-mail best practices could similarly help spam filters and consumers distinguish between legitimate businesses and unlawful spammers.

Government can help by jump starting independent e-mail trust authorities through legislative initiatives. We believe legislation is necessary in this area because today, even though many individual companies are doing the right thing, there are no broadly adopted e-mail best practices. There is also no easy way for these companies to participate in such programs and show that they adhere to best practices. With a critical mass of participants, filters will work as intended and block unlawful spam from reaching consumers' inboxes.

To encourage the widespread adoption of e-mail best practices, a legislative incentive is needed. We suggest an ADV, or advertisement label, be put on all unsolicited commercial e-mail unless the sender comes within a safe harbor that requires membership in a best practice program. To be clear, we are not proposing a standalone ADV requirement; rather, we see it as a means to drive the widespread adoption of e-mail best practices. There are incentives other than ADV labeling that Congress could also select.

Without mandating a technology or one-size-fits-all solution, our safe harbor identifies several basic components that industry guidelines must incorporate, such as giving consumers notice of how e-mail addresses will be used and to whom they will be disclosed. But the proposal is market-based permitting industry to take the lead in developing specific guidelines within these parameters. We expect a number of industry safe harbor organizations to emerge.

We encourage the members of these subcommittees to include a legislative incentive that drives the widespread adoption of e-mail best practices in any anti-spam proposal. The importance of promoting technological solutions to fight spam should not overlooked.

In conclusion, we commend the subcommittees for holding this hearing today and appreciate your determination to seek strong legislation to help stem spam. Microsoft is committed to working with you to craft effective Federal anti-spam legislation. Thank you.

[The prepared statement of Ira Rubinstein follows:]

PREPARED STATEMENT OF IRA RUBINSTEIN, ASSOCIATE GENERAL COUNSEL, MICROSOFT CORPORATION

Chairman Stearns, Chairman Upton, Ranking Member Schakowsky, Ranking Member Markey, and Members of the Subcommittees: My name is Ira Rubinstein and I am an Associate General Counsel at Microsoft Corporation. I want to thank you for the opportunity to share Microsoft's views on an issue that needs the attention of Congress and the work of your subcommittees: the adoption of effective anti-spam legislation that complements technological and industry-based measures and strengthens existing enforcement tools. There are plenty of statistics that document with convincing evidence that spam presents an intolerable burden to consumers and network operators alike, but all the evidence most Americans need is to log on their computer in the morning and see a string of e-mails that are at best distractions and all too often are illegal or shocking.[1]

Microsoft is here today because the risk of inaction and the risk of not combating spam will render this vital communications medium so cluttered with interference that it will no longer be seen as a reliable and efficient communications tool. Spam filters are doing their best; indeed, Microsoft's filters block over **2.4 billion** spam messages a day. But the filters cannot keep up with the ever-growing volume of spam. And consumers, understandably, are quickly losing confidence in the value of their inboxes. We welcome the important work of the Subcommittees and the sponsors of anti-spam legislation and look forward to working with you to see that strong anti-spam legislation is passed to preserve e-mail as an important link in our society.

Microsoft brings to the debate on spam a perspective that sees the problem from different angles and reflects the policy balance facing the Subcommittees. As a provider of Internet and e-mail based services, Microsoft currently bears the bandwidth, storage, and software costs of processing spam and spends countless hours responding to customer concerns about their receipt of ever-growing amounts of junk e-mail. As a developer of filtering technology, we are constantly trying to prevent spam from clogging our e-mail system and stay a step ahead of spammers who use a range of illicit practices to avoid detection. And, as a company that uses e-mail to responsibly communicate with customers, we worry that our messages are getting lost in the noise of spam.

This perspective drives us to recommend a balanced, multi-pronged approach to combating spam. This approach depends on the combined efforts of industry and government, and includes the following elements:

(1) Developing and implementing new and more sophisticated technological tools to combat spam;
(2) Aggressive enforcement campaigns by both the private and public sector to penalize illicit spamming practices and deter others from engaging in these activities; and
(3) Federal legislation that strengthens existing enforcement tools and encourages the widespread adoption of e-mail best practices and a means for filters and consumers to identify senders that adhere to such practices.

First, I address the focus of this hearing—legislation to combat spam. I next turn to a discussion of technological developments and how we in industry are using our know-how to develop cooperative strategies to track down spammers. I then describe

[1] Last year, an estimated 1.8 billion spam e-mails were sent each day, accounting for nearly 40 percent of all e-mail sent over the Internet. This year, that number is expected to climb to well over 10 billion a day. That is over half of all e-mail sent worldwide and is up from 7 percent in 2001. *See* Jonathan Krim, "Spam's Cost to Business Escalates," *Washington Post* March 13, 2003 at A1 (citing study conducted by Brightmail Inc.).

some of our recent enforcement actions against spammers and our work with law enforcement around the world to combat this growing problem.

STRONG FEDERAL ANTI-SPAM LEGISLATION IS NEEDED

Microsoft supports strong federal anti-spam legislation because the current legal and regulatory regime is simply not up to the task. Although ISPs have achieved some success in using litigation and other techniques to police spam, existing laws need to be strengthened to focus on the problems raised by spam, such as the forging of sender information, that make it difficult to prosecute spammers successfully. Also, the spam problem is not one that can be eradicated through the efforts of Microsoft and other ISPs alone. For these reasons, we support federal anti-spam legislation that strengthens existing enforcement mechanisms, including the ability of ISPs to prosecute spammers on behalf of their customers, and provides both law enforcement and the FTC with additional means to penalize spammers. A number of important legislative proposals have been introduced along these lines, including H.R. 2214 and H.R. 2515, and we commend the sponsors of these bills for their insight and look forward to continuing to work with them to craft effective anti-spam legislation.

As the Subcommittees consider these proposals and seek to write legislation, we urge you to adopt:

- **Incentives for legitimate marketers to distinguish themselves and thereby improve technology.** Legislation has a role to play in supporting effective filtering technology by creating incentives for e-mail marketers to adopt e-mail best practices and to certify themselves as trusted senders who can be more easily identified by consumers and filters alike. Promoting technology in this fashion is an important addition to any anti-spam proposal.
- **Strong civil and criminal penalties for fraudulent e-mails.** Anti-spam legislation should prohibit the use of false or misleading header information (including source, destination and routing information), false or misleading subject lines, and the misuse of third-party domain names and IP addresses. It also should capture all bad actors involved in the chain of sending fraudulent e-mail.
- **Effective ISP, State AG and FTC Enforcement.** Enforcement is a critical component of attacking the spam problem. ISPs and law enforcement currently invest considerable time and effort to locate and prosecute spammers on behalf of their customers. Anti-spam legislation should support these efforts and not raise roadblocks—such as burdens of proof or affirmative defenses—that will inhibit meaningful enforcement.
- **Express language that preserves ISPs' right to combat spam.** ISPs have the incentive to combat spam; it is essential that ISPs maintain the ability to do so. Any anti-spam law should expressly state that its provisions do not impose an obligation upon ISPs to carry or block certain types of e-mail messages. Such a provision would not shelter ISPs from liability for filtering; rather, it would simply clarify that the anti-spam law does not grant senders of e-mail messages new rights that they do not have today.
- **Federal preemption with appropriate carve outs.** Federal preemption of state statutes that regulate the sending of commercial e-mail messages is needed, provided the federal anti-spam law contains strong substantive requirements. However, ISPs rely heavily on state contract and trespass laws, as well as laws relating to computer fraud and theft, in their fight against spammers. Thus, preemption in any anti-spam law should carve out such important state laws.

Industry Best Practices Buttressed by Strong Enforcement

These legislative principles seek to enhance existing anti-spam technologies and leverage the self-regulatory features of a best-practices regime with serious, and necessary, enforcement mechanisms. To date, much of the effort in the fight against spam has been devoted to "filtering," which involves the automatic analysis of e-mail messages to determine whether or not they are spam. Once a filter has determined that a message is spam, the e-mail system can take appropriate action, such as placing the message in a Junk Mail folder or deleting it prior to delivery. Filtering has proven to be a useful and necessary mechanism to reduce the volume of spam traveling over ISP and corporate networks.[2] Already, filters on the servers at

[2] An internal IT consultant at a Fortune 50 energy company conservatively estimates that filtering enables the company to save between $100 and $200 million per year. *See* Meredith Levinson, "Seething Over Spam," CIO, Jan. 2003, *available at* http://www.cio.com/archive/111502/et—article.html.

MSN and Hotmail block more than **2.4 billion** messages a day, before they ever reach our customers' inboxes.

Even with the passage of legislation, filtering will continue to play an essential role, both as a means of dealing with those who ignore or are beyond the scope of the law (*e.g.,* foreign spam) and to help consumers manage their inboxes. But technology needs help. Today, because filters do not have detailed information about senders, they may misclassify legitimate e-mail as spam (producing so-called "false positives") and mistakenly fail to catch all spam (producing "false negatives"). By providing filters with more information about senders of commercial e-mail, we can reduce the risk of these types of mistakes and we can improve consumer's confidence in the e-mail messages they receive.

Both industry and government have important roles to play in enabling filters to work better. Industry can help by creating independent e-mail trust authorities that will establish commercial e-mail guidelines and certify senders who follow such guidelines through "seals" that can be read by filters and understood by consumers. Similar authorities already help in protecting consumer's privacy online, with organizations such as TRUSTe and BBBOnline providing certification for websites that follow certain privacy guidelines. Backed by sufficient industry support, e-mail best practices could similarly help distinguish between legitimate businesses and spammers.[3]

Government can help by "jump starting" the creation of and participation in independent e-mail trust authorities. Today, few industry members follow broadly adopted e-mail guidelines and even fewer utilize technology to show that their messages adhere to such guidelines. An effective way to encourage marketers to adopt e-mail best practices is to give them an incentive to do so. Our proposal is that an advertisement or "ADV:" label be put on all unsolicited commercial e-mail unless the sender comes within a Safe Harbor that requires membership in an FTC-approved self-regulatory organization that complies with certain e-mail best practices. We want to make it clear that we are not proposing a stand-alone "ADV:" requirement but rather see it as a means to drive the widespread adoption of e-mail best practices. There may be other sound ideas on giving industry incentives to adopt e-mail best practices but use of the "ADV:" label has the additional benefit of allowing consumers to easily identify unsolicited commercial e-mail and to customize their spam filters to either deliver such mail or automatically delete it.

Without mandating a technology or one-size-fits-all solution, this Safe Harbor proposal identifies several basic components that industry guidelines must incorporate, such as notice to consumers regarding the use and disclosure of their e-mail addresses. But the proposal is market-based, permitting industry to take the lead in developing specific guidelines that go above and beyond the basic e-mail best practices identified. This will allow industry self-regulatory organizations to emerge and compete on the basis of the strength of the e-mail practices they certify and on their enforcement. The Safe Harbor proposal also gives the FTC the authority to ensure e-mail trust authorities adopt e-mail practices that satisfy legislative requirements. Participants that fail to live up to the guidelines would face involuntary termination and mandatory public reporting. In addition, such participants would be referred to the FTC, thus providing the FTC with an additional enforcement tool.

Critics claim that industry can do this on its own and therefore legislation is not necessary. But without appropriate incentives, there is no guarantee that a critical mass of industry members will certify their adherence to industry e-mail best practices. Without a critical mass, makers and users of spam filtering software will not bother to modify their software to recognize senders that participate in e-mail best practice programs. If only a few makers of email software modify their software to recognize such participants, few, if any, senders will comply because it would not be worth the expense.

On the other hand, with a critical mass of participants, developers and users of spam filtering software would find it very useful to use a certificate of compliance with e-mail best practices as a means to help them avoid filtering good mail. In addition, legitimate senders would find it worth their cost to sign up. Better yet, if most or all legitimate mail senders sign up, then any remaining commercial e-mail would be from those unlawful spammers who do not abide by e-mail best practices and such e-mail could be filtered aggressively. In the end, filters would work as intended and block unlawful spam from reaching consumers' inboxes.

Microsoft believes that the widespread adoption of e-mail best practices along with a method to associate e-mail communications from businesses that adopt such best practices will ameliorate many of the problems currently associated with spam.

---

[3] One program that has established guidelines for e-mail communications is described at http://www.postiva.com/article/sitemap.

Consumers will be able to exercise choice since they can recognize e-mails from businesses that follow e-mail practices with which they are comfortable; businesses will be able to distinguish their legitimate electronic communications from spam; and filters will be better equipped to identify e-mail communications from legitimate senders, thereby reducing false-positive and false-negative problems.

SPAM THREATENS VIABILITY OF E-MAIL AS A COMMUNICATIONS MEDIUM

The reason why strong federal anti-spam legislation is needed is because spam plainly threatens the viability of what has become a critical communications medium. The anti-spam software company Brightmail has projected that at least half of all e-mails individuals and businesses receive will be spam by September 2003 or earlier.[4] By 2007, unless significant changes are made, it is estimated that more than 70 percent of all e-mail messages will be spam.[5]

The reason for this exponential growth is simple: spam is cheap and easy to send. For roughly ten dollars a month, a spammer can obtain an ISP account and for another thirty dollars, websites such as BulkBarn.com offer all of the following: 300,000 "fresh bulk e-mail addresses" a week, bulk e-mail starter kits, and free bulk e-mail software.[6] Using such systems, spammers can send 650,000 e-mails per hour from an inexpensive mail server. And given that 100 responses for every 10 million messages sent can generate a profit, spammers have no financial incentive to stop the massive junk mailings.[7] There is little reason for a spammer to limit the number of messages sent, or be selective about the chosen recipients, since the marginal cost of every additional message is effectively zero.

Of course, spam is cheap to send, but not to receive. Ferris Research estimates that spam will cost U.S. corporations more than $10 billion in 2003.[8] This figure includes productivity losses and the additional equipment, software, and manpower needed to combat the problem. According to some analysts, it costs roughly $250 to send a million spam messages, but it costs about $2,800 in lost wages, at the federal minimum wage, for those same million spam messages to be deleted.[9] And spam impacts all organizations, big and small. IDC estimates that for a company with 14,000 employees, the annual cost to fight spam is $245,000.[10]

ISPs are hit particularly hard by the spam problem. They spend millions of dollars each year because of spam, implementing and updating filtering software, providing additional server space and processor power to deal with the high volumes of e-mail, and giving support to customers frustrated by the receipt of a barrage of unwanted messages. In addition, the transport and delivery of spam places significant stress on ISPs' mail servers, delaying the speed and effectiveness of all e-mail communications and causing system outages.

Spam also harms the ability of legitimate businesses to use e-mail to communicate with existing customers. Many businesses are simply afraid to use e-mail to contact their customers for fear of being branded spammers. Others are concerned that their e-mails will not be found among the mass of spam filling up most consumers' in-boxes. This is of particular concern for critical service industries such as security and insurance firms, where customer contact is regulated and necessary and the communication vehicle they use must be reliable.

The economies of spam favor the abusers and disfavor the victims—i.e., consumers. Consumers are forced to spend time and energy assessing, reviewing, and discarding spam. In a study recently released by Symantec Corporation, 65 percent of the 1,000 people surveyed reported spending more than 10 minutes each day dealing with spam.[11] And 37 percent of the survey respondents indicated that they

---

[4] PR Newswire, "Spam on Course to Be Over Half of All E-mail This Summer," July 1, 2003.

[5] ePrivacy Group, "Spam: By the Numbers" (2003), *available at* http://www.eprivacygroup.com (citing Radicati Group).

[6] Melissa Solomon, "The Other Side," *Computerworld,* November 11, 2002, *available at* http://www.computerworld.com/softwaretopics/software/groupware/story/0,10801,75736,00.html.

[7] ePrivacy Group, "Spam: By the Numbers" (2003), *available at* http://www.eprivacygroup.com (citing the *Detroit Free Press*); Mylene Mangalindan, "For Bulk E-mailer, Pestering Millions Offers Path to Profit," *Wall Street Journal,* November 13, 2002.

[8] Scott Bekker, "Spam to Cost U.S. Companies $10 Billion in 2003," *ENT News,* January 9, 2003, *available at* http://www.entmag.com/news/article.asp?EditorialsID=5651 (citing conclusions of Ferris Research study). [*can we cite to actual Ferris Report?*]

[9] Theo Emery, "Meeting Takes Aim at Spam," *Associated Press* (citing researcher at MIT), *available at* http://www.ohio.com/mld/beaconjournal/business/5028845.htm.

[10] Jonathan Krim, "Spam's Cost to Business Escalates," *Washington Post,* March 13, 2003 at A1, *available at* http://www.washingtonpost.com/ac2/wp-dyn/A17754-2003Mar12 .

[11] News Release, "Symantec Survey Reveals Growing Concerns Over Spam," http://www.symantec.com/press/2002/n021202.html.

received more than 100 spam messages each week.[12] Consumers also must contend with e-mail messages that use misleading subject lines to induce them—or, worse, their children—into viewing messages that contain sexually explicit material. According to Symantec's survey, 69 percent of respondents agreed or strongly agreed that spam is generally harmful to e-mail users. In addition, 77 percent of respondents with children under the age of 18 noted that they are concerned or very concerned about their children reading spam.[13]

From virtually any perspective, spam has become a significant problem that threatens to cripple the worldwide e-mail system. Consumers are walking away from their e-mail accounts because they simply can't deal with the problem. It is time for the private and public sectors to come together to preserve the viability of this critical communications medium.

INDUSTRY IS DEVELOPING NEW TECHNOLOGICAL TOOLS TO COMBAT SPAM

We recognize that federal legislation alone is not sufficient to combat spam. This is why a critical element of Microsoft's multi-faceted anti-spam strategy focuses on developing new and more sophisticated technological tools. Recognizing the increasing importance of fighting spam on behalf of our customers, we recently created a new Anti-Spam Technology and Strategy Group that brings together specialists from across the company and integrates all of our anti-spam strategy and R&D efforts. The combined efforts and expertise of this group has enabled us to create new anti-spam technologies that are even more precise, easier to use, and adaptable. We are working to integrate them into more of our products, particularly MSN, Hotmail, Outlook and Exchange.

For example, MSN 8 employs machine-learning technology to enable customers to train their filters to separate desirable e-mail from undesirable spam. It also uses a collection of more than 200 million e-mail addresses, called a Probe Network, to attract spam before it is delivered to a customer's e-mail inbox. Finally, it allows customers to choose from three levels of filtering protection to capture certain types of incoming e-mails, or they can choose to receive e-mails only from individuals who are on their "safe lists." Microsoft also recently updated MSN 8 with further improvements in its spam technologies, giving customers an option to block offensive images in e-mail, and adding the ability to filter mail in languages besides English.

Microsoft also recently announced the inclusion of new anti-spam technologies in our new Exchange Server 2003 for partners. One tool allows partners to integrate their anti-spam solutions with Exchange Server 2003 functions. Partner solutions will be able to scan incoming e-mail messages and attach a numeric score, or "Spam Confidence Level" (SCL), to each message. The SCL indicates the probability that the message is spam, and based on a threshold set by an administrator, the message will be forwarded to either the recipient's inbox or junk mail folder. Exchange 2003 also allows administrators to assign enterprise-wide "allow/deny" lists and to integrate real-time black hole list services, which provide immediate spam blocking if a sender is a known spammer. In addition to its anti-spam tool, Exchange Server 2003 works with junk mail filters in Microsoft Office Outlook 2003. These filters allow users to block content using default settings, assign "safe" and "block" lists, automatically file junk mail to their trash folders, and profile spam by assigning points or scores to certain keyword identifiers.

Microsoft has also joined forces with other ISPs to better enable systems operators and consumers to block and filter spam. In April, Microsoft, AOL and Yahoo! announced a wide-ranging set of initiatives to fight spam together. Since then, Earthlink has joined the effort, which involves promoting business guidelines, best practices and technical standards that can help curb spam sent or received via any online service or computing platform.

As an example of our combined work in this regard, we are working on a new initiative aimed at eliminating the common practice of "domain spoofing" where spammers substitute fictitious sending addresses and even remove all origination data to mask their true identity and location. Under this initiative, software used in transmitting and receiving e-mail will be able to determine whether a message that claims to originate from fred@example.com was actually sent from example.com. Spam filters can then take into account evidence of a spoofed domain when deciding whether or not a message is spam. This simple change alone will help filter out a significant percentage of spam.

ISPs are working together to support other anti-spam technological advancements, including restricting e-mails from systems determined to be open to unau-

[12] *Id.*
[13] *Id.*

thorized use (such as open relays, open routers, or open proxies). We are also working together to share information about spammers who set up many different e-mail accounts to avoid detection. This will help put an end to this game and shut spammers down more effectively.

ENFORCEMENT IS A CRITICAL COMPONENT OF COMBATING SPAM

Enforcement is another critical element of our multi-pronged approach to fighting spam. On June 16, Microsoft filed 15 lawsuits in the United States and the United Kingdom against companies and individuals alleged to be responsible for billions of spam messages sent in violation of state and federal laws. We have undertaken this enforcement campaign in response to the thousands of subscriber complaints received every day. Like other providers or Internet access and e-mail services, our top priority is ensuring that our subscribers feel comfortable using e-mail to communicate.

Our aggressive litigation campaign is targeted at stopping some of the most offensive e-mail practices affecting Microsoft customers. In some cases, defendants are alleged to have used deceptive and misleading subject lines to disguise e-mail messages that actually contained pornographic images, dating service solicitations and other adult services. One case involves e-mail messages that include a false virus warning. Recipients are instructed to download an "update" purported to protect their system, when in fact the download is nothing more than a toolbar that appears to track their movements on the Internet. In other cases, defendants are alleged to have "spoofed" the sender's e-mail address, making it seem that the spam originated from hotmail.com or other recognized senders. Among the defendants in the lawsuits are several individuals and entities that are listed as known spammers on Internet registries that monitor spam activities worldwide.

Microsoft will continue to work with law enforcement around the world to enhance their enforcement efforts against spammers who rely on fraudulent means of transmission to circumvent anti-spam filters and mislead recipients. Such efforts will include: (1) developing better mechanisms for preserving electronic evidence relating to spammers' activities; (2) coordinating among ISPs and industry members to help ensure that anti-spam enforcement efforts are most effectively deployed against spam senders who cause the greatest impact on consumers; and (3) similarly coordinating in referring spammers for civil or, where appropriate, criminal enforcement actions. The goal of this effort will be to make spammers more accountable and to deter would-be spammers from using such "outlaw" techniques to send e-mail to consumers.

Spam is a serious problem and the public and private sectors must coordinate on a broad response if we are going to be effective in addressing it. We believe that a multi-faceted approach is needed: better technology tools to enable consumers to keep spam from getting to their computer screens; more collaboration among the industry leaders so we can combine our resources; aggressive enforcement against people who are breaking the law; and effective federal anti-spam legislation that strengthens enforcement tools and enables technology to work better for the benefit of consumers. We commend the Subcommittees for holding this hearing today and appreciate your determination to seek strong legislation to help combat spam. And we thank you for extending us an invitation to share our experience and recommendations with you. Microsoft is committed to working with you to craft effective federal anti-spam legislation that will thwart the efforts of those who abuse e-mail and preserve the viability of the medium.

Mr. BURR [presiding]. I thank the gentleman.

The Chair recognizes Mr. Misener for opening statement.

STATEMENT OF PAUL MISENER

Mr. MISENER. Thank you, Mr. Chairman, very much and good afternoon. My name is Paul Misener. I am Amazon.com's vice president for Global Public Policy. Thank you very much for inviting me to testify this afternoon.

Mr. Chairmen, Amazon.com deplores spam. We find it annoying and often offensive and increasingly designed to defraud, confuse or trick consumers. Therefore, tempered by the recognition that legitimate businesses occasionally make honest mistakes, we ask that you pass a strong, effective, nationwide anti-spam law.

It almost goes without saying that spam annoys and often offends consumers. At very little cost to themselves, spammers cram our e-mail boxes full of messages from shady businesses about questionable products and services and often in ways that shock even the most worldly adults. The sheer volume of spam makes it increasingly difficult for consumers to receive the e-mail, both personal and commercial, they want. Accordingly, Amazon.com's practice is to never spam. We send e-mail only to those individuals—our customers—with whom we have an extant relationship. And we provide our customers thorough choice mechanisms that allow them to determine for themselves how much, if any, e-mail they receive from Amazon.com. We believe this is simply good, pro-customer business practice.

But spam has become even worse than annoying and often offensive. Spam is increasingly used to defraud, confuse and trick consumers. Many employ well-known fraud schemes, others may be more subtle, yet use fraud techniques that predate e-mail communications. Offers to get rich quick, lose weight fast and find a date nearby are nothing new and are common in spam. Although efforts to confuse consumers are somewhat more sophisticated, spammers use classic sleights of hand, such as subject lines that entice recipients to open e-mails they otherwise would not. Examples are commercial e-mails that use highly informal or personal subject lines. The confusion doesn't last long, however, for once a consumer opens the message and finds an advertisement for diet pills the sleight of hand becomes obvious. This spam approach is not unlike common physical mail advertisements that are intentionally shaped, formatted and colored to look like a check. The whole idea is to get consumers to open the envelope but, once inside, the deception is over.

Increasingly, however, Amazon.com has observed, and been a victim of, highly sophisticated techniques that convincingly trick consumers into thinking that an e-mail is coming from a reputable sender. This kind of deception is particularly insidious because the fraud not only involves what is said or how it is said but who purportedly is saying it. Indeed, over the past few months, many consumers have received commercial e-mails from addresses such as frank@amazon.com or sally@amazon.com, but such e-mails were not sent by Amazon.com or anyone who works for the company. They are part of a growing problem called "spoofing," whereby headers of commercial e-mails are intentionally forged to appear to come from reputable companies or individuals. Technological solutions to the spoofing problem are elusive.

Legal solutions are somewhat more promising. Current law, however, could be dramatically improved with new, nationwide, anti-spam legislation. Amazon.com is very grateful, Mr. Chairmen, that you and members of your subcommittees here are working on such legislation in a bi-partisan fashion, in close cooperation with the Judiciary Committee. We particularly appreciate the strong national policy that would be established by passing an anti-spam law this year and would support the inclusion of a provision that would allow the FTC to prosecute knowing beneficiaries of spam, not just the spammers themselves. But on behalf of our customers and company, Amazon.com will support particular anti-spam legislation

only if it recognizes that legitimate businesses occasionally make honest mistakes that should not be proscribed. Please allow me to explain.

Because commercial e-mail necessarily involves computers and human programmers, there have been and will continue to be occasional e-mail mistakes, no matter how many preventative measures are taken. Such truly honest mistakes are rare and certainly are not the cause of the in-box clutter and associated consumer angst that have led us all to this point. Of the acts that would be prohibited by the comprehensive anti-spam bills now before the House, honest mistakes are obviously plausible only for accidentally sending e-mail to individuals who have opted-out of receiving them. Proscribing such mistakes would have the perverse effect of discouraging e-mail use by the most reputable companies. Amazon.com believes that H.R. 2214 and H.R. 2515 would wisely distinguish between actions that may plausibly be mistakes and those that almost certainly involve unlawful intent. They would require plaintiffs complaining of commercial e-mail being sent after an opt-out choice to allege with particularity that the defendant has engaged in a, quote, "pattern or practice" of ignoring such choices. No such pattern or practice allegation would be needed for complaints regarding, for example, false headers.

In conclusion, Mr. Chairman, Amazon.com deplores spam. On behalf of our customers and company, and tempered by the recognition that legitimate businesses occasionally make honest mistakes that should not be proscribed, Amazon.com respectfully asks that you pass strong, effective, nationwide anti-spam legislation this year. Thank you again for asking me to testify, Mr. Chairman. I look forward to your questions.

[The prepared statement of Paul Misener follows:]

PREPARED STATEMENT OF PAUL MISENER, VICE PRESIDENT FOR GLOBAL PUBLIC POLICY, AMAZON.COM

Good morning, Chairman Upton and Chairman Stearns; Mr. Markey and Ms. Schakowsky; and members of the Subcommittees. My name is Paul Misener. I am Amazon.com's Vice President for Global Public Policy. Thank you very much for inviting me to testify today.

Messrs. Chairmen, Amazon.com deplores spam. We find it annoying and often offensive and increasingly designed to defraud, confuse, or trick consumers. Therefore, tempered by the recognition that legitimate businesses occasionally make honest mistakes, we ask that you pass a strong, effective, nationwide anti-spam law.

SPAM ANNOYS AND OFTEN OFFENDS CONSUMERS

Messrs. Chairmen, it almost goes without saying that spam annoys and often offends consumers. At very little cost to themselves, spammers cram our email boxes full of messages from shady businesses, about questionable products and services, and often in ways that shock even the most worldly adults. The sheer volume of spam makes it increasingly difficult for consumers to receive the email, both personal and commercial, they want.

AMAZON.COM'S PRACTICE IS TO NEVER SPAM

Accordingly, Amazon.com's practice is to never spam. We send email only to those individuals—our customers—with whom we have an extant relationship. And we provide our customers thorough choice mechanisms that allow them to determine for themselves how much—if any—email they receive from Amazon.com. We believe this is simply good, pro-customer business practice.

SPAM IS INCREASINGLY USED TO DEFRAUD, CONFUSE, OR TRICK CONSUMERS

But spam has become even worse than annoying and often offensive. Spam is increasingly used to defraud, confuse, or trick consumers. Many employ well-known fraud schemes, such as the infamous Nigerian businessman hoax. Others may be more subtle, yet use fraud techniques that predate email communications: offers to get rich quick, lose weight fast, and find a date nearby are nothing new, but are common in spam.

Although efforts to confuse consumers are somewhat more sophisticated, spammers still use classic sleights of hand, such as subject lines that entice recipients to open emails they otherwise would not. Examples are commercial emails that use highly informal or personal subject lines like, "Party Next Week!" or "how's it going?" The confusion doesn't last long, however, for once a consumer opens the message and finds an advertisement for diet pills the sleight of hand becomes obvious. This spam approach is not unlike common physical mail advertisements that are intentionally shaped, formatted, and colored to look like a check. The whole idea is to get consumers to open the envelope but, once inside, the deception is over.

Increasingly, however, Amazon.com has observed—and been a victim of—highly sophisticated techniques that convincingly trick consumers into thinking that an email is coming from a reputable sender. This kind of deception is particularly insidious because the fraud not only involves what is said or how it is said, but who purportedly is saying it.

Indeed, over the past few months, many consumers have received commercial emails from addresses such as frank@amazon.com or sally@amazon.com. But such emails were not sent by Amazon.com or anyone who works for our company. They are part of a growing problem called "spoofing," whereby headers of commercial emails are intentionally forged to appear to come from reputable companies or individuals.

Technological solutions to the spoofing problem are elusive. At the network level, shortcomings in the underlying email software communications protocols make spoofing relatively easy to accomplish, yet virtually impossible to stymie. And, at the local consumer level, filtering software cannot effectively block spoofed messages without also blocking many legitimate ones. Legal solutions are somewhat more promising. Amazon.com and other companies are investigating spoofing incidents and considering a variety of civil actions. We also are aware that the FTC and state attorneys general have brought and are considering additional civil and criminal fraud or trade practice actions.

AMAZON.COM SUPPORTS ANTI-SPAM LEGISLATION

Current law, however, could be dramatically improved with new, nationwide, anti-spam legislation. Amazon.com is very grateful, Messrs. Chairmen, that you and members of your Subcommittees are working on such legislation, in a bi-partisan fashion, and in close cooperation with members of the Judiciary Committee. We particularly appreciate the strong, national policy that would be established by passing an anti-spam law this year, and we would support the inclusion of a provision that would allow the FTC to prosecute knowing beneficiaries of spam, not just the spammers themselves. But, on behalf of our customers and company, Amazon.com will support particular anti-spam legislation only if it recognizes that legitimate businesses occasionally make honest mistakes that should not be proscribed.

Please allow me to explain.

HONEST, INFREQUENT MISTAKES SHOULD NOT BE PROSCRIBED

Because commercial email necessarily involves computers and human programmers, there have been and will continue to be occasional email mistakes, no matter how many preventative measures are taken. Such truly honest mistakes are rare and certainly are not the cause of the in-box clutter and associated consumer angst that have led us all to this point. Not only are these mistakes expected and essentially not preventable, the harm to consumers is minimal, and there already are strong market forces at work: Reputable companies simply do not want to irritate consumers who have asked not to be bothered.

Of the acts that would be prohibited by the comprehensive anti-spam bills now before the House, honest mistakes are obviously plausible only for accidentally sending email to individuals who have opted out of receiving them. Proscribing such mistakes would have the perverse effect of discouraging email use by the most reputable—and thereby most exposed—companies. Every day, Amazon.com sends tens of thousands of emails to our customers and, thus, just one simple mistake (such as accidentally sending a notice of a new jazz CD release to customers who have

elected not to receive email on jazz music), could expose us to astronomical penalties. Surely, this is not the goal of anti-spam legislation. And, of course, the other acts that would be prohibited by the anti-spam bills—such as falsifying email headers—are so necessarily intentional or systematic that it would be implausible to claim that they are merely the result of honest mistake.

Amazon.com believes that H.R. 2214 and H.R. 2515 would wisely distinguish between actions that may plausibly be mistakes and those that almost certainly involve unlawful intent. They would require plaintiffs complaining of commercial email being sent after an opt-out choice to allege with particularity that the defendant has engaged in a "pattern or practice" of ignoring such choices. No such pattern or practice allegation would be needed for complaints regarding, *e.g.*, false headers.

Importantly, the "pattern or practice" language in these House bills would not create a loophole for the real spammers to escape punishment. In the first place, to reiterate, it does not apply to the prohibited acts that almost certainly are intentional or systematic, such as the falsification of header information; rather, it would only apply in the circumstance where an email is sent to an individual who has opted out of receiving such email. Moreover, true spammers do not have legitimate businesses that would occupy the vast majority of their emails. As a business necessity, spammers simply must have a pattern or practice of spamming, not just send an occasional spam. In other words, it will be very easy to tell the difference between the honest, infrequent mistakes of companies not in the spam business from the true spammers, who must spam most or all of the time.

CONCLUSION

In conclusion, Mr. Chairman, Amazon.com deplores spam. On behalf of our customers and company, and tempered by the recognition that legitimate businesses occasionally make honest mistakes that should not be proscribed, Amazon.com respectfully asks that you pass strong, effective, nationwide anti-spam legislation.

Thank you again for inviting me to testify. I look forward to your questions.

Mr. BURR. Thank you very much.

The Chair would recognize Mr. Hirschman for the purposes of an opening statement.

STATEMENT OF KENNETH HIRSCHMAN

Mr. HIRSCHMAN. Thank you, Mr. Chairman. Mr. Chairman and members of the committee, thank you for inviting me to testify. My name is Ken Hirschman, and I am general counsel of Digital Impact. Digital Impact is a provider of online direct marketing solutions for enterprises, including numerous Fortune 500 companies who have embraced permission-based e-mail as a viable and efficient customer communication and marketing tool. Digital Impact is also a founding member of the E-mail Service Provider Coalition of the Network Advertising Initiative, which was formed to represent the interests of e-mail service providers. Thirty-four other e-mail service providers have joined Digital Impact in the E-mail Service Provider Coalition, all of which are struggling with the onslaught of spam and the emerging problems related to the deliverability of legitimate and wanted e-mail.

E-mail service providers enable their customers to deliver volume quantities of e-mail messages. While E-mail Service Providers serve the marketing needs of the business community, marketing is by no means the only focus of E-mail Service Providers. E-mail Service Providers also deliver transactional messages, such as account statements, airline confirmations and purchase confirmations, e-mail publications, such as online newsletters, affinity messages and relational messages.

We believe that much can be done to solve the problem of spam. At the most fundamental level, we believe that we need to create accountability within the e-mail delivery system. Spammers spend

their days inventing new methods to obscure and falsify their identity in order to sneak past existing filters and avoid accountability. Legitimate e-mail service providers would never engage in such practices. We believe through a combination of Federal legislation and technology we can bring accountability to e-mail.

Part of the problem in treating the spam epidemic is that spammers enjoy anonymity. Spammers hide behind open relays, as I said before, they forge their identity, and they deceive recipients with misleading from and subject lines. Make no mistake, the business of spamming is one of fraud and deception. The E-mail Service Provider Coalition recently proposed an architectural blueprint to respond to this problem. The blueprint, called Project Lumos, is designed to force senders of volume e-mail to incorporate authenticated identification into every message sent. The use of authenticated identification, together with a rating of sending practices over time, prevents spammers from hiding behind the technology of e-mail and forces all senders to be accountable for their sending practices. We have engaged with many of the major ISPs and other groups on this effort and are greatly encouraged by the traction our effort has gained since our launch just 3 months ago.

But technology isn't enough. The E-mail Service Provider Coalition strongly supports Federal legislation to respond to the growing menace of spam. We believe that strong preemptive Federal legislation will be a critical component in the successful resolution of the spam problem. One issue that has been raised in the discussion of proposed Federal spam legislation is that of a safe harbor. Such a provision would be welcome in this legislation as it would mandate accountability by requiring all mailers to identify themselves and adhere to standards of behavior in order to benefit from its protections. In addition, and probably more important, a safe harbor will offer redress to consumers that is not present in the proposed legislation.

Again, Digital Impact and the rest of the members of the E-mail Service Provider Coalition are very supportive of the Rid Spam Act. We will continue to work with staff on certain details of the bill, but we look forward to seeing a Federal law enacted this year. Mr. Chairman, on behalf of Digital Impact and the E-mail Service Provider Coalition, I want to pledge that we will continue to work with you and members of your staff. Spam is a complex problem and efforts to craft solutions must be thoughtful, robust and effective. Thank you and I look forward to any questions you may have.

[The prepared statement of Kenneth Hirschman follows:]

PREPARED STATEMENT OF KENNETH HIRSCHMAN, VICE PRESIDENT & GENERAL COUNSEL, DIGITAL IMPACT, INC.

Mr. Chairman and Members of the Committee, I want to thank you for inviting me to testify. My name is Ken Hirschman, and I am Vice President and General Counsel of Digital Impact, Inc. Digital Impact is the premier provider of online direct marketing solutions for enterprises, including numerous Fortune 500 companies who have embraced permission-based email as a viable and efficient customer communications and marketing tool.

Digital Impact is also a founding member of the Email Service Provider Coalition of the Network Advertising Initiative (NAI), which was formed to represent the interests of email service providers. Thirty-four other email service providers have joined Digital Impact in the ESP Coalition, all of which are struggling with the onslaught of spam and the emerging problems related to the deliverability of legitimate and wanted email.

The NAI is a cooperative group of companies dedicated to resolving public policy concerns related to privacy and emerging technologies. In the past, the NAI has created self-regulatory programs for online ad targeting and the use of web beacons. The group has now turned its focus to the growing problem of spam and the related concern of email deliverability.

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

Email service providers enable their customers to deliver volume quantities of email messages. These messages originate from the full spectrum of the US economy—large and small businesses, educational institutions, non-profits, government agencies, publications, and affinity groups all use the services of ESPs to communicate with their customers, members and constituents. While ESPs often serve the marketing needs of the business community, we also deliver transactional messages (such as account statements, airline confirmations, and purchase confirmations), email publications, affinity messages and relational messages.

The ESP industry is robust and growing. Within the ESP Coalition, we estimate that the 35 members provide volume email services to over 250,000 clients. These customers represent the full breadth of the U.S. marketplace—from the largest multi-national corporations to smallest local businesses; from local PTAs to national non-profit groups and political campaigns; from major publications with millions of subscribers to small affinity-based newsletters.

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

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

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

THE THREAT OF SPAM AND THE SOLUTION(S) TO SPAM

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

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

The media and marketplace have been replete with spam solutions for years. Some of these solutions have performed commendably in the fight against spam. But the problem still exists and continues to grow. Increasingly, we are presented with the question: can anything be done?

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

So how do create accountability within the email system?

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

THE TECHNOLOGICAL COMPONENT

Part of the problem in solving spam is that spammers enjoy impunity through anonymity. Spammers hide behind open relays, they falsify their online identities (a practice popularly known as "spoofing") and they deceive recipients with misleading "from" and "subject" lines. Make no mistake—the business of spamming is one of fraud and deception.

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

The NAI recently proposed an architectural "blueprint" to respond to this problem. Essentially, the NAI's blueprint, called "Project Lumos," is designed to force senders of volume email to incorporate authenticated identification into every message sent. The use of authenticated identity, along with a rating of sending practices over time, prevents spammers from hiding behind the technology of email and forces all senders to be accountable for their sending practices. We have engaged with many of the major ISPs and other groups on this effort and are greatly encouraged by the traction our effort has gained since our launch of project Lumos in April of this year.

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

THE SOCIAL COMPONENT

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

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

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

THE LEGISLATIVE COMPONENT

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

In the United States today, 33 states have enacted some form of spam legislation. Many more are considering spam legislation in their current legislative sessions. Unfortunately, the standards applied by these statutes (and proposed in pending bills) are not harmonized. As a result, we have a crazy quilt of differing standards that has created an unnecessarily complex compliance system. To make matters worse, enforcement within the global medium of email is exceedingly difficult when limited by state boundaries. We need preemptive federal legislation to unify these standards and provide powerful tools to enforcement officials.

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

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

We have a very real example of what a private cause of action means when included in a spam statute. In the state of Utah, a spam statute was passed last year that allows for a private cause of action and class action suits. A single plaintiff's class action law firm in Utah has filed hundreds (and by some accounts, over a thousand) class action lawsuits under this statute. But the firm is not pursuing spammers. Given the cost and complexity of finding actual spammers, this firm has targeted leading companies and brands—using firm employees as plaintiffs and offering pre-complaint settlements for several thousands of dollars—knowing that companies would rather pay the nuisance value of these suits than submit to the costly process of proving their innocence. Perhaps most telling is the fact that there is no data to suggest that the amount of spam in Utah has been reduced by even one message.

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

Let me make one thing perfectly clear: the debate over "opt-in" or "opt-out", regardless of what standard is eventually adopted, will not result in the reduction of spam. Spammers rely on deception, not permission. They do not care about whether they have any sort of relationship with the recipient of the message. They pay no heed to all of the existing state laws regarding spam. The most restrictive "opt-in" spam statute will do nothing to dissuade spammers from sending their messages.

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

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

Again, we strongly support the RID SPAM Act. We will continue to work with staff on a few issues we have with the bill, but look forward to seeing a law enacted this year.

THE THREAT OF FILTERING AND BLACKLISTS

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

According to a report by Assurance Systems, in the fourth quarter of 2002, an average of *15% of permission-based email was not received* by subscribers to the major ISPs. Some ISPs had non-delivery rates that were startling: NetZero, 27%; Yahoo, 22%; AOL, 18%; Compuserve, 14%; and AT&T, 12%.

The same report for the third quarter of 2002 showed an average of 12% non-delivery rate for the major ISPs—*meaning that the filtering of permission-based email increased 25% in a single calendar quarter.* Some of the volume email campaigns within the Assurance Systems report had non-delivery rates as high as 38%.

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

One of the main drivers in the false positive problem is the emergence of blacklists. These are lists of alleged spammers that ISPs can use to filter incoming email. The blacklist operator builds a registry of IP addresses that they believe are associ-

ated with spam and makes it available publicly. Currently, there are an estimated 300 blacklists in operation.

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

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

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

CONCLUSION

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

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

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

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

Mr. STEARNS. I thank the gentleman.

Ms. Selis?

STATEMENT OF PAULA SELIS

Ms. SELIS. Thank you, Mr. Chairman.

Mr. STEARNS. Just pull the mike up close to you.

Ms. SELIS. There we go. Thank you, Mr. Chairman, members of the committee, and thank you for having me testify today. My name is Paula Selis, and I am senior counsel with the Washington State Attorney General's Office, Consumer Protection Division. Led by our attorney general, Christine Gregoire, Washington has been a pioneer in the fight against unlawful spam and was one of the first to pass a law in 1998 prohibiting false or misleading subject lines, headers and points of origin. Our law has survived a constitutional challenge that took us to the U.S. Supreme Court and has been used as a successful enforcement tool not only by our office, but by ISP's, some of whom are here today, and private individuals, consumers themselves.

But has it been enough to stop the onslaught of spam? It has not. Spam continues to be the No. 1 source of consumer complaints to our office. It continues to bring pornography, phony get-rich-quick schemes, pyramid schemes and computer viruses into our homes. One State alone cannot change the landscape. It is simply not enough of a deterrent to spammers that they might be sued in 1, 2 or even 12 States. As long as it is cheap to send spam, when even a 1 percent rate of return on millions of e-mail messages yields a profit, spammers will make money and stay in business. That is why we need a strong Federal law-to create a deterrent that reaches further than the States can go and raise the cost of doing business for spammers so it is no longer profitable to operate. We must take the profit out of spam to take the spam out of our in-boxes.

The bills currently before your committee must be viewed in light of this bottom line analysis. Do they effectively deter spammers by raising their cost of doing business? Is the cost of violating the law high enough to force compliance with it? To accomplish these goals, the bills must not only create uncapped financial penalties for violations, they must also empower as many entities as possible to take action. Not only should States, ISPs and the FTC have the right to sue spammers under every cause of action under the law, so should private consumers who must bear the brunt of in-boxes filled with junk. The bills also need to create as many substantive protections as possible and leave a clear path for States to take action when their laws are stronger. Causes of action for false subject lines and dictionary attacks where a domain can be overwhelmed by a flood of spam are essential. Mandatory identifier information as well as opt-out options are also essential. Criminal penalties, which the State of Virginia has pioneered, should be a fundamental part of the legislation, but there must be adequate civil enforcement ability to assure those substantive requirements are complied with.

A comparison of the two bills under consideration demonstrates the relative strength of one over the other. While their aims are similar, H.R. 2515 provides more substantive protection, more enforcement options and more deterrent effect. H.R. 2515 not only requires the inclusion of identifier information in a piece of spam, it creates a cause of action for States and ISPs against a spammer who fails to comply. H.R. 2214 does not. Like many strong laws, including Washington's, H.R. 2515 prohibits a very common tactic for spammers—the use of false subject lines. H.R. 2214 does not. H.R. 2515 permits a State to sue a spammer who fails to honor an opt-out request. H.R. 2214 does not.

The limitation on damages in H.R. 2214 is also problematic. The bill limits damages to $100 per violation, in contrast to the more effective deterrent level of $500 provided for in H.R. 2515. This limitation on per-violation damages in 2214 is compounded by the limitation on aggregate damages that can be obtained by a State enforcement authority. There is no reason to cap damages for violations involving hundreds of millions of spam. It is unprecedented. H.R. 2515 does not contain these limitations.

Additionally, H.R. 2214 creates burdens on enforcement that are unprecedented in consumer protection statutes. While the bill pro-

hibits a spammer from sending additional spam once a consumer has opted out of receiving it, a violation can only be demonstrated if the spammer knew or should have known of the opt-out request. This means an enforcement authority, such as the FTC, must prove the spammer's level of knowledge to prevail in court, a standard unknown under currently existing trade law. The level of knowledge required under 2214 to prove a civil violation is more akin to that of a criminal statute. In, contrast, H.R. 2515 does not create these barriers to civil enforcement.

In conclusion——

Mr. STEARNS. Do you mind just taking your speaker and shutting it off for a second?

Ms. SELIS. Okay.

Mr. STEARNS. Okay. Now try it.

Ms. SELIS. All right.

Mr. STEARNS. Yes.

Ms. SELIS. Okay. We will go from here. These differences as well as others in the two bills are surmountable and should not stand in the way of passing effective legislation. Our office will continue to work with staff to provide support and suggestions based on our own experience with our own State law.

In conclusion, we support the work of this committee in tackling the enormous and growing issue of spam. We urge you to pass a bill that is as strong as possible, that gives consumers and ISPs adequate substantive protections and creates sufficient deterrent mechanism to take the profit out of spam. Thank you.

[The prepared statement of Paula Selis follows:]

PREPARED STATEMENT OF PAULA SELIS, SENIOR COUNSEL, WASHINGTON ATTORNEY GENERAL'S OFFICE OF ATTORNEY GENERAL

My name is Paula Selis and I am Senior Counsel with the Washington State Attorney General's Office Consumer Protection Division. Led by our Attorney General, Christine Gregoire, Washington has been a pioneer in the fight against unlawful spam and was one of the first to pass a law in 1998 prohibiting false or misleading subject lines, headers and points of origin. Our law has survived a constitutional challenge that took us to the U.S. Supreme Court, and has been used as a successful enforcement tool not only by my office, but by ISP's and private individuals.

But has it been enough to stop the onslaught of spam? It has not. Spam continues to be the number one source of consumer complaints to our office. It continues to bring pornography, phony get-rich-quick schemes, pyramid scams and computer viruses into our homes.

One state cannot change the landscape. It is simply not enough of a deterrent to spammers that they might be sued in one, two, or even twelve states. As long as it's cheap to send spam, when even a 1% rate of return on millions of email messages yields a profit, spammers will make money and stay in business.

That's why we need a strong federal law—to create a deterrent that reaches further than the states can go, to raise the cost of doing business for spammers so it's no longer profitable to operate. We must take the profit out of spam to take the spam out of our in-boxes.

The bills currently before your committee must be viewed in light of this bottom line analysis—do they effectively deter spammers by raising their cost of doing business? Is the cost of violating the law high enough to force compliance with it?

To accomplish these goals, the bills must not only create uncapped financial penalties for violations—they must also empower as many entities as possible to take action. Not only should states, ISP's and the FTC have the right to sue spammers under every cause of action under the law, so should private consumers who must bear the brunt of in-boxes filled with junk.

The bills also need to create as many substantive protections as possible, and leave a clear path for states to take action when their laws are stronger. Causes of action for false subject lines and "dictionary attacks" where a domain can be over-

whelmed by a flood of spam are essential. Mandatory identifier information as well as opt-out options are also essential. Criminal penalties, which the state of Virginia has pioneered, should be a fundamental part of the legislation. But there must be adequate civil enforcement ability to assure those substantive requirements are complied with.

A comparison of two of the many bills under consideration demonstrates the relative strength of one over the other. While their aims are similar, HR 2515 provides more substantive protection, more enforcement options and more deterrent effect. HR 2515 not only requires the inclusion of identifier information in a piece of spam—it creates a cause of action for states and ISP's against a spammer who fails to comply. HR 2214 does not. Like many strong state laws, including Washington's, HR 2515 prohibits a common tactic for spammers—the use of false subject lines. HR 2214 does not. HR 2515 permits a state to sue a spammer who fails to honor an opt-out request. HR 2214 does not.

The limitation on damages in HR 2214 is also problematic. The bill limits damages to $100 per violation, in contrast to the more effective deterrent level of $500 provided for in HR 2515. This limitation on per-violation damages in HR 2214 is compounded by the limitation on aggregate damages that can be obtained by a state enforcement authority. There is no reason to cap damages for violations involving hundreds of millions of spam. HR 2515 does not contain these limitations.

Additionally, HR 2214 creates burdens on enforcement that are unprecedented in consumer protection statutes. While the bill prohibits a spammer from sending additional spam once a consumer has opted out of receiving it, a violation can only be demonstrated if the spammer knew or should have known of the opt-out request. This means an enforcement authority, such as the FTC, must prove the spammer's level of knowledge to prevail in court, a standard unknown under currently existing trade law. The level of knowledge required under HR 2214 to prove a civil violation is more akin to that of a criminal statute. In, contrast, HR 2515 does not create these barriers to civil enforcement.

These differences as well as others in the two bills are surmountable and should not stand in the way of passing effective legislation. Our office will continue to work with staff to provide support and suggestions based on our experience with our own state law.

Strong legislation is only one part of the solution. As a state attorney general's office, we believe that consumer education is also important, as is the advent of technology. If legislation is passed, it must be flexible enough to allow for new technologies that may ultimately be more effective than any law. There is no easy fix to this problem, and it will take all the tools we have to address it.

In conclusion, we support the work of this committee in tackling the enormous and growing issue of spam. We urge you to pass a bill that is as strong as possible—that gives consumers and ISP's adequate substantive protections, and creates sufficient deterrence and meaningful enforcement mechanisms to take the profit out of spam.

Mr. STEARNS. I thank the gentlelady.

Mr. Murray?

STATEMENT OF CHRISTOPHER MURRAY

Mr. MURRAY. Subcommittee Chairman Stearns and other distinguished members of the committee, I am here today to represent the print and—Consumers Union, the print and online publisher of Consumer Reports magazine. I would like to thank you for the opportunity to testify before the committee today.

As the excellent testimony of the witnesses have gone before me has indicated, spam is a source of heartburn, upset and nausea that is rising in the throats of consumers. I don't think I need to detail the enormous costs that are entailed in spam. I will note there is one study that came out last week which indicated that spam costs every business in America $874 for every employee, every year. Those businesses will end up passing all of those costs on to consumers. As Mr. Rubinstein indicated, we are in an arms war with spammers right now. They put in better filters, the spammers get smarter software to send out their spam. They get

better personnel to try and beat the spammers and the spammers end up working around the clock to beat the new personnel. So it doesn't seem that failing some solid legislation coming out of Congress this year that we are going to do anything abou this for consumers.

I will note one new kind of spam I am hearing about is wireless phone spam, and a friend of mine even has some patents for location-based wireless spam which would allow a spammer to say, "Well, you are a half mile from a Starbucks right now. I will give you 50 cents off of your next latte if you come by in the next 30 minutes." That is kind of a nightmarish consumer scenario for me and I would like to see this bill address wireless spam.

I agree wholeheartedly with the drafters of both bills that the No. 1 problem and step No. 1 for cleaning up spam is the criminal element in spam, the fraudulent spam we are seeing. I have heard reports that two-thirds of all spam have some kind of fraudulent content in them. So that is where we need to start. And I think labeling pornography is also a big step in the right direction, although I would like to see in whatever legislation comes out of committee I would like to see the Wilson-Green approach which ensures that consumers don't have to view the pornography to opt out.

Which brings me to my primary area of concern with H.R. 2214 and H.R. 2515, which is that both bills have as their core solution opt-out for consumers. Imagine that you put a do not solicit sign in the front door of your home and the way that that "do not solicit" sign worked was that every solicitor who came by your front door got one shot at you, and you could opt-out with each company that comes by your door and potentially each branch of the company that comes by your door, except I think we can all see you would spend a whole lot of time opting-out. And there is a bit of a consumer paradox right now. Consumer Reports in the latest August issue we recommend that when consumers get spam they do nothing. You don't view it, you don't buy anything from spam, and you don't even allow—you disable the preview pane of your browser, of your e-mail program so that you can't even see the spam because as soon as you view the spam, the spammer will know that you have received it and he will know that that is a live address.

So there is this paradox consumers find themselves in which is we are telling them not to opt out but if opt out is the core solution that we provide, I don't know that we are going to give them a different recommendation because there is still going to be an immense volume of spam that is coming from overseas, and there is no way for the consumer to tell the difference between an e-mail from the Netherlands or an e-mail that is coming from a domestic source.

So I would like the committee to perhaps examine to see if there is some kind of opt out plus. I know that opt-in probably is not politically realistic but is there some way we could provide a less burdensome opt-out for consumers? The Federal "do-not-call" list, which the FTC with the full support of the administration just put in place 2 weeks ago, has received an overwhelming consumer response. It has been an enormous consumer success, and something that is closer to that model might be an effective mechanism for

consumers. Now, I understand that with a "do-not-spam" registry there are some security concerns, but I wonder again if there is some sort of opt-out plus that we could look at which is perhaps some way consumers can know if it is a trustworthy opt out. I would like to work with the committee on that.

I will note in passing, Senator Hatch mentioned a few weeks ago that his committee was willing to look at opt out as—excuse me, to look at opt-in and he also noted that we would be wise to look at successful models that have come before us. The Telephone Consumer Protection Act, the junk fax law, has been a great consumer success, and the two key elements of that were that it was an opt-in regime, and it had a private right of action for consumers. I think the committee would be wise to consider those approaches.

I am pleased to agree, again wholeheartedly, with the ends of everyone that is at the table today, and I am sure that we can reconcile our differences as to the means. Thank you for the opportunity to testify.

[The prepared statement of Christopher Murray follows:]

PREPARED STATEMENT OF CHRIS MURRAY, LEGISLATIVE COUNSEL, CONSUMERS UNION

Subcommittee Chairmen Stearns and Upton, Ranking Members Schakowsky and Markey and other distinguished members of the Committee, thank you for the opportunity today to represent Consumers Union,[1] the print and online publisher of Consumer Reports, in your exploration of H.R. 2214, the "RID-SPAM Act" (sponsored by Reps. Burr, Sensenbrenner, and Tauzin).

It is almost unnecessary for me to detail what the problem with "spam"[2] is, because every time we open up our email inboxes we are confronted with exactly how bad things have gotten. When I arrive at work every morning, I can be confident that I will be greeted with at least a dozen messages advertising everything from life insurance and credit card offers to Viagra alternatives and pornography.

The ingenuity of spammers appears to be bottomless.[3] They find our addresses in novel ways. They have figured out myriad methods to avoid being filtered by Internet Service Providers (ISPs) and consumers. They have discovered how to commandeer our computers to send spam for them, and they are even finding new devices to spam us on. For example, text messaging on mobile phones, an increasingly popular application for consumers, is also becoming a haven for spam. While filtering technologies are becoming increasingly effective, unfortunately their efficacy is not increasing as fast as the volume of spam is growing.

Spam costs consumers and businesses money.

Some estimate that roughly 40% of all email is spam[4] and experts say that by the end of this year more than half of all email traffic will be spam. Consumers pay for all that spam, because when ISPs' costs go up—because ISPs have to buy more servers and pay personnel to figure out how to filter that spam—consumers' monthly ISP subscription fees go up.

---

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

[2] See Jonathan Krim, "*Protecting Its Proprietary Pork*." *Washington Post,* July 1, 2003 (E01). "Early Internet users coined the term spam to describe junk e-mail after a skit by the comedy group Monty Python. In the routine, a group of patrons at a restaurant chant the word "spam" in louder and louder volume, drowning out other conversation."

[3] See attached article, "E-Mail Spam: How to Stop It From Stalking You." *Consumer Reports,* August 2003.

[4] See Jonathan Krim, "Spam's Cost to Business Escalates." *Washington Post,* March 13, 2003 (A01).

One company estimates that spam will cost business $10 billion dollars this year alone (due to lost productivity, bandwidth costs, and money spent on filtering tools).[5] A study released last week estimates that spam costs businesses $874 per employee every year, because employees spend an average of 6.5 minutes every day dealing with it.[6]

America Online, the largest ISP, is currently blocking up to **2.4 billion** spam messages every day.[7] The costs of the bandwidth and servers required to move that volume of spam are astronomical—when we add the costs of sophisticated filtering systems and personnel to battle the continually escalating spam arms race, the costs of spam to ISPs (and ultimately to consumers) is truly staggering.

Recently the Washington Post reported that mainstream e-commerce companies are selling consumers email addresses to spammers.[8] For example, when consumers purchased popular "Hooked On Phonics" products, their addresses were being sold in complete violation of their privacy policy. That is, the company told consumers that they would not sell their personal information and then turned around and did precisely the opposite. "Hooked on Phonics" corporate parent subsequently updated their privacy policy and said that they meant to update it earlier; they claimed they had done nothing wrong, they were simply slow to update their privacy policy.

Even worse, one company who was contracting with a 3rd party "shopping cart" provider (the mechanism used by consumers to complete an electronic commerce transaction) had a privacy policy which would have prevented consumers' email addresses from being shared with anyone. However, consumers might not have noticed that the shopping cart company behind the scenes of the electronic transaction—"Cart Manager"—had a completely different privacy policy and that by purchasing a product online, they were unwittingly making themselves vulnerable (there was no link to the shopping cart company's privacy policy in the process of check out).[9]

A relatively new practice, known as "email appending," raises enormous privacy concerns. Email appending is the practice of harvesting a consumer's email address from a Web site or other means and combining that consumer's email address with their mailing address, telephone number, and other personally identifiable information.

Mainstream companies such as Sears are using email appending to merge customers email addresses with their mailing addresses and their automotive repair histories. A marketing magazine recently told its readers how to "email append" their mailing lists:

> Send an Excel spreadsheet of your customers' names, addresses and phone numbers to an e-mail appending company, and the appending company will send back e-mail addresses that belong to those customers.
>
> What the appending company doesn't mention is that often it is missing a good deal of the information that you possess, and it may decide to append your data to its files just as it appends its e-mail addresses to yours. That means you are paying the company to incorporate your information into its e-mail database.
>
> For example, the automotive department at Sears provides its customers' names, addresses, phone numbers, and car models, makes and repair histories to e-mail appending firms when it requests customers' e-mail addresses. Sure, the company gets the e-mail addresses, but at the same time it contributes to privacy erosion—all so it can send an e-mail about its lube, oil and filter change special.[10]

A large percentage of spam is also fraudulent and/or misleading, making it a serious consumer problem as well as difficult to prosecute. The Federal Trade Commission (FTC) recently issued a report[11] regarding false claims in spam, which found that 96% of spam had false information in either the message text or in the "From" and "Subject" lines.

Clearly, spam is ripe for legislative action. We agree with the ISPs and others that strong criminal enforcement and an ISP right of action are essential ingredients to successfully reducing spam. But thus far the bills proposed, including H.R. 2214, have an "opt-out" of spam as part of their core solution. In other words, an

---

[5] See www.ferris.com/rep/200301/SM.html.

[6] "Spam: The Silent ROI Killer" by Nucleus Research. More information at: www.pcworld.com/news/article/0,aid,111433,00.asp.

[7] See testimony of Ted Leonsis (Vice Chairman and President, Advanced Products Group, America Online) before the Senate Commerce Committee, May 21, 2003.

[8] Jonathan Krim, "Web Firms Choose Profit Over Privacy." *Washington Post,* July 1, 2001 (A01).

[9] Id.

[10] See Mike Banks Valentine, "E-Mail Appending Erodes Privacy." CRM Buyer Magazine, May 23, 2002. www.crmbuyer.com/perl/story/17914.html

[11] www.ftc.gov/reports/spam/030429spamreport.pdf

ISP must first pass on the spam to consumers, consumers must then read the spam, and then they can exercise their right to stop receiving messages from that particular sender (perhaps at their peril as described below). We believe H.R. 2214 needs to be improved because it lacks an "opt-in" provision and private right of action for consumers at the same time that it excludes class action suits. This puts too much burden on consumers to block spam and makes it too difficult to hold spammers legally accountable for their inappropriate interference with consumers' email.

Imagine that you put a "do not solicit" sign at the front door of your home, and every company in the world could only ring your doorbell once, at which point you would have the option to tell that salesperson that you did not want to be contacted anymore. Of course, in addition to telling that salesperson you didn't want to be solicited, you would have to do the same for solicitors that work for a different branch of the same company. You would need to keep track of each company you told not to solicit you, and if a company violated your request, you could petition the Federal Trade Commission to take up your case.

Of course, this is an absurd burden to place on people. We all know that "do not solicit" means exactly that. Consumers can say no to advertising at their front door, period. The Federal Trade Commission's recent enactment of a robust "do not call" list means that now consumers have a tool to say no advertising at the dinner table. It is now incumbent on Congress to provide consumers with a tool to say no to advertising on our computers.

When the Federal Trade Commission recently took a close look at spam and what could be done to reduce it, many, if not most of the participants in that workshop agreed that opt-in was the best way to eliminate spam. It would be unwise for Congress to proceed down the opt-out path, which was clearly disfavored by experts.

Senate Judiciary Committee Chairman Hatch suggested several weeks ago that he would be willing to consider drafting legislation that entails an opt-in approach. He noted that one of the primary weaknesses of opt-out is that it leaves the burden on the consumer to eliminate spam. "People who receive dozens, even hundreds, of unwanted emails each day would have little time or energy for anything other than opting-out from unwanted spam." [12]

Senator Hatch continued on to say that,

> "[a] third way of attacking spam—and one that was favored by many panelists and audience members at the FTC forum—is to establish an opt-in system, whereby bulk commercial email may only be sent to individuals and businesses who have invited or consented to it. This approach has strong precedent in the Telephone Consumer Protection Act of 1991 (TCPA), which Congress passed to eliminate similar cost-shifting, interference, and privacy problems associated with unsolicited commercial faxes. The TCPA's ban on faxes containing unsolicited advertisements has withstood First Amendment challenges in the courts, and was adopted by the European Union in July 2002." [13]

As Senator Hatch points out, the Telephone Consumer Protection Act (also known as the "Junk Fax" law) could serve as a good model for dealing with spam. That law successfully helped eliminate junk faxing by 1) establishing an opt-in regime and 2) preserving a private right of action against violators, especially by allowing for the possibility of class action enforcement. We believe that the threat of class action enforcement combined with an opt-in approach is the best way to reduce spam for consumers.

In addition, Congress should not allow ISPs to be the primary entities driving a legislative solution. ISPs are an integral part of any solution, as their technical expertise and participation in enforcement is essential, but they have mixed incentives with regard to spam.

ISPs have clear incentives to reduce some amount of spam, because it costs them an enormous amount of money—except where the ISP is also a marketer. In the case of AOL and Microsoft, the two largest ISPs, those companies have clear incentives to get rid of other people's spam, but not such clear incentives to have limitations on their own spam. In fact, it may be that the best way for AOL and Microsoft to maximize their marketing revenues is to get rid of everyone's spam but their own, so that they can charge would-be spammers for preferred placement of spam. As the Washington Post recently reported, California state legislators were recently pressured by these companies as they tried to beef up spam regulations:

> One [California] state senator, who represents several Los Angeles suburbs, accused Microsoft of eleventh-hour arm-twisting to exempt Internet service pro-

[12] Senator Orrin Hatch and Senator Patrick Leahy Press Release, "*Hatch, Leahy Target Most Egregious Computer Spammers*." Jun. 18, 2003.

[13] Id.

viders from responsibility for being the conduits of spam. Firms such as Microsoft, America Online and Yahoo Inc. market to their own members, and large portions of overall e-mail traffic traverse their systems.

"Microsoft is talking out of both sides of its mouth," said state Sen. Debra Bowen (D), who points to statements by Microsoft Chairman Bill Gates about how much the company is fighting to eliminate junk e-mail. But "their focus has been on getting immunity for themselves and preserving their ability to strike deals to send spam," she said.[14]

Ronald Scelson, also known as the "Cajun Spammer," testified before the Senate Commerce Committee[15] that some ISPs are signing "pink contracts' which allow spammers to send emails to ISPs' subscribers, charging the spammers more than they charge other commercial clients.

If these allegations are true, then it is unwise for Congress to give ISPs consumers' proxy on spam by allowing ISPs to have a right of action against spammers at the exclusion of individual suits and class actions. Giving ISPs a right of action will certainly help those ISPs to maximize the revenues they receive from spammers by providing them with a very large stick for spammers that do not pay, but it does not appear to be the best way to reduce spam.

Until Congress enacts meaningful legislation to fix the spam problem, Consumer Reports recommends that consumers deal with spam by doing nothing. This means do not respond to spam, do not view spam, and most especially, do not opt-out of spam because this will tell spammers that your email address is a functioning one.

This recommendation—that consumers do nothing with spam, and especially do not opt-out—is at obvious odds with bills that provide for opt-out as their way to clean up spam. That is because when consumers opt-out they are verifying for a spammer that their email addresses are current. Under an opt-out law, consumers would ostensibly have a remedy with spammers within the United States (i.e. spammers using opt-out for illegitimate purposes such as verifying that an email address is current could be prosecuted), but the opt-out law would still not apply for any spam originating outside the U.S.—spammers in other countries or offshore could not be prosecuted. Furthermore, it would be extremely difficult for consumers to tell whether email is originating from the U.S. or elsewhere.

In other words, once an opt-out spam bill were enacted into law, because of the continued possibility of cross-border fraud, we would still recommend to consumers that they should not exercise the opt-out—leaving consumers no better off than they are today.

In our August issue of Consumer Reports, we recommend the following 8 ways to block spam:

1. Don't buy anything promoted in spam. Even if the offer isn't a scam, you are helping to finance spam.
2. If your email address has a "preview pane," disable it to prevent the spam from reporting to its sender that you've received it.
3. Use one email address for family and friends, another for everyone else. Or pick up a free one from Hotmail, Yahoo!, or a disposable forwarding-address service like www.SpamMotel.com. When an address attracts too much spam, abandon it for a new one.
4. Use a provider that filters email, such as AOL, Earthlink, or MSN. If you get lots of spam, your ISP may not be filtering effectively. Find out its filtering features and compare them with competitors'.
5. Report spam to your ISP. To help the FTC control spam, forward it to uce@ftc.gov. ("uce" stands for unsolicited commercial email).
6. If you receive spam that promotes a brand, complain to the company behind the brand by postal mail, which makes more of a statement than email.
7. If your email program offers "rules" or "filters," use one to spot messages whose header contains one of more of these terms: html, text/html, multipart/alternative, or multipart/mixed. This can catch most spam, but may also catch most of the legitimate emails that are formatted to look like a Web page.
8. Install a firewall if you have broadband so a spammer can't plant software on your computer to turn it into a spamming machine. An unsecured computer can be especially attractive to spammers.

As mentioned earlier, as a legislative remedy, an opt-in regime (with a private right of action) appears to be the best choice. We recommend that consumers not opt-out of spam because this will simply confirm for the spammer that their email address is a live one. Opting out means getting more spam.

---

[14] Jonathan Krim, "Internet Providers Battling to Shape Legislation: Microsoft, Others, Said to Want Immunity." *Washington Post,* July 5, 2003 (D10).

[15] Testimony of Ronald Scelson before the Senate Commerce Committee, May 21, 2003.

If we put ourselves in the shoes of a consumer trying to opt-out from spam several years from now, imagine trying to tell the difference between spam that is from a legitimate marketer, spam that originated from an overseas or offshore server, and spam that is simply a ripoff. There is no way I can think of under an opt-out regime to differentiate between these different types of spam. Opt-out may turn out to be a cop out.

It may be that there is a possibility for a modified version of opt-out, such as opt-out that allows for an entire domain to opt-out (e.g. "aol.com" could opt-out for all its users, so that individual users, such as "jane—doe@aol.com" do not have to give their names to spammers). This is one potential implementation of the "national do not spam" registry proposed by Senator Schumer. I have some misgivings about a "national do not spam" registry because of the obvious security risks posed by such a list, but I wonder if allowing entire domains to opt-out obviates some of those potential risks.

In addition, by including preemption of state laws and class actions, I believe HR 2214 will fail to stem the rising tide of spam. Congress should enact federal legislation that offers basic protection for consumers, and states should have a right to increase such protections based on unique local needs, just as the FTC did with the Federal "Do Not Call" list.

Any solution in the end will need to involve a variety of methods and actors, including a legislative remedy (opt-in with both private and ISP rights of action in addition to criminal enforcement), action from industry to improve filtering technologies as well as a way to attack the problem across international borders. It will be critical that Congress address the immense volume of fraud in spam, but Congress should also consider measures that will address mainstream companies' use of spam. While fraud is a huge problem, consumers' annoyance with spam does not end with rogue spammers. Just as the FTC's national "do not call" list allowed consumers to say no to advertising at the dinner table, consumers should have the ability to say no to all spam, even when that spam comes from companies that are not engaged in fraud.

Mr. STEARNS. I thank you, Mr. Murray. I think we are finished with the opening statements, so I will open up with some questions. Mr. Beales, I will start with you. You have heard the opening statements from the members and you have also heard from our panel. Of the two bills that we have, I guess the question would be do you favor one bill over the other?

Mr. BEALES. We haven't taken a position on a particular piece of legislation. We have tried to talk about the kinds of provisions that we think are useful, and I think there are attractive features of each bill.

Mr. STEARNS. That is what I would say based on what you—I thought you would say that. So you feel that the two bills have aspects about them that are appropriate or suitable but neither one of the bills as they stand now alone, in your opinion, would be suitable?

Mr. BEALES. Well, I think that is right. I think that is right as well. I mean I think—we think legislation should leave us some flexibility to address problems as they emerge, and I think a great example is dictionary attacks. A year ago we would have said, and I think the bill said a year ago, harvesting is it, that is what we need to prohibit. They didn't say a word about dictionary attacks. This year, dictionary attacks are the way spammers are generating their messages. Without some flexibility to address that kind of change in practice through rulemaking, we are going to be back in the soup in fairly short order.

Mr. STEARNS. I am going to go to Microsoft on this, but let me ask you, Mr. Beales, what is your view on sort of a safe harbor approach to label e-mail as a means of fighting spam?

Mr. BEALES. Well, we are skeptical about labeling e-mail as a solution, because we think what ends up happening, and it certainly

showed up in our false claims in spam study, is you get compliance and ADV label by legitimate marketers, but you don't get compliance by the people who are the problem. What we found in our study was—and, you know, there are 10 States that have an ADV requirement. One of them is California. I don't think spammers can plausibly say, "Well, we didn't know anybody on our list lived in California." What we found was only 2 percent of the spam in our sample of 1,000 had the label.

Mr. STEARNS. Okay. Mr. Rubinstein, Microsoft believes that, "The widespread adoption of e-mail best practices along with a method to associate e-mail communication from business that adopt such best practices will ameliorate many problems currently associated with spam." I think that is a quote you used. That suggests that you perhaps—you and Mr. Beales might not agree, and I thought you might just comment on it.

Mr. RUBINSTEIN. Sure.

Mr. STEARNS. Just pull the mike up if you would.

Mr. RUBINSTEIN. Sorry. I think there are three things that recommend a safe harbor approach. One is that it helps reinforce the distinction between legitimate senders and spammers. The second is that it could improve filtering technology by providing additional inputs to filters, namely that the mail is from a company that adheres to best practices. That allows filters to act more aggressively against mail lacking that indication and to do so without being more inaccurate in creating false positives or false negatives. And then, finally, I think, as Mr. Murray pointed out, it could help restore confidence, consumer confidence in opt outs.

In response to Mr. Beales, I think in fact we may not be disagreeing as much as it may seem, because, again, we have not proposed ADV labeling as a stand-alone solution in any Federal legislation. Rather, we see it as an incentive for companies to join safe harbor programs, but we would be happy to consider other possible incentives. Some that have already been under discussion include a presumption of compliance for companies that participate in best practice programs, namely the compliance with the 101(a) type requirement. This would not affect fraud.

Mr. STEARNS. So what would be the Federal Government's role dealing with e-mail?

Mr. RUBINSTEIN. Well, the Federal Government's role would primarily be to jump start this process. Today, there are a lot of companies doing the right thing, but there are no widely adopted best practices. If there was a strong incentive for companies to sign up for best practices, then it would become quickly adopted across the board. And until it is pervasive, until a large number of companies take advantage of this approach, it won't provide the benefits that we see to it.

Mr. STEARNS. One of the differences between the bills is in the ability to sue, and, Mr. Murray, we went back and looked at your testimony before the Judiciary Committee yesterday on spam. In response to a question from Chairman Coble, you indicated that plaintiffs could sue senders of commercial e-mail, "They would go first after the deep pockets." Given that most spammers are judgment-proof, aren't civil and criminal penalties against spammers a more effective deterrent to spam?

Mr. MURRAY. I think that spam is such an enormous problem that we need to recruit the help of all sides of this, and I do believe that consumers are an absolutely integral piece of that, because press accounts have indicated that some ISPs, not all ISPs, are signing contracts with spammers for preferred placement of spam.

Mr. STEARNS. But you see the problem with your statement saying they will go after the deep pockets. That might be somebody, somewhere out there and that just creates a huge amount of litigation, jury trials, when we are trying to deter this.

Mr. MURRAY. Yes, sir, Mr. Chairman, but first there would have to be bad behavior to instigate that litigation. And the question that Chairman Coble asked me yesterday was about who would people go after first, and I think we do know that people would likely go after the money. But assuming that the people with the money have done some bad behavior, then I don't think that that is necessarily out of line.

Mr. STEARNS. My time has expired. Mr. Boucher?

Mr. BOUCHER. Thank you, Mr. Chairman, and I want to thank each of the witnesses for your very helpful testimony here today. Let me just pursue a couple of questions that are related to differences that appear in the two bills that are before us and get the benefit of the views of anyone who wants to respond with respect to these specific provisions.

First of all, one of the bills provides that an opt-out once it is taken is effective with regard to the sender of spam but not with regard to affiliates of that sender. So a bank that has 100 affiliates, as many banks do, having separately incorporated their various branches or divisions, could be subject to a single opt-out for the sender alone but not for all of those many affiliates. A separate opt-out under that bill would be required for each. Is there any justification for a provision such as that or do you see that as a loophole that could render the opt-out right less simple and less effective than it needs to be? Who would care to answer? Ms. Selis?

Ms. SELIS. I will take a stab at that from a consumer's perspective. Most consumers don't differentiate between one affiliate and the other. They get a piece of spam in their e-mail and they just don't want it. They don't want that piece of spam, they don't want a piece of spam from an affiliate. Oftentimes, they don't want a piece of spam from anyone. And to create an extra hurdle for them by requiring them to opt-out as to particular affiliates of a business will require them to opt-out repeatedly and put another burden on them. It gives them less control over their e-mail box, which is not what I think this committee wants to do.

Mr. BOUCHER. All right. Thank you. Mr. Murray?

Mr. MURRAY. If I could just add briefly. I understand the intent behind that is to enable consumer choice. If perhaps consumers have some more distinguished preferences that they would like to be able to receive information from one company and not from another, I don't think that is necessarily a bad thing as long as it is accompanied by the possibility of a global opt-out, as long as more detailed requests for opt-out have alongside one opt-out that will cover everything that is very transparent and very obvious to the consumer, I don't know that there is great harm in that.

Mr. BOUCHER. But you are saying that at a minimum there ought to be a single opt-out opportunity——

Mr. MURRAY. Absolutely.

Mr. BOUCHER. [continuing] with respect to the sender and all affiliates.

Mr. MURRAY. Absolutely.

Mr. BOUCHER. Others care to comment on that? Mr. Betty?

Mr. BETTY. I don't know that it is really the most relevant issue, because the people that we are trying to get don't really care what regulations you put into place for opt-in or opt-out. As indicated by Mr. Beales, most of the responses that you send when you try to find out where the stuff is coming from is it bounces, it falses. The true marketers are going to try to comply with what consumers want anyway. So I don't know a universal opt-out or a single opt-out is really relevant at all.

Mr. BOUCHER. Well, some people simply aren't going to obey the rules no matter what. I mean that is your point.

Mr. BETTY. That is right.

Mr. BOUCHER. But we have to try to write this law in such a way that we target those who are going to respect it and then we will leave it to law enforcement to target those who don't. But thank you. Let me move on to another question.

The definition of e-mail strikes me as being particularly important. One of the bills would define spam as commercial e-mail, the primary purpose of which is commercial, but e-mail that is drafted in such a way that is partly commercial and partly informative, perhaps, or in some other way arguably non-commercial would fall outside the net. And I can imagine a lot of creative ways that spammers could redraft their messages so that arguably the primary purpose in the minds of some might not be commercial. Is that a problem or should we simply say commercial e-mail generally would be defined as spam and be subject to the opt-out? Views on that. Mr. Beales?

Mr. BEALES. Well, the—I am sorry, I lost the thread of your question.

Mr. BOUCHER. Well, the question simply is this: One bill says that spam is anything that has a primary commercial purpose. The other bill simply says that it is unsolicited commercial e-mail. So the question is, is it unduly limiting to have this qualification that the primary purpose of the message has to be commercial?

Mr. BEALES. And I think we would prefer that it not be a primary purpose. An important purpose, a principal purpose, language like that might make sense. I think there is an issue there because there are a lot of—I mean you have probably been e-mailed newspaper articles, for example, that have advertising along with them. A purpose of that communication is to sell, a purpose, but I don't think most people would call that kind of advertising that goes with that newspaper article spam in quite the same way. And I think the definition needs to distinguish those cases but we think the primary purpose kind of language is problematic.

Mr. BOUCHER. Okay. Yes, Mr. Rubinstein?

Mr. RUBINSTEIN. We share the committee's concerns with loopholes, as expressed earlier in the opening statements, but I would like to point out one—just make one other observation.

Mr. BOUCHER. Which concern do you share because several opinions have been expressed.

Mr. RUBINSTEIN. Well, the concern that the way this is defined may create loopholes, and I think that would be a mistake. But there is another issue that I would like to address that——

Mr. BOUCHER. You are saying that saying primary purpose is unnecessary in this case and could be problematic?

Mr. RUBINSTEIN. No. I am saying that we also need to look at the combination of that definition with how exceptions are treated, and that is another difference in the bill. Document 2515 tends to treat exceptions in terms of enumerating specific examples for which opt-out would not be required, such as product updates, security updates, warranty information and so on. Our only concern around this is that there are other possible examples that may not be included in that list. One obvious one would be updates to a privacy statement that make a material change in that privacy statement. That is not on the list. There may be other things that are not on the list that represent important communications between a company and its customers. So we are just a little bit concerned about that approach that only enumerates specific exceptions rather than providing broader——

Mr. BOUCHER. Mr. Rubinstein, thank you very much. My time has expired. Thank you, Mr. Chairman.

Mr. STEARNS. Gentleman's time has expired. Thank you. The chairman of the Telecommunications and the Internet Subcommittee, Mr. Upton.

Mr. UPTON. Well, thank you, Mr. Chairman, and I will try to make sure I don't repeat questions that might have been asked. If I do, please bear with me and I will get the answer later on. Mr. Beales, I would be interested to know what the FTC's stand is on a "do-not-spam" list. As we saw, I thought it was important legislation that we passed earlier this year, the "do-not-call" list, which is now being implemented and your operators are taking lots of calls all the time, including from my house, and it seems like it was a very good idea, welcomed by the American public for sure, and I would be interested to know what your thoughts are if we develop something like a "do-not-spam" list along those same lines. What is it workability?

Mr. BEALES. Well, we think it is a very intriguing idea, but, unfortunately, there are three differences from phones that make it not at all clear that we can do it at this point. One is it is easy to identify valid phone numbers and so a list of valid phone numbers doesn't have much value. A list of valid e-mail addresses is a whole different story, and that is what a do-not-spam list would be. That problem is compounded by, two, that we can't trace the spammer, we can't tell where it is coming from, and we need to give that list to spammers and somehow only give it to good guys who will use it to purge their lists and not as a list, and that is hard to imagine how we could enforce that.

The third problem is the size of the data base. People change their e-mail addresses all the time, and what we would have over time is a larger and larger data base of more and more dead e-mail addresses. That would help with the first problem but it really wouldn't help us to be able to process it at all. So we think it is

an intriguing idea but at this point we don't know how we could do it.

Mr. UPTON. I would also note as you make that point that whereas most homes have one hard line, maybe two if they have got a computer if they don't have cable for high speed, or perhaps a cell phone or two, but most—I look at my own family, we have got a good number of e-mails. My son has got two, my daughter has got two, my wife and I have one, so you have got a lot more e-mails than you do number of households that are out there. Any other comments from the rest of the panel, any concurrence? Mr. Murray?

Mr. MURRAY. Chairman Upton, I wonder if there is—there was an intriguing idea raised by a journalist from the Washington Post, which was a "do-not-spam" list where domains could opt-out, where, for instance, AOL.com could choose that its members not receive spam or MSN.com or Earthlink, and I wonder if that is some sort of a hybrid that we could work with.

Mr. UPTON. Mr. Rubinstein, do you have a comment?

Mr. RUBINSTEIN. I would concur with Mr. Beales and also point out in response to an earlier comment from Congresswoman McCarthy that in opposing the Missouri State bill, we did so explicitly because it provided for a "do-not-spam" list and we have opposed that, both in State law and Federal law. As to Mr. Murray's suggestion, I am not really certain, and I would ask Chuck Curran to comment too, I am not really certain how a large ISP would handle a domain-based opt-out given there would be often be disagreements among its own subscribers as to what domain to opt-out from, and I don't know how we would resolve those disagreements.

Mr. UPTON. Let me get to another question before my time expires. I confess that I am an AOL subscriber, and I also confess, Mr. Betty, that a number of my family are Earthlink subscribers as well. As I sat down at my computer last night looking over the e-mail from over the 4th, Mr. Curran, we have got as AOL, as a subscriber, I have got the little icon that allows me to say no more and it is spam, block it forever. Tell me how that system works. How do I know—I mean there was a fear for a long time that if you did that, the folks that are sending you this junk know that is a live person and they may in fact try to come back at you. How does your system work on your end when the user says, "I don't want to get that stuff anymore," and how long does it take?

Mr. CURRAN. If you are referring to the report spam feature——

Mr. UPTON. Yes.

Mr. CURRAN. [continuing] what we use that as is a reporting tool for two purposes, one of which is to, in effect, get real-time feedback about what our members are reporting as spam to enhance our ability to do technological filtering of that same type of spam.

Second, that reported spam is transferred to a data base which can be mined for information about the largest scale spammers. In effect, it is a way to build a data analysis to support enforcement and preventative technology. So it is not—the spam is not being—your report of spam is not being forwarded on to that——

Mr. UPTON. Well, let me just—as an example, last week I refinanced my house. I don't need to do that again for a while, I hope. There must have been 10 or 12 refinancing bids unsolicited that

came in on my e-mail that I deleted last night, and I checked them as spam. Is there a likelihood then those are going to come back from those same——

Mr. CURRAN. Regrettably, mortgage refinance spam is a mainstay of today's spam, so there may be an issue of pure coincidence. I too have engaged in a mortgage refinance, but I am also getting random offers of mortgage refinances, so there may not necessarily be——

Mr. UPTON. But are the same folks going to come back at you a second or third time even if you say this is spam and I don't want it, Mr. Betty?

Mr. CURRAN. In many——

Mr. UPTON. Yes. So are you saying it was a worthless exercise for me rather than simply hit the delete button and go through the process?

Mr. BETTY. I mean I can't speak for what AOL does but we get a lot of feedback as well, and after you have identified where the spam is coming from after you have gotten the first several it doesn't really help to get the next 200,000. But if these people are trying to defraud consumers, the fact that you are reporting it back to us, we really do know, we are spending lots of money trying to solve this problem for the consumers. What we suggested is they just delete it, and we continue to work on tools to allow you not to get it the first time, and we have now taken the step to integrate it with your mailbox so you won't get it if you don't want it.

Mr. UPTON. I know my time is expired.

Mr. STEARNS. Gentleman's time has expired. Gentleman from Texas?

Mr. GREEN. Thank you, Mr. Chairman, and let me first start out, one, to thank, like my colleagues, all our panel for, listening to ours, and I said it earlier, to some members of our panel, that we are still working on putting together a bill and sometimes us listening to each other in our opening statements let us know where we are so we can see where we are going. But your testimony today has been really helpful.

In an earlier hearing, I ran out of time and I am sure I will today, but we submitted questions to the FTC and I would like to read one into the record. It compares one spam bill, H.R. 2214 that imposes a knowledge standard the Commission must prove to successfully bring a civil action for violations of three provisions of the bill. And we asked the FTC how does this compare with common FTC enforcement authority? Is it safe to say that the FTC would be less likely to bring in action in situations where it would be required to prove a knowledge standard. Let me read into the record, Mr. Chairman, the response from the Federal Trade Commission to that.

Mr. STEARNS. Do you want to make it part of the record by unanimous consent?

Mr. GREEN. I would like to make it part of the record.

Mr. STEARNS. By unanimous consent.

Mr. GREEN. "In conclusion, the knowledge standards contained in H.R. 2214 exceeds those required to obtain a district court injunction or administrative cease and desist order under Section 5 of the FTC Act. Further, the knowledge standards contained in H.R. 2214

are unnecessary in connection with the civil penalty action in light of the knowledge standard imposed for civil penalty actions under the FTC Act, Section 18, rule violations. Moreover, the knowledge standards set forth in 2214 are expressed differently from those in the FTC Act potentially giving rise to the litigation issue about the differences in the standard. Given the harmful nature of the conduct prescribed by this proposed legislation, the FTC should be able to enjoin future violations readily and to impose civil penalties where appropriate without duplicate burden of meeting two arguably different knowledge standards. Therefore, we anticipate that retention of the knowledge standards in H.R. 2214 will reduce the enforceability of the provisions." This is in response to a question of the FTC.

Mr. Beales, in your response to Chairman Stearns' question, you stressed the flexibility of the FTC. Does one bill provide better flexibility to the FTC, the Burr bill, 2214 or the Wilson-Green bill? which provides better flexibility in your opinion?

Mr. BEALES. Well, there is somewhat more flexibility in the Wilson-Green bill, but it is still quite limited in terms of the rulemaking authority that we have. I mean——

Mr. GREEN. So you would prefer—I am going to run out of time—the Wilson-Green bill provides more flexibility but not near as much as the FTC would like. Is that correct?

Mr. BEALES. That is correct.

Mr. GREEN. Okay. Given that the Wilson-Green bill has no knowledge standards that address the dictionary attacks, can you say that the FTC prefers, in your opinion, the Wilson-Green bill or that we are closer to what you would prefer?

Mr. BEALES. There a number of things in that bill that we think are improvements over what is in 2214, but we haven't taken a position at all on which——

Mr. GREEN. I understand, and we understand also Federal agencies shouldn't take positions, but, again, it is in your opinion.

Let me ask some questions of our ISPs, both AOL, Earthlink and Microsoft. Both 2214 and 2515 contain several civil provisions. It is important for ISPs to be able to enforce each section, and please if you could do it as brief as possible because, again, we have just a brief time to ask questions. Mr. Chairman, are we going to have a second round of questions?

Mr. STEARNS. I don't know. I just——

Mr. GREEN. I know it is late and our witnesses have been here a good while, so——

Mr. STEARNS. And we probably have some votes coming. I think—you know, I have tried to be liberal on the time, just some people going over 1 or 2 minutes, and some who did not have an opening statement so they will have 8 minutes. And the panel has also been here very patiently.

Mr. GREEN. Well, then I would like to ask if we could submit questions like I have done before with the Federal Trade Commission.

Mr. STEARNS. Yes, absolutely.

Mr. GREEN. I will put it in the record today and in future hearings we will put those into the record. But mainly I guess to summarize all the questions for the ISPs, the Burr bill does not permit

ISPs to enforce the inclusion section of the bill. Would it be helpful to ISPs to have that specific inclusion so you can enforce those inclusion sections? Earthlink? Microsoft?

Mr. CURRAN. Yes, it would.

Mr. GREEN. Okay. And that, generally, is the opinion of all three that are on the panel? Okay. Mr. Chairman, I will yield back my—well, I don't have any time left. And, again, I will submit questions to our panel.

Mr. STEARNS. All right.

The gentleman from Arizona is recognized.

Mr. SHADEGG. Thank you, Mr. Chairman. I am going to follow the model that Mr. Boucher set and put this question to the panel. Anybody who wants to answer, I would like to do so. I do have restraints on time. I also want to follow up on a question that he asked. The two bills have different definitions, he called them definitions of e-mail, I would call them definitions of the application of the law. In either case, in one case it says they must have a partial purpose which is commercial, in the other case it says if they have any commercial purpose at all, then they are covered by the span of the law. It seems to me, my own bias, that you have a broader definition, if there is any commercial purpose in the e-mail, it ought to be covered by the law, and then you write safe harbor or opt-out language that would protect it. But I am interested in your professional opinion on that issue of the definition within the two different bills. Yes, sir?

Mr. BEALES. Well, I think the broader definition is, in general, preferable, but I think it does need to be limited to address the advertising problem in some way, because there are a lot of communications that are—that may be advertising supported and where there is partly a commercial purpose for something that comes in electronically or via e-mail.

Mr. SHADEGG. Well, as I understand the Wilson bill, the Wilson bill says if there is any commercial purpose to the e-mail, then it is covered by the law. Whereas the other piece of legislation by Mr. Burr and Mr. Tauzin says if it is primary or for a principal purpose, it is commercial. And the problem I have is I think that fudge language will allow somebody to come in and just put a whole bunch of content in there and allege, "Well, my primary or principal purpose wasn't commercial, and therefore I didn't have to comply with this law."

Ms. SELIS. If I could respond to that——

Mr. SHADEGG. Please.

Ms. SELIS. [continuing] I think of it as an enforcement question. I think about what it is going to be like to——

Mr. SHADEGG. As a former attorney general, so do I.

Ms. SELIS. Yes. When you go into court what is their first defense going to be? Well, it wasn't primarily commercial, it was just in part. And the question is how many loopholes, how many hurdles are we going to put in the law such that when an enforcement official goes in, be it the FTC, be it a State attorney general, even be it the ISPs, how many of those hurdles are they going to have to jump over, how many defenses are going to be in there, and I see that language of primary as being a hurdle, frankly.

Mr. SHADEGG. Any other comments on that question? Let me ask a second question. Congressman Cox talked about the issue of the application of the law of trespass. Do any of you—have any of you given thought to the application of the law of trespass to this issue? Do any of you have strong feelings that we should not try to seek to extend the law of trespass to this? Because I consider it a trespass. Whether it is trespass into my computer or trespass into a space on the Internet service provider that I am currently renting, it seems to me when you send me an e-mail I don't want, you are trespassing. Comment on that? Yes, sir. Mr. Murray.

Mr. MURRAY. The case that I believe Representative Cox was referring to is the Hamidi v. Intel case which recently came down. I did not read the decision carefully but what I saw distinguished in that case was political speech versus commercial speech. And what they said was we will not limit political speech over companies' networks. We will not allow you to censor your employees' political speech. I think that this——

Mr. SHADEGG. Yes, I would agree with that.

Mr. MURRAY. [continuing] is a clear distinction between—this is only commercial speech which is within the purview of both of these bills.

Mr. SHADEGG. Other comments on the extension of the law of trespass explicitly?

Mr. CURRAN. The doctrine of trespass has always been vital to ISPs' protection of their networks. That said, recognize that there are 50 States. This is the common law of each particular State. California's decision may not be binding as it applies, while certainly influential.

Mr. SHADEGG. Well, we can write a statutory provision on trespassing into Federal law in this legislation, I think.

Mr. Cox seems to think so as well.

Mr. CURRAN. It is a difficult area in terms of leaving to the States their historical area of competence as to the protection of private property rights of which trespass is one of the core.

Mr. SHADEGG. So you have a reservation about that.

Mr. CURRAN. It is an interesting issue.

Mr. SHADEGG. It is an interesting issue. Other comments? Safe harbor, there is a limited safe harbor provision in one of the bills and no safe harbor provision in the other. Would any of you advocate that we need—there was some comment earlier about some of the opt-outs or some of the provisions that would not be covered, that specifically say, well, a warranty update or a privacy policy update gets you out of coverage under the law. Are there other safe harbors that any of you would advocate? Yes, sir?

Mr. HIRSCHMAN. Can you hear me?

Mr. SHADEGG. Yes.

Mr. HIRSCHMAN. I would certainly advocate some form of safe harbor for any form of statute that were enacted, primarily because it would further the concept of accountability. It would force people to come forward and say, "I am a mailer and this is the IP address through which I am mailing." This is a practice that we at Digital Impact already do. We go to ISPs and we say, "Here is a list of all of our IP addresses with a list of the clients behind them. Do as you see fit but we are going to use best practices." I have no doubt

that the best practices that we require our clients to use are going to be better than whatever we will see in legislation or regulation because we are extremely strict. What I would like to see is some form of safe harbor whereby if a company has satisfied all the conditions of the safe harbor, they could avoid the costly litigation of trying to prove that e-mail wasn't commercial or that e-mail was not unsolicited or the rest of the litigation that can go along with this.

Mr. SHADEGG. Yes. I actually have read the safe harbor provision that is in the legislation, and I don't think it makes sense but I think we should have safe harbor provisions along the lines of what you suggest where if you engage in these practices and you in fact have done them all, you ought to be able to get yourself out of the litigation loophole. So I appreciate your testimony.

Mr. STEARNS. Thank the gentleman. The gentleman from Massachusetts.

Mr. MARKEY. Thank you. Mr. Murray, if you get spammed on your desk, at least you can leave your desk, but if you get spammed on your wireless device, it is traveling with you. You are like a mobile target for spammers. Are you of the opinion that the legislation which we pass should also deal in a comprehensive way with the wireless world so that we in an anticipatory way try to avoid having the same mess created in the wireless world that has already been created in the online world?

Mr. MURRAY. From a consumer perspective, I think that it is critical that we consider wireless spam, which is ramping up extremely quickly. The growth rate of wireless spam is quite troubling. There is a political expediency question which Representative Burr raised. I think consumers should get a spam bill and they should get one soon.

Mr. MARKEY. Did you say there is an expediency issue?

Mr. MURRAY. Yes, sir.

Mr. MARKEY. What is that?

Mr. MURRAY. Just in the sense of I would like to see a bill come out of committee, and if that were terribly controversial and it would risk stopping the bill——

Mr. MARKEY. Should it be controversial?

Mr. MURRAY. I don't think it should at all, but I have worked with—let me restate that. I think that consumers absolutely deserve a strong wireless spam measure, and I would love to see it included in this bill. I would hope that it wouldn't be controversial on the committee or in the full House.

Mr. MARKEY. So you do support it wholeheartedly, though.

Mr. MURRAY. Absolutely.

Mr. MARKEY. Okay. The Cellular Telephone and Internet Association, CTIA, estimates that last December wireless carriers processed more than 1 billion text messages, four times higher than just 1 year earlier. In Japan, the dominant wireless carrier, Dokamo, processes 1 billion messages a day, and some estimate that 80 percent of that is unsolicited messages. So from a—again, from a political perspective but more importantly from a consumer perspective, isn't this the time, isn't this the place to do it rather than waiting? We might not return to the issue for 4 or 5 years?

Mr. MURRAY. Absolutely. I agree with that 100 percent. And as I noted earlier, there is the possibility that as we put in a location-based tracking system for cellular users, that we will see location-based spam, and I think that we should be working on killing wireless spam and all of its iterations.

Mr. MARKEY. But you are saying that you don't want it to be delayed a day, though. How much time would you delay if there was opposition to protecting against wireless?

Mr. MURRAY. I believe that that falls more clearly within your realm of expertise.

Mr. MARKEY. Thank you so much, yes.

And we will try to make that determination, because I don't think it would really be a good idea for us not to take this opportunity, which might not arrive for several more years if we don't take it as this train is leaving the station. And I think, to be honest with you, it would really irritate people so much more to be spammed on their cell phone than they ever feel in terms of irritation on their computer. I mean it just would wind up causing something that would match the reaction to the national do not call list that we have been seeing over the last 9 days in America. So I thank you, Mr. Chairman, very much, and I look forward to working toward the goal of including very strong wireless spam protection language in this comprehensive bill.

Mr. STEARNS. Okay. Mr. Beales, I understand you have to leave, and so we want to thank you very much for your kindness and patience in staying, and we will look forward to talking to you again.

Mr. BEALES. Thank you very much.

Mr. STEARNS. And Mr. Walden, you have 8 minutes. You didn't have an opening statement, so you are recognized.

Mr. WALDEN. All 8 minutes was for Mr. Beales but that is okay. No, I am just kidding.

Mr. Rubinstein, you talked about the idea of e-mail best practices and a seal that could accompany, I assume, the e-mail so you would know as the recipient. Is that how that would work?

Mr. RUBINSTEIN. Yes.

Mr. WALDEN. Would there be some guarantee that the seal wouldn't be counterfeited by one of these spammers? Can you prevent that?

Mr. RUBINSTEIN. I think in order for such a seal to be effective, it would have to rely on digital signatures or other encryption techniques to prevent that type of spamming, which would certainly completely undermine the program.

Mr. WALDEN. Right. And you are confident that technology, the encryption technology would work against these folks?

Mr. RUBINSTEIN. I think that would be the best approach from a security standpoint, but it might be harder to implement. Another possibility is to use IP addresses but then we would have to address some of the ways that those can be spoofed. So there are discussions underway looking at the appropriate technology.

Mr. WALDEN. Ms. Selis, welcome as a fellow Northwesterner. I represent the district right up against Washington State. I wondered when we are talking about trying to track these people down, the way they make money is through people's credit cards on the Internet, I would guess, pretty much—I mean how do they—some-

how they are getting paid for the porno or whatever. Is there a way to go after it from the financial side or the tax side?

Ms. SELIS. Well, your question brings up sort of the fundamental issues with tracking spammers. What we found in our cases is that almost inevitably the merchant, the one who is getting the credit card payment, is not the spammer. The merchant is getting leads from the spammer who in turn is contracting to somebody else to get leads, who in turn is contracting with somebody else, et cetera, et cetera. To give you an example, in one of the cases we brought against a company out of Minnesota, we had to send 14 pre-suit subpoenas to determine exactly who the sender was, and we couldn't do it through the merchant. The merchant was a debt-adjustment company who was in fact from credit card payments in Florida, but that merchant has bought a leave list from somebody else who in turn who had gotten the leads from somebody else, et cetera, et cetera. So would that we could do it that easily, it takes oftentimes—somebody pointed out that it took 2 years to track a spammer that way.

Mr. WALDEN. I also want to ask about this issue of pop-up ads. How do they differ from spam if at all, and how do you nuke them? See, I am in favor of the death penalty for those folks, whoever they are out there. It is absolutely outrageous invasion of privacy, invasion of my private property that this stuff goes on, and there is no good, easy way to get rid of it, and I am curious, how do you feel either of these bills would address that issue, which I think is far more insidious than spam, which is bad enough. I agree with the former chairman's—you know, putting them in the line of cockroaches, although I don't think cockroaches are this bad. Yes, Mr. Betty?

Mr. BETTY. Pop-ups, singularly, the largest thing people hate is spam, the second thing people hate most are pop-up ads. They are very different than spam. How you deal with those issues are different. Like we have done in the spam case, we took a leadership position in that. We offer our users a tool called Pop-up Blocker. I think I have gotten one or two pop-up ads in the last year. I mean there are technologies out there that can prevent these from coming to your web browser. You just have to go to the right people to get it implemented.

Mr. CURRAN. Yes. Fortunately, that issue is much more amenable to technological solutions, and like Earthlink we have introduced pop-up blockers that enable users to deal with the issue at the browser level. So that is perhaps a good news story.

Mr. WALDEN. Yes. Did anybody else have comments on that particular side of things? Yes.

Mr. MISENER. If I may, Mr. Walden, just to go back to the earlier question you asked Ms. Selis about the beneficiaries of spam and it has always seemed to me that the business model of spamming would dry up if no one ever paid——

Mr. WALDEN. Right.

Mr. MISENER. [continuing] for the products advertised. And, therefore, we certainly would support any kind of an additional remedy given to either the State AGs, to the FTC, the Attorney General of the United States or perhaps the ISPs themselves for going after the beneficiaries, the knowing beneficiaries of spam.

And as you may be aware, Chairman McCain offered an amendment to S. 877 recently which would do just that, and we certainly do support that approach.

Mr. WALDEN. What about best business practices among businesses to make sure they know where they are getting their lists or put a privacy statement that says, "We don't know where we are getting this list of e-mail contacts," so the consumers would know?

Ms. SELIS. Well, the notion of best practices, and it has been talked about here, I think it is important also to recognize that you can have best practices but if you have no enforcement mechanism for a violation of those best practices——

Mr. WALDEN. Oh, yes. I am with you on that.

Ms. SELIS. [continuing] they are worthless. So I think it is an intriguing idea. If you put a burden on the merchant who purchases the list to disclose where he got the list or to say, "I don't know where I got the list," or to charge him what some level of liability for getting the list from a spammer. And I think there are some provisions in both of these bills that would do that with assisting and facilitating language. So I think there is fodder for that in the current legislation.

Mr. WALDEN. Okay. The other issue, our own server in my company got hacked into and used as, I guess, a way to bounce e-mail through to other accounts. The only way we knew was because it quit working effectively for our uses, and it turned out it was somebody overseas doing it and it was porno and all of that. Does anything we do here in either of these bills give us the ability to go after these jokers that are operating on some island where there is no governance or in countries where we are unable to really track them down? And it is really a two-part question. One, what do you do in the ungoverned areas? And, two, it seems to me there is also an international trade component that needs to come up in our trade discussions with countries who don't enforce laws against spamming that we may want to have enforced here. And I would welcome your input on those two subjects.

Mr. CURRAN. I think it is also important to consider that while your servers may have records showing that the spam came from an international source, it is also entirely possible that it is a U.S.-based spammer who relayed from an offshore computer back into your computer. So you don't necessarily want to assume too quickly U.S. spammers——

Mr. WALDEN. Right. Good point.

Mr. CURRAN. [continuing] who spam in the English language and negotiate their transactions in dollars are necessarily moving away from the United States when the opportunities are rich enough to, in effect, bounce offshore their computer——

Mr. WALDEN. And then it comes back.

Mr. CURRAN. Exactly. It is a series of piggyback moves. So, certainly, from our perspective, the U.S.-based spammer environment is target rich in terms of the need for enforcement, and we shouldn't let the prospect of potential international issues deter us from taking action against the U.S.-based spammers.

Mr. WALDEN. All right. I appreciate that, and I will close with this one comment. I am not usually a big advocate for lawsuits, but I will tell you what, when you talk about $876 per employee in a

company, I can tell you it is happening because you have got to bring in some high-priced IT person to fix the problem and put in the latest firewalls and all of that. And I think there ought to be a private right of action with multiple damages. I mean I want to go after these people and shut them down and make them pay or it is going to destroy the usefulness of the Internet. It is already destroying small business out there, and something has to happen. So I appreciate all your comments and your testimony today, Mr. Chairman, and I yield back.

Mr. STEARNS. Thank the gentleman. Mr. Davis, recognized for 8 minutes.

Mr. DAVIS. Thank you, Mr. Chairman, and thank you to the witnesses for staying so long. First, I would like to know to what extent there is a consensus in the panel as to the target we have been discussing today, whether there is a prevalent business model for the spammer? Ms. Selis a little while ago described what seemed to be a former business model in terms of what is motivating the spammer, who ultimately is the client or beneficiary? Is there a consensus here? Is it clearly a profit-minded agent who is motivated by the extent to which those few people are actually positively responding to the spammer and providing something of value? Does someone want to take a stab at this?

Mr. CURRAN. I think there are a couple of different business models. There is the spammer who sends on their own behalf and transacts directly. There are professional spammers who rent their services out for hire and who will deliver a script on behalf of a particular advertiser. There is also a lot of lead generation spam where complex business structures are used to—that somebody is an independent agent or contractor, allegedly, will drive traffic toward a particular web site in effect generating leads and getting a cut. But you are correct that ultimately the name of the game is to facilitate even transactions by a fractional portion of the recipients.

Mr. DAVIS. I would presume that from the ISP perspective there is obviously value to your bottom line in minimizing the pop-ups and spamming for the sake of your customers. Some of the written testimony suggests that perhaps not in the case of you but others in your industry you may have some conflict of interest here in two respects I would like you to comment on or anyone else. The first is the extent to which you are arguably spamming your own subscribers, and, second, the extent to which there is a temptation or opportunity for you to share in some of the profits these spammers are deriving by charging them an extra price for the privilege of using your network.

Mr. BETTY. We absolutely wouldn't take any money from a spammer, and we actively shut them down and sue them when we can find them. So that is not a concern of ours at all. We don't practice really—we don't rely on advertising-related revenues, we rely on the money we get on a monthly basis from our consumers as the basis of the relationship with them. So the monies we spend are trying to enhance our fundamental value proposition that we offer, and we will continue to do that if there are no other alternatives.

Mr. RUBINSTEIN. I would concur with that. Microsoft doesn't spam its customers, and we don't profit in any way from spam or sharing, making spam available to—making our customer list available to spammers. I would also add that we do send commercial e-mail to our customers, but it would qualify under this—it would not be treated as spam under this bill.

Mr. DAVIS. Because of the prior existing relationship.

Mr. RUBINSTEIN. Either it is a strictly prior existing relationship or it is subject to an opt-out, so we would readily abide by all of the requirements in this bill.

Mr. MISENER. Mr. Davis, it seems to me that there is one other potential conflict here with the ISPs, which we have raised before, and, hopefully, it is not one that would ever come to pass. But the concern would be that many ISPs have multiple businesses. They not only are providing communications services but also running, for example, e-commerce businesses, certainly for profit. The concern would be that any self-help, any self-remedy offer to ISPs allowed them to filter e-mail in an anti-competitive fashion. And so we certainly would hope that none of the discussion today would allow—or none of the provisions of the bills that would be passed or considered in Congress or here in the House would envision ISPs being able to somehow skirt anti-competition law, and perhaps that can be taken care of in report language.

Mr. DAVIS. To Ms. Selis, how would an aggregate damage cap affect your ability as an attorney general's office as well as others to bring suits against spammers?

Ms. SELIS. Well, there is frankly no reason for it. It would be problematic. When you talk about spammers, you talk about huge volumes. I recently deposed a defendant in one of my cases who sent out 55 million spams a day, and he did this over a period of time. And to put a cap on that kind of activity simply makes no sense, because it is such widespread activity, he is making so much money that if we put a cap o this, if we arbitrarily said X amount of dollars, $1 million, it wouldn't be an effective deterrent for somebody with that huge an operation. So I don't see any reason for it. There is no cap in any other kind of trade violation which this is under existing Federal law, and I don't see any good reason for it in this area either.

Mr. DAVIS. The Burr-Tauzin bill contains a knowledge standard that you as an attorney general would have to prove as part of the bill. How do you think that would impact your ability to effectively enforce such a law?

Ms. SELIS. Well, again, I think that it is a real deterrent to good enforcement, and, again, it is unprecedented. Under existing trade law, intent is not an element of proof. It is an element of proof in a criminal case, and it should be because there are higher penalties in a criminal case, but under the consumer protection law there is no knowledge standard, and to have to prove a defendant's state of mind means more litigation, more cost to the States, more cost to the FTC, more cost to the taxpayers and less effective litigation in the long run.

Mr. DAVIS. The Burr-Tauzin bill, obviously, in a good faith effort to try to boil down the solution here refers to primary purposes Representative Shadegg alluded to. It seems vague. Does anyone

on the panel want to argue that that is not overly vague in terms of having meaningful enforcement here? Does anyone on the panel want to argue that there ought to be a separate opt-out request for each affiliate of a company?

One of the other differences between Wilson-Green and the Burr bill is that Wilson-Green adopts—and I am co-sponsor of Wilson-Green as you can probably tell—adopts the post office standard in terms of protecting people as far as pornographic material. I am trying to stop my sons from growing up too quickly. It is a losing battle. This is a particularly good one for me. Does anyone question whether the Wilson-Green approach is the preferable approach on this particular issue or whether there is something in between?

One of the other differences between the two bills is that Wilson-Green specifically targets as a violation dictionary attacks. I have talked to high schools in my home Tampa that are experiencing this. Does anyone question whether our bill ought to specifically be prohibiting dictionary attacks?

Mr. CURRAN. That is definitely a positive addition.

Mr. DAVIS. Mr. Chairman, thank you very much. That concludes my questions.

Mr. STEARNS. Thank you. The gentlelady is recognized for 5 minutes.

Ms. WILSON. Thank you, Mr. Chairman. I wanted to thank you all for your testimony, and I read your written testimony and have been listening to the testimony in the anteroom here. I appreciate your time and your patience. I had a couple of questions and first for Mr. Curran. Has AOL ever spammed its members?

Mr. CURRAN. Spam is the No. 1 complaint that our members have about our service, so that is not something that we want to do. If we communicate with our members by e-mail, we always provide them an opt-out. And not only that, we offer them a general opt-out in our privacy policy so that they don't ever have to hear from us if they don't want to. And, obviously, that situation is quite different from the experience that many of our members have in the mailbox where they have the kind of outlaw spam that contains a non-working opt-out, completely falsified headers and no meaningful way for the consumer to exercise to choice.

Ms. WILSON. Is ShopDirect.aol.com part of AOL or is that a false header?

Mr. CURRAN. Shop Direct is in fact part of—is part of AOL. And Shop Direct—people who use the Shop Direct service may hear from Shop Direct, but they can always opt-out from those e-mails.

Ms. WILSON. Mr. Chairman, I would just like to make this document as part of the record. It is actually a spam e-mail to me from America Online, I am one of your subscribers and requested multiple times to opt-out. It is a problem even under your service.

Mr. Rubinstein, do you ever——

Mr. STEARNS. So ordered by unanimous consent.

[The document follows:]

Wilson, Heather

From: [redacted]@aol.com
Sent: Sunday, October 21, 2001 8:51 AM
To: Unsubscribe@shopdirect.aol.com; TOSspam@aol.com
Subject: Re: hawilson: Does your computer need a check up? unsubscribe

Dear AOL,

This is the second unsolicited commercial e-mail message I have recieved from AOL. The first was on October 19th and my request to not receive these e-mails is copied, below. It has been 24 hours since making my first request to be removed from your marketing list.

I have not "opted in" to your e-mail marketing and I have not recieved these kinds of messages from you before. This appears to be a new marketing effort undertaken by AOL directly to its subscribers.

As I said before, you probably want to inform your Legislative Liaison staff in Washington that you have recieved this e-mail.

Sincerely,

Heather Wilson
Member of Congress
New Mexico

In a message dated 10/20/2001 6:30:55 PM Mountain Daylight Time, AOLSpecialOffers@shopdirect.aol.com writes:

> Dear [redacted],
> Give your PC a check up every time you turn it on without doing ANYTHING!
> AOL's <A HREF="aol://4344:157.emm6922.751279.681592378">PowerSuite Deluxe </A>, created specially for AOL members, is the easiest way to TUNE UP and TURBOCHARGE your computer!
> And don't be bothered with deleting unnecessary files, troubleshooting a problem with your modem, or figuring out how to change a setting that you didn't mean to change!
> PowerSuite Deluxe is the only resource you need to keep your computer running at PEAK PERFORMANCE with little effort! The CD-ROM set includes:
> - CleanSweep2000 - Need more disk space? Who doesn't? Let this software by Norton clean up your hard drive for you! You don't even need to be at the computer since you can schedule regular cleanings!
> - FirstAid 2000 - What a life saver! This software identifies most problems before they even happen!
> - Second Chance 2000 - Ooops! Didn't mean to change that setting? Or wish you hadn't downloaded that file? Let Second Chance take you back in time to restore your system to an earlier "checkpoint."
> - WebRecord - That was the coolest web site!!....but what was it and how did I

> find it? Let WebRecord keep track of every site you visit and save the
> addresses
> for you!
> - Interactive Guide to Learning Windows - Let a Microsoft expert walk
> you through Windows. Go through every tutorial or just jump around to the
> areas you need help with.
>
> SO TAKE CHARGE AND MAKE YOUR PC WORK HARDER FOR YOU!
>
> To find out even more about PowerSuite Deluxe please <A
HREF="aol://4344:157.emm6922.751279.681592378">CLICK HERE</A>: Your
> satisfaction is guaranteed with our 30-day money back offer and easy return
> policy. If you're not satisfied, simply return your order for a full
refund
> including shipping and handling!
>
> In an effort to help our preferred members enhance their overall AOL
> experience, AOL Shop Direct is happy to bring the best and most widely-used
> products directly to you! Nothing could be easier, faster, more secure or
> convenient than purchasing our best product through AOL Shop Direct. And,
> everything is 100% guaranteed!
>
> Thank you for choosing AOL Shop Direct.
>
> Sincerely,
>
> AOL Shop Direct
> Customer Service Department
> (KW: SHOP DIRECT)
>
> - Subscription Information
> While AOL Shop Direct is happy to bring the best and most widely-used
> products directly to you, we also respect your right to privacy online. If
> you do not wish to receive any further messages from AOLSpecialOffers@AOL
> Shop Direct, please reply to this message and type "unsubscribe" in the
> subject line and include the original message. This option will not affect
> any preferences you may have previously expressed with respect to other
> America Online emails.
>
Subj: Re: [redacted]: Automatically clean-up your hard drive
Date: 10/19/2001 7:48:05 AM Mountain Daylight Time
From: [redacted]
To: Unsubscribe@ShopDirect.aol.com
BCC: Dawn.Petchell@mail.house.gov

Dear AOL,

You are sending me unsolicited commercial e-mail. I have not "opted in" to this type of e-mail and you should consider this to be formal notification that you should take me off your list.

You may wish to notify your legislative liaison in Washington that I have made this request.

Sincerely,

Heather Wilson
Member of Congress
New Mexico

Ms. WILSON. Thank you, Mr. Chairman.

Mr. Rubinstein, does Microsoft spam their MSN or Hotmail members?

Mr. RUBINSTEIN. Like AOL, we communicate with our customers by e-mail, but we always offer an opt-out with one narrow exception, which is Hotmail sends a monthly subscriber letter and that is an opt-in letter that you agree to receive as part of the service, and it is one letter per month. Other than that, I am sure that we make every effort not to spam our customers, but we may have made mistakes in the past, and if we have, I would only emphasize that those are mistakes not a business practice. We don't profit from spam, and we try to avoid sending spam. And once this bill is passed, we would certainly comply with all the requirements under the bill.

Ms. WILSON. Mr. Betty, in your testimony, in your written testimony anyway, you say that 20 million e-mails could be sent for $149 or less, and I am concerned—and Ms. Selis, you also addressed this same issue—of how do you—how can you make the penalty high enough to discourage the practice? How can you make the cost high enough to discourage the practice so that the potential cost is worse than the gain of continuing to be a spammer, at least on the civil penalty side? How do you go—how should we go about doing that in statute, and what are the most important things to keep in mind? I know that is something of an open-ended question but if you could address that.

Mr. BETTY. I think not having limitations on awards is a big deterrent. People that are repeat offenders if they get increasingly egregious, it would be okay. Our experience when you get to the most notorious of them they aren't making tons of money, they are scraping by a living, and even when you get these awards you are never going to get any recovery but it is such a deterrent that it does prevent them from continuing or they go to jail. So I don't—except for putting them in jail and making it easier for us to get to that point, there is not much we can do.

Ms. WILSON. And perhaps, Mr. Murray, I would like to end with you, and I also found your testimony to be interesting on this issue of what is commercial e-mail. And from your perspective, having looked at both of these approaches and probably numerous others, what is the best approach to defining what it is that consumers have the right to opt-out of?

Mr. MURRAY. Well, I will say for starters that I think primary purpose provides wiggle room that is just unnecessary. I know the representative from the Federal Trade Commission indicated that there were some e-mails we would like to allow through if it comes from a newspaper and it is an article with an advertisement attached. I don't see—even if we provide for an opt-out, that is not particularly onerous. So I don't see any reason to not have a broad definition of what is unsolicited commercial e-mail. I think that providing loopholes is just setting up consumers for more spam.

Ms. WILSON. Thank you. And I want to thank all of you. I think Mr. Davis said something that I think was really striking is this question of should customers be required to opt-out of every affiliate, and nobody seems to think that that is the right approach. I think several of those questions were really telling. It is a very se-

rious problem, and it is a—everybody thinks that they are not the ones who spam and it is all the other guys, they are all legitimate. But if I am the one who is cleaning it out of my mailbox, I should have the right to say, "Take me off your list. I didn't opt-into any of this." And as far as I am concerned, if I am paying for the service, I should have that right. I thank all of you for your time and your patience today.

Mr. STEARNS. I thank the gentlelady. The gentlelady from California is recognized for 5 minutes.

Ms. ESHOO. Thank you, Mr. Chairman, again for having this important hearing and to all of the panelists. I think that you have given us a good deal of information today, and what I thought I would do since I am the last one, I believe, to make some comments and ask a question is to see if I can summarize because I listened very hard throughout this hearing to what your answers were to the questions that were posed.

Does everyone agree that this has to be enforceable? All right. Everyone is nodding, so no one disagrees. That is applies to all commercial e-mail. Everybody agree on that? All right. That there be strong language that protects not only adults but most especially children from pornographic spamming and just the crap that is out there. I don't know what other way to put it. I don't want to dignify what is done, so maybe that is a good word for it. Everyone agree to that? All right, we have consensus on that. Do you all agree that affiliates be included in the opt-outs? I think that question was asked, but I want to be sure that everyone agrees on that. All right. Are you nodding too? Yes? All right.

I am sorry that the gentleman from the Federal Trade Commission had to leave when he did. I was dying to ask him a few questions, but I think that as a committee we should pose to the Federal Trade Commission some questions, and that is how long did it take the FTC to develop the do not call list, and I think that a list that is developed on this is a cannot spam list. I mean we really have to be tough about it. But I think that we should go back and examine how that was constructed and what were the hurdles for the FTC? How long did it take for them to weed all of that out? Is there a possibility of including in legislation the whole notion of a cannot spam list through the FTC that they would help to make work and actually implement.

It is my recollection, and I don't know if this is an accurate one, but my sensibilities tell me that they were not all that enthused very early on about a national do not call list, and we helped to make that work. I mean certainly there had to be an appropriation but we worked on that for a while. I think that what we do has to be able to weed out the worst of the worst who send and then flip around their e-mail address.

And, again, Mr. Chairman, I hold—I am going to be really consistent about this, that if we don't get this right, we are going to have tens of millions of Americans on our back and justifiably so if we really miss the mark on this. And no one, I don't think, is going to be congratulatory if we put something on the books that cannot be enforced. And I think that, Ms. Selis, you have been enormously helpful today in the answers that you have given to several of my colleagues. So I don't know what other questions I

would ask other than maybe I will ask Ms. Selis given what Washington State has adopted and you have that in place, do you have any recommendations to us that you would make that as strong as your enforcement is, is there something that was left out of this that we can—out of your experience that we can benefit from? Outside of the strong enforcement provisions, are there any other recommendations that you would make to us?

Ms. SELIS. Well, I think that the one thing we can't do is be 50 States or the Federal Government.

Ms. ESHOO. Exactly.

Ms. SELIS. And——

Ms. ESHOO. That was going to be one of my summary questions. Everyone here agrees that we would all benefit from a national law, a strong umbrella rather than—anyone ever try to open an umbrella in the rain when it is not working well? We all know what that is. So we need a strong Federal umbrella.

Ms. SELIS. Right. We need as many people, as many entities who can all do their own level of enforcement in order to stop this problem. One State isn't going to do it, five States isn't going to do it. ISPs, private citizens, a private right of action I think is really important here. It will take a lot of people to solve this problem.

Ms. ESHOO. In listening to the panelists, I think that we always listen for on this side of the dias where you agree with one another and where you disagree, because those are the things—I mean we end up being referees in all of this and try to come out with the best product for the American people. Where are the disagreements here? It sounds to me like you are all kind of agreeing with each other. What are the disagreements amongst you? One of them might be private right to action, yes, and, most frankly, I don't think that would ever get out of a subcommittee or a full committee here. That is just my opinion, but is there anything else that is contentious? Gee, you were all so talkative, now you are so quiet. No. So there really isn't any—there aren't any great bones of contention between you?

Mr. RUBINSTEIN. I am not sure about between us but——

Ms. ESHOO. Well, the panel. I mean you have listened same way as I have all day.

Mr. RUBINSTEIN. The panel did—several people expressed themselves in opposition to the do-not-spam list. I don't know if that is the consensus view of the panel, but that is maybe the trend from what I heard.

Mr. STEARNS. Time of the gentlelady is expired.

Ms. ESHOO. Can he answer? Mr. Chairman, can he answer.

Mr. STEARNS. Sure. Oh, absolutely. Go ahead.

Mr. BETTY. There is very clear consensus on the key, key problems of dealing with all this outlaw spam. And as far as the other elements, they are more perhaps just differences of degree in terms of complementing the anti-outlaw provisions with things that provide for proper consumer choice but not a lot of disagreement.

Ms. ESHOO. Okay. Thank you very much. And thank to you, Mr. Chairman.

Mr. STEARNS. I thank the gentlelady, and I remind all members that the record will remain open if members want to ask questions, particularly to the Federal Trade Commission Chairman. And I

want to thank all the panelists for their time, their answers to our questions. And with that, the subcommittee—both subcommittees are adjourned.

[Whereupon, at 4:50 p.m., the subcommittees were adjourned.]

○