UNSOLICITED COMMERCIAL ELECTRONIC MAIL ACT OF 2001 AND THE ANTI-SPAMMING ACT OF 2001

HEARING

BEFORE THE

COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTH CONGRESS

FIRST SESSION

ON

H.R. 718 and H.R. 1017

MAY 10, 2001

Serial No. 24

Printed for the use of the Committee on the Judiciary

Available via the World Wide Web: http://www.house.gov/judiciary

U.S. GOVERNMENT PRINTING OFFICE

72–304 PS WASHINGTON : 2001

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

COMMITTEE ON THE JUDICIARY

F. JAMES SENSENBRENNER, JR., WISCONSIN, *Chairman*

HENRY J. HYDE, Illinois
GEORGE W. GEKAS, Pennsylvania
HOWARD COBLE, North Carolina
LAMAR SMITH, Texas
ELTON GALLEGLY, California
BOB GOODLATTE, Virginia
STEVE CHABOT, Ohio
BOB BARR, Georgia
WILLIAM L. JENKINS, Tennessee
ASA HUTCHINSON, Arkansas
CHRIS CANNON, Utah
LINDSEY O. GRAHAM, South Carolina
SPENCER BACHUS, Alabama
JOE SCARBOROUGH, Florida
JOHN N. HOSTETTLER, Indiana
MARK GREEN, Wisconsin
RIC KELLER, Florida
DARRELL E. ISSA, California
MELISSA A. HART, Pennsylvania
JEFF FLAKE, Arizona

JOHN CONYERS, JR., MICHIGAN
BARNEY FRANK, Massachusetts
HOWARD L. BERMAN, California
RICK BOUCHER, Virginia
JERROLD NADLER, New York
ROBERT C. SCOTT, Virginia
MELVIN L. WATT, North Carolina
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
MAXINE WATERS, California
MARTIN T. MEEHAN, Massachusetts
WILLIAM D. DELAHUNT, Massachusetts
ROBERT WEXLER, Florida
TAMMY BALDWIN, Wisconsin
ANTHONY D. WEINER, New York
ADAM B. SCHIFF, California

TODD R. SCHULTZ, *Chief of Staff*
PHILIP G. KIKO, *General Counsel*
JULIAN EPSTEIN, *Minority Chief Counsel and Staff Director*

CONTENTS

MAY 10, 2001

OPENING STATEMENT

The Honorable F. James Sensenbrenner, Jr., a Representative in Congress From the State of Wisconsin, and Chairman, Committee on the Judiciary ... 1

WITNESSES

The Honorbale Heather Wilson, A Representative in Congress From the State of New Mexico
Oral Testimony 4
Mr. Rick Lane, Director, eCommerce & Internet Technology, U.S. Chamber of Commerce
Oral Testimony 9
Prepared Statement 10
Mr. Marc Lackritz, President, Securities Insudtry Association
Oral Testimony 12
Prepared Statement 14
Mr. Paul Misener, Vice President for Global Public Policy, Amazon.com
Oral Testimony 17
Prepared Statement 19
Mr. Wayne Crews, Director of Technology Studies, CATO Institute
Oral Testimony 21
Prepared Statement 23

APPENDIX

STATEMENTS SUBMITTED FOR THE RECORD

Prepared Statement by the Honorable George Gekas, A Representative in Congress From the State of Pennsylvania 61
Prepared Statement by the Honorable Bob Goodlatte, A Representative in Congress From the State of Virginia 62
Prepared Statement by the Honorable John Conyers, A Representative in Congress From the State of Michigan 63
Prepared Statement by the Honorable Howard Berman, A Representative in Congress From the State of California 64
Prepared Statement by the Honorable Sheila Jackson Lee, A Represetative in Congress From the State of Texas 64
Prepared Statement by Laura Murphy, Director and Marvin Johnson, Legislative COunsel, American Civil Liberities Union 65

UNSOLICITED COMMERCIAL ELECTRONIC MAIL ACT OF 2001 AND THE ANTI-SPAMMING ACT OF 2001

THURSDAY, MAY 10, 2001

HOUSE OF REPRESENTATIVES,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Committee met, pursuant to notice, at 9:30 a.m., in Room 2141, Rayburn House Office Building, Hon. George W. Gekas presiding.

Mr. GEKAS [presiding]. The hour of 9:30 having arrived, the hearing will come to order. We note the presence of the gentleman from Texas, Lamar Smith, who, along with the Chairman now, constitutes a hearing quorum, legitimizing the entire enterprise.

This hearing has been set to hear testimony on two bills that are of mounting interest to the entire commercial world and to the telecommunications world and to everyone, really. They will be on the subjects that are contained in two bills, H.R. 718, the "Unsolicited Commercial Electronic Mail Act of 2001," introduced by Representative Heather Wilson, and H.R. 1017, the "Anti-Spamming Act of 2001," introduced by Representative Goodlatte.

Both of these bills address problems that have been perceived, imagined, or conceived in the e-mail syndrome, and the bills touch upon most of these apparent or actual problems. There are significant differences which will be highlighted I'm sure by the testimony of the various witnesses. We bring into it, consciously or unconsciously, consideration of constitutional prohibitions, whether or not other acts of Congress are already in place to cover some of the subject matter that are included in these bills, whether or not unintentional abuse occurs, and when you call it abuse, that's in the eyes of the beholder.

Almost everyone agrees that consistent with current law and consistent with our overall intention in these matters, that outright fraud must be dealt with. The question is, will these bills add anything to that community of sanctions that are already in the law.

All these questions and many more, I hope, will be answered through the question and answer period that will follow the presentation of our witnesses.

We now note the presence of a full quorum with additional Members already at their seats. We will begin the testimony.

I will acknowledge that the gentleman from Virginia, Mr. Goodlatte, one of the authors of one of the bills, will be accorded an

opening statement and he may proceed now if he is prepared to do so.

Mr. GOODLATTE. Thank you, Mr. Chairman.

Mr. Chairman, I appreciate you and Chairman Sensenbrenner holding this hearing on what I perceive to be one of the more serious problems that we have with the effective use of the Internet today, and I want to particularly commend my colleague, Heather Wilson, for her work on this issue and the legislation that she has introduced and passed through the House Commerce Committee.

That legislation is somewhat different from the legislation that I have introduced, but it is definitely headed in the right direction and I look forward to working with her and the Members of this Committee and her Committee to come up with a bill which she can carry forward to the floor of the House and hopefully have all of us unified in an effort to address this serious problem with regard to spam.

I have a very lengthy prepared written statement, Mr. Chairman, which I would offer for the record and not read into the record. I would, however, point out what I perceive to be the most serious nature of this problem, and that is what I perceive to be the unethical way in which spammers, commercial spammers, are attempting to subvert the processes used by Internet service providers to regulate what goes on on their systems to avoid the systems crashing and to help provide a service to their customers so that they don't see a continuation of the explosion in the amount of spam that people are receiving.

In 1999, the average consumer received 40 pieces of spam. Some independent studies indicate that that's going to increase 40-fold by the year 2005 to 1,600 pieces of spam for the average consumer.

The Internet service providers engage in a number of activities to attempt to reduce that spam and those who want to defy them, and the many, many consumers who talked to me about the need to control this use a number of means to try to circumvent that process. And the legislation that I've introduced would impose greater sanctions and penalties on those who attempt to do this by making sure that there are criminal sanctions for attempting to subvert this process.

One of the most serious aspects of this is the actual theft of other people's identity using their e-mail address in order to break up spam into smaller packets of—going to groups of people, and in doing so, they I think are very deliberately, particularly when they're sending things like pornographic spam, causing a lot of harm to people when their identification is being used to send out pornography to other people unbeknownst to them and simply as a way of circumventing the efforts of the Internet service providers to prevent these kinds of things from happening.

It's a serious problem that makes the Internet a less useful tool and less desirable thing to use at a time when it is growing dramatically and has tremendous potential for businesses and families, and it is my hope that we will pass legislation that will give law enforcement and Internet service providers and consumers more effective tools to deal with this problem.

Thank you, Mr. Chairman.

Mr. GEKAS. We thank the gentleman.

I ask unanimous consent that the written statement of the gentleman from Virginia and the written statement of any of the Members of the Committee be admitted into the record.

I also ask unanimous consent in two or three other arenas: that the Chair be authorized to declare recesses during today's hearing; I ask unanimous consent that all Members and witness statements be included in the record; and I also ask unanimous consent that the record remain open to receive written responses to written questions that may be submitted to the witnesses and that extraneous material pertinent to the hearing may be included in the record.

We will proceed, then, in a——

Mr. SCOTT. Mr. Chairman?

Mr. GEKAS [continuing]. Segue that has been accorded—yes, the gentleman from Virginia.

Mr. SCOTT. Are you going to afford the opportunity for this side to make an opening statement?

Mr. GEKAS. The only opening statement that I thought would be efficacious would be that of the gentleman from Virginia whose bill is one of the two vehicles that we are considering. I was not going to—I was not going to prolong the hearing with the written—the opening statements. Does the gentleman insist, does he wish to——

Mr. SCOTT. Well, Mr. Chairman, we would insist on having the opportunity to have an opening statement.

Mr. GEKAS. Well, let me debate that with you, but if the gentleman insists, the gentleman is recognized.

Mr. SCOTT. I don't have an opening statement, Mr. Chairman, but I just wanted the opportunity.

Mr. GEKAS. Well, then, I insist you make one. [Laughter.]

Mr. GEKAS. I am going to wait until you make one.

No. Does anyone else have an opening statement which he feels must be made at this time in accompanying—in accompanying the written statements that already have been admitted through unanimous consent?

Mr. CONYERS. Mr. Chairman?

Mr. GEKAS. The gentleman from Michigan does have that prerogative.

Mr. CONYERS. With great trepidation, may I approach the Chair for a few moments' discussion?

Mr. GEKAS. Absolutely. The gentleman from Michigan is recognized. I wish you had a discussion with Mr. Scott before you started.

Mr. CONYERS. How genial.

Members of the Committee and Mr. Chairman and witnesses, I want to say first of all that Mr. Gekas should be congratulated for protecting the jurisdiction of the Committee and holding timely hearings.

Spam is not a trivial issue and anyone using the Internet will tell you it's no fun being constantly bombarded with unsolicited e-mails, and any parent can tell you about the problems of young children being exposed to pornographic spam, and it's costly, too. It takes time to delete and block them out. ISPs must have extra server capacity to handle the flood of e-mails. I am not surprised that the worldwide cost of spam has been estimated at over $9 bil-

lion annually. America Online believes spam accounts for 30 percent of its e-mail traffic.

Now, I hope we can approach this problem with some constitutional discretion. The majority promotes federalism and talks about how congressional action frequently erodes States' rights in the areas of hate crimes, civil rights. But sometimes we find it promoting criminal—well, it promotes legislation that imposes Federal criminal penalties for sending e-mails, and on this issue, I have to tilt in their direction because I'm just not convinced that people want—that we really want people sitting in Federal penitentiaries for sending e-mails.

So I join with the Chair in an inquiry about this very important subject.

Mr. GEKAS. We thank the gentleman.

We will proceed with the panel of witnesses.

Since the opening statement of the gentleman from Virginia, Mr. Goodlatte, as an author of the bill, sets the stage, we will follow with the testimony of the lady from New Mexico, Heather Wilson, the author of the other salient featured bill. She is well known to her colleagues, of course. She is the representative from the State of New Mexico and has been an important cog in the wheels of legislation in our House of Representatives.

We recognize the lady from New Mexico.

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

Ms. WILSON. Thank you, Mr. Chairman. It is a pleasure to be here today. I also wanted to thank the gentleman from Virginia for working—for working on this issue so hard.

The—the bill that—that has passed the Commerce Committee includes some provisions where this is the Committee of expertise and, in fact, those initial ideas came from this Committee and from Mr. Goodlatte in the last session of Congress where we worked together to incorporate those in the Rules Committee, and we reintroduced the bill this year—it passed the House 427 to 1, and we reintroduced the bill this year with his provisions remaining in it knowing that there may be some—some polishing, some issues that—that this Committee would like to do with respect to the criminal aspects of the bill, and I look forward to continuing to work with him on those things, particularly where he has expertise that I do not have, frankly nor does the Commerce Committee, which is why there is joint jurisdiction on these issues.

I first started getting interested in this problem when I started getting junk e-mail. Shortly after I was elected to Congress, I got a junk e-mail that—from somebody that I didn't recognize. It said, "What the Federal Government doesn't want you to know." And thinking this was from a constituent that was telling me about the latest scam at the Defense Department or something, I clicked on the link and found myself in a pornographic Web site without any warning whatsoever, and I concluded from that that the Federal Government doesn't want you to know about female anatomy.

Actually what I—what I began doing was talking with other people about the problem and recognized that I wasn't alone and, in fact, junk e-mail costs the economy about $10 billion a year. The

cost has shifted from the individual sending the e-mail to the Internet service provider. It is a large shifting of advertising costs because it's about as cheap to send a million e-mails as it is to send one.

But more importantly, while as parents you have rights in Federal law to stop junk mail, to stop junk faxes, to stop the telemarketers, and even to put a no-trespass sign on your lawn, you have no rights with respect to the Internet. If you say take me off your list, in many cases the reply address doesn't work, or what it really does is convert—confirm that they've got a live one and they can sell your name for more money than they would if you said nothing at all.

There is a right of free speech on the Internet, but there is no right to force you to listen or to force your children to be subjected to some of the things that I would prefer not be in my home, and I would expect that you wouldn't prefer either.

What this bill does, H.R. 718 does, is require accurate return addresses on unsolicited commercial e-mail, makes a very narrow definition of what unsolicited commercial e-mail is to meet the constitutional tests and problems that Mr. Conyers accurately identifies, makes it illegal to continue to send junk e-mail to someone after they've been asked to be removed from a distribution list. You kind of get one bite of the apple. You get to send that first junk e-mail, whether it's from Eddie Bauer or a porn site, but if somebody says, take me off, you have to respect their—their right to not listen.

It requires that unsolicited commercial e-mail be labelled, which is actually a help for legitimate mail between—that may be in large quantities between a company and subscribers to a service because it's easier to screen it out if it has some kind of a label on it, and sets various penalties for continuing to send junk e-mail after they've been asked to stop.

It does have a private right of action. It also has a limited right of action for State attorneys general with respect to protecting all of the citizens in their States; recognizes that we want to promote growth on the Internet and promote commerce on the Internet while controlling cost-shifting.

I think that this is—there are a couple of issues that I think I want to address that I think are controversial ones. I don't think that the fraudulent routing proscription alone is enough. I mean, I get commercial e-mail at home, whether we do our—my husband does our—manages our retirement accounts online with Schwab; Eddie Bauer sends me their latest sales; I even get Amazon.com. That's by my choice. But when I get unsolicited commercial e-mail that I find offensive, or I get too much of it and I just don't want to have to delete it from my in-box, I should have the right to say no, and I should be able to enforce that right whether it's in metro court or through my State attorney general, or with the Federal Trade Commission.

The flood of get-rich-quick schemes and mortgage refinance offers and pornography that comes in unsolicited commercial e-mail shouldn't be an obligation of the consumer to just put up with. They should have similar rights as they do under—for regular mail and for telemarketing and so forth.

If we only limit this to fraudulent route—fraudulent routing proscription alone, as some of the folks who will testify today will suggest, or suggest in their written testimony, what that really means, if you're shameless and you give legitimate routing information, that's okay.

Well, that's not okay for me as a parent and it shouldn't be okay for this Congress to say, as long as you don't lie about who you are, as long as you don't use somebody else's return mail address, it's okay to send pornography to children and you have to put up with it. That's not the way it should be.

As I said, I believe that there is a right of free speech on the Internet. The bill that we drafted and has passed, passed last year overwhelmingly in this House, recognizes that right. But you do not have a right to force me to listen, and this bill gives citizens and consumers and parents the right to say no, stop sending this to me, and puts the force of law behind it.

I also know that there's some controversy about giving Internet service providers the rights to—to enforce their own policies with respect to junk e-mail. Reality is they have that right now. There is—Internet service providers are not a common carrier. It's not the telephone company. These are private networks that are all linked together in a cooperative kind of Wild West system, and it works very well.

But they have rights to limit what goes onto that network now and they enforce it, and sometimes it's a problem because when companies, whether it's Schwab sending out their monthly statements that all look the same in a mass amount, get slowed down because there's a suspicion that maybe this is unsolicited junk e-mail, when, in fact, it's not, I think this bill will actually help that problem because unsolicited commercial e-mail must be labelled and it will allow Internet service providers to more easily screen using technology and software.

The final thing that I wanted to mention is that issue of, well, isn't there screening technology available for this, can't you push on, you know, Parentcontrols.com to keep some of this out of your—out of your in-box.

It is true that there is technology to help filter this. That technology is imperfect, and what the bill that I've introduced recognizes is that—that your rights as a citizen don't depend on the virtues of technology. You still have those rights to say take me off your list, and you should have those rights, and you shouldn't have to depend on imperfect technology that doesn't always screen out what you want it to screen out in order to—in order to exercise your rights.

The bill does include a private right of action, and I feel very strongly about that. It shouldn't be—you shouldn't have to as a citizen appeal to the Federal Government to say, So-and-So is not doing their job. If you've asked to be taken off a list, if you've asked for your children to be taken off a list, and you've given a reasonable period of time for that—for that to occur, continued infringement of your right to privacy, continued use of your computer and of your time, is an infringement on you and your resources and the sanctity of your home and your family, and you should have a private right of action under law.

I wanted to thank the Chairman for holding this hearing. I think we are working together with Mr. Goodlatte and others who have an interest in this—in this issue, in this bill. We're on the verge of passing a very good piece of legislation that benefits families, and I'm very proud to have been part of working on this, and I look forward to continuing to work with you on it.

Mr. GEKAS. We thank the lady and invite her to remain, if she wishes, for the question and answer period, and, of course, if the press of business calls her away, we will understand.

Let the record indicate that present for this hearing, in addition to the individuals already named, the gentleman from Virginia, Mr. Scott; the gentleman from New York, Mr. Nadler; the gentleman from California, Mr. Berman; the gentleman from Florida, Mr. Keller; the lady from Pennsylvania, Ms. Hart; the gentleman from Arizona, Mr. Flake.

With that, we will indulge in introduction of the individuals who will testify.

Mr. Rick Lane, who serves as the Director of eCommerce and Internet Technology for the U.S. Chamber of Commerce joins us today.

Mr. Lane is responsible for coordinating the development and implementation of the Chambers' eCommerce and Technology legislative and policy initiatives.

Mr. Lane came to the U.S. Chamber from his position as the Director of Legislative Affairs for the international law firm of Wheel, Gotshaw and Mangus. Prior to joining that firm, Mr. Lane was the co-founder and Executive Director of the Modern Education Technology Center, Inc., an educational technology private/public partnership.

From 1988 to 1993, Mr. Lane worked for U.S. Representative Joseph D. Early as an Associate Staff Member to the House Appropriations Committee.

Mr. Lane has also served in leadership positions on a variety of Federal, State and local commissions and committees, including serving on the United States Federal Trade Commission's Advisory Committee on Online Access and Security.

Mr. Lane has also served as Chairman of the Montgomery County Cable and Communications Advisory Committee for a period of 2 years.

Mr. Lane holds an undergraduate degree from the College of Holy Cross.

Next in line to testify is Mark E. Lackritz, who was named President of the Securities Industry Association in December 1992, after serving that institution as Executive Vice President and head of the Washington office since April 1990.

Prior to joining that association, Mr. Lackritz was Executive Vice President and head of the Washington office of the Public Securities Association, now known as the Bond Market Association, a trade group representing bond dealers, from 1987, it was, until 1990.

Previously, he had extensive experience on Capitol Hill. He was Staff Director and Chief Counsel for the Subcommittee on Telecommunications and Finance of the House Energy and Commerce Committee from 1984 to 1987.

From 1974 to 1977, he was Deputy Chief Counsel to the United States Senate Budget Committee, and in 1973 and '74 was an Assistant Counsel to the Senate Watergate Committee.

Mr. Lackritz also was a partner of the former Washington-based law firm Wold, Harkrader and Ross, specializing in litigation, lobbying, trade regulation and international arbitration.

Mr. Lackritz serves on a number of boards and advisory groups, including the Financial Accounting Standards Advisory Council, the American Council on Capital Formation, the Securities Industry Institute, and the Securities Industry Foundation for Economic Education. He was a presidential delegate to the National Summit on Retirement Savings, and a presidential appointee to the White House Conference on Social Security.

He received his law degree in 1973 from Harvard University, a master's degree in economics in 1971 while on a Rhodes Scholarship at Oxford, and a bachelor of arts degree in public policy in 1968 from Princeton University.

Joining him at the witness table is Paul Misener, the Vice President of Global Public Policy at Amazon.com. Both an engineer and lawyer, Mr. Misener is responsible for formulating and representing Amazon.com public policy positions work worldwide.

Mr. Misener currently serves as President of the Internet Commerce and Communications Division of the Information Technology Association of America and member of the ITAA Board of Directors.

Formerly a partner and chairman of eCommerce and Internet Practice at the law firm of Wiley, Rein & Fielding, Paul also served as Senior Advisor and Chief of Staff to an FCC Commissioner.

The final witness is Wayne Crews, the Director of Technology Policy at the Cato Institute. Mr. Crews examines regulatory policy issues such as market alternatives to mandatory open access in network-based industries, Internet governance issues, and other regulatory issues, including antitrust, private, and intellectual property.

Before joining the Cato Institute, Mr. Crews was Director of Competition Regulation Policy at the Competitive Enterprise Institute, and he has served in various other capacities in this field for a long period of time.

We will ask the witnesses to begin in the order in which they were introduced. We will limit each one at the first stage to 5 minutes, and then ask them to remain for the questions that will follow.

We will begin with Mr. Lane. We will use your written statement for purposes of the record and ask you to proceed.

Mr. CONYERS. Mr. Chairman, we don't know anything about their families or their kids or—— [Laughter.]

Mr. CONYERS. I mean, what is this?

Mr. GEKAS. That will come during the question and answer period.

Mr. CONYERS. Okay. All right. Thank you.

Mr. GEKAS. Mr. Lane.

STATEMENT OF RICK LANE, DIRECTOR, eCOMMERCE & INTERNET TECHNOLOGY, U.S. CHAMBER OF COMMERCE

Mr. LANE. Thank you, Mr. Chairman.

Mr. Chairman, Ranking Member Conyers, and Members of the Committee, I am Rick Lane, Director of eCommerce & Internet Technology for the United States Chamber of Commerce.

As you know, the U.S. Chamber is the world's largest business federation, representing more than three million businesses worldwide.

Mr. Chairman and Members of the Committee, I welcome the opportunity to testify on the parameters that we believe should be used in developing legislation that would set the legal framework for businesses that are interested in using commercial e-mail as a marketing tool.

The U.S. has the largest and most dynamic economy in the world. Consumers benefit from a growing range of choices for products and services while the competition between businesses to attract customers is continually intensifying.

E-commerce and the use of technology have played a significant role in expanding the options for consumers and fundamentally changed how businesses interact with their customers. While these innovations have created new opportunities for consumers and businesses, concerns have been raised about how these new technologies may impact privacy, IP, cyber-crime, taxation, trade, and a consumer's basic relationship with a business.

The use of the Internet for commercial purposes is increasingly becoming a make-or-break proposition for businesses throughout the world seeking to maintain a competitive edge. As e-commerce makes the transition from the early hyper-growth stage to the steady long-term growth, it will require a framework that stimulates innovation and private enterprise, and minimizes cumbersome Government regulation.

At the same time the Internet has changed the dynamics for business, it has given consumers a powerful new tool. At no other time in history has the consumer been in such control over their economic domain.

By using the Internet, they now have the power to gather information to comparison shop with little or no cost, which helps to ensure that the service or products they receive from a business are satisfactory. This new consumer power is but one reason why Congress needs to look at market-driven solutions as a more efficient and effective means of consumer protection than just legislation.

Although the use of e-mail for marketing purposes is in its infancy, businesses are developing best practices that use—in their use of commercial e-mail due to the pressures put on them—put upon them by their customers and potential customers. However, the concerns that are driving the current debate on commercial e-mail are not the proactive steps of legitimate businesses, but the misuse of commercial e-mail by individuals who are using this incredible new tool to deceive and commit fraud or send pornographic materials to consumers.

Legislation regulating the use of the commercial e-mail must be narrowly targeted to focus on these clear abuses without interfering with the development of legitimate use of electronic mail for

marketing purposes. Thus, in drafting legislation, we believe the following principles should apply:

The primary focus of legislation regarding commercial e-mail should center around combatting the sending of e-mails with inaccurate header or routing information. These practices not only harm consumers, as we heard thus far, but it also harms legitimate businesses by creating a climate of mistrust of legitimate commercial e-mail.

Legislation must be looked at from an international perspective as well, and what impact such legislation will have on the U.S.—ability of U.S. companies to compete abroad.

Legislation needs to address the concerns of parents and others who want to protect their children or themselves from receiving sexually oriented advertisement. Like fraudulent e-mail, this also creates a climate of mistrust.

Legislation regulating the Internet must also preempt inconsistent State laws and not contain a private right of action. Duplicative and overlapping enforcement mechanisms, particularly provisions granting private rights of action and enforcement capability to State AGs, has the potential to not only create 50 different rules, but would encourage, we believe, frivolous litigation to collect money for little or no harm.

Finally, we strongly disagree with those who state that the use of commercial e-mail is an invasion of privacy. It may be an annoyance, but receiving e-mail from a legitimate business or an individual is not an invasion of privacy. Too often, the privacy issue is used as a means to promote other legislative objectives. We should not fall into this trap when discussing the use of commercial e-mail. Businesses fully realize in order to build a business in the 21st Century, they must develop consumer trust; however, this cannot be accomplished just through legislation, but will require proactive steps taken by businesses to instill consumer confidence through their actions.

Thank you again for this opportunity to testify today, and I would be pleased to answer any questions that you may have.

[The prepared statement of Mr. Lane follows:]

PREPARED STATEMENT OF RICK LANE

Mr. Chairman and members of the committee, I am Rick Lane, Director of eCommerce and Internet Technology for the United States Chamber of Commerce. The U.S. Chamber is the world's largest federation of business organizations, representing more than three million businesses and professional organizations of every size, in every business sector, and in every region of the country. The Chamber serves as the principal voice of the American business community here in this country and around the world through our 89 American Chambers of Commerce abroad.

Mr. Chairman and members of the Subcommittee, I welcome the opportunity to testify on the parameters that we believe should be used in developing legislation that would set the legal framework for businesses that are interested in using commercial e-mail as a marketing tool.

The U.S. has the largest and most dynamic economy in the world. Consumers benefit from a growing range of choices for products and services, while the competition between businesses to attract customers is continually intensifying.

E-commerce and the use of technology have played a significant role in expanding the options for consumers, and fundamentally changed how businesses interact with their customers. The rapid growth of this technology in just a few short years is a clear harbinger of more pervasive changes in the near future. While these innovations have created new opportunities for consumers and businesses, concerns have

been raised about the how these new technologies may impact privacy, intellectual property, cyber crime, taxation, trade, and a consumer's relationship with a business.

E-commerce and the use of the Internet is no longer a pet-project of corporate IT departments. It is increasingly becoming a make or break proposition for businesses throughout the world seeking to maintain a competitive edge. The development of e-commerce has taken place at a heady pace, stimulated by the ability of entrepreneurs to compete in a remarkably free marketplace. As e-commerce makes the transition from the early hyper-growth stage to steady long-term growth it will require a framework that stimulates innovation and private enterprise and minimizes cumbersome government regulation.

E-commerce and the Internet have drastically changed the public policy debate. It is impossible just to apply old legislative paradigms to the new economy without fully understanding the broad implications such paradigms may have on the incredible growth of e-commerce. Many of the issues surrounding e-commerce are far too complex and moving too fast for legislators and regulators to fully grasp and foretell the unintended and potential negative implications that legislation or regulations may have on this dynamic sector.

At the same time the Internet has changed the dynamics for business, it has given consumers a powerful new tool. At no other time in history has the consumer been in such control over their economic domain. By using the Internet they now have the power to comparison shop with little or no cost which helps to ensure that the service or products they receive from a business are satisfactory. Unfortunately, many of the pure dot-com players found this out too late and are now suffering the consequences because consumers went to their competitors.

This new consumer power is but one reason why Congress needs to look at market driven solutions as a more efficient and effective means of consumer protection than just legislation. Businesses understand all too well that if they are not providing a customer with what that customer needs, other businesses will. No longer is a customer bound by geographic location to a business, but in a nano-second can travel anywhere in the world to buy that same product and get the exact service they want with just a click of the mouse.

Although the use of electronic e-mail for marketing purposes is in its infancy, businesses are developing best practices in their use of commercial e-mail due to the pressures put upon them by their customers and potential customers. Thus we believe that initial legislation regulating the use of commercial e-mail must be narrowly targeted to focus on the clear abuses without interfering with the development of legitimate uses of electronic mail for marketing purposes.

We must also be conscious not to look at this legislation just from a U.S. perspective, but from an international perspective as well with the ability of U.S. companies to compete abroad. For example, if the United States passes overly broad e-mail restrictions, other countries are very likely to follow our lead. This would hinder the ability of U.S. business, especially small businesses, to approach potential customers at home and abroad and to provide upstart competition to established companies in key markets. Alternatively, if the U.S. passes overly broad e-mail restrictions, U.S. companies will be constrained by liability and litigation while unscrupulous companies outside the U.S. continue their fraudulent ways.

The concerns that are driving the current debate on commercial e-mail are not the proactive positive steps of legitimate businesses, but the misuse of commercial e-mail by individuals who are using this incredible new tool to deceive and commit fraud or send pornographic materials to consumers.

Unfortunately for legitimate business, the perception seems to be that a large percentage of commercial e-mail is fraudulent. Therefore, the primary focus of legislation regarding commercial e-mail should center-around combating the sending of fraudulent and deceptive e-mail. Critics of commercial e-mail are absolutely right that this type of commercial e-mail hurts consumers and legitimate businesses and must be stopped. Fraudulent and deceptive e-mail not only harms consumers, but it also harms legitimate businesses by creating a climate of mistrust of legitimate commercial e-mail. That is why the Chamber would support legislation targeted toward making it illegal to send information with misleading or inaccurate header, contact, routing information or e-mail text with the intent to deceive or commit fraud against a consumer.

We also believe that legislation needs to address the concern of parents and others who want to protect their children or themselves from receiving sexually oriented advertisement. Like fraudulent e-mail, this also creates a climate of mistrust for legitimate e-mail marketers.

In addition, the Chamber believes that legislation regulating the use of commercial e-mail must preempt inconsistent state laws. Duplicative and overlapping en-

forcement mechanisms, particularly provisions granting private rights of action and an enforcement capability to state attorneys general, has the potential to not only create 50 or more rules, but would encourage frivolous litigation to collect money for little or no harm. While we applaud attempts to limit the use of private rights of action, these limitations do not overcome our serious concerns with such an ill-advised enforcement scheme.

Finally, we strongly disagree with those who state that the use of commercial e-mail is an invasion of privacy. It may be an annoyance, the e-mail may be fraudulent, but receiving e-mail from a legitimate business or an individual is not an invasion of privacy. Receiving e-mail is no more of an invasion of one's privacy than receiving a letter in the mail. Too often, the privacy issue is used as a means to promote other legislative objectives. We should not fall into that trap when discussing the use of e-mail for commercial purposes.

What does the use of commercial e-mail mean to the future of our economy? Because it is still in its infancy no one really knows. What we do know is that the use of the Internet will continue to create market efficiencies that will generate economic growth in a free market economy and will provide consumers with more product choices and services. Businesses fully realize that in order to build a business in the 21st Century they must develop consumer trust. However, this cannot be accomplished just through legislation, but will require proactive steps taken by business to instill consumer confidence though their actions.

Thank you again for the opportunity to testify today. I would be pleased to answer any questions you might have.

Mr. GEKAS. We thank the gentleman and we turn to the next witness, Mr. Lackritz.

STATEMENT OF MARC LACKRITZ, PRESIDENT, SECURITIES INDUSTRY ASSOCIATION

Mr. LACKRITZ. Thank you, Mr. Chairman. I appreciate the opportunity to be here today to testify on this legislation. I wanted to thank you, Mr. Chairman, for that very fulsome and generous introduction before. So I won't talk about—about who I'm representing, other than to say I'm here to testify on behalf of the Securities Industry Association, which is the national trade association for the broker-dealer industry, and also to testify on behalf of the Financial Services Coordinating Council, which is comprised of five leading trade associations in financial services: The American Bankers Association, the American——

Mr. GEKAS. You just added to the introduction.

Mr. LACKRITZ. I'm sorry?

Mr. GEKAS. You just continued to add to the introduction.

Mr. LACKRITZ. I apologize. I apologize. But my colleagues from those associations would be very upset if I didn't mention I was also testifying on their behalf.

Also included the American Council of Life Insurance, and also the Investment Company Institute.

Mr. Chairman, the technological innovation that has spread so globally and so rapidly has really reordered and reshaped the global economy. The leading edge of the powerful new wave of innovation is the information revolution, which has been essential to improving the world's productivity. The speed of the Internet's development and adoption are incomparable with any other communications technology ever.

It has also been a very powerful force in the democratization of the financial marketplace. In 1983, for example, an estimated 42 million Americans owned stocks directly or through mutual funds. By 1999, that figure had grown by 86 percent to over 78 million

households. And average trading volumes, Mr. Chairman, had increased 12 times in only 16 years.

Technological advances such as the Internet have brought many benefits to investors, issuers, and the securities industry. Information is more ubiquitous, more products and services can be offered with greater efficiency and lower cost, and larger, more competitive marketplaces have been created. And it's technology which has literally re-engineered the financial marketplace.

In the United States, investors have embraced the Internet to manage their finances. In fact, it's often described that the Internet is sort of the killer ap—that Internet trading is the killer ap in the new environment.

In 1995, only one firm offered online trading. Five years later, last year, there were more than 200 online trading firms, 19 million accounts, and $1.1 trillion invested online. And last year, 42 percent of all retail securities transactions were entered over the Internet.

Last year, Congress enacted the E-Sign Act, which gave legal standing to electronic signatures. As a result, many financial services firms began offering their consumers subscription-based products, such as newsletters, research reports, that kind of thing, via e-mail that allow their consumers to request the delivery of trade confirmations, monthly statements, prospectuses, and other customer communications mandated by the securities laws. These communications may number in the millions per day for some of our larger firms.

For the new cyber-economy to flourish, we should allow electronic commerce to grow in an environment driven by consumers and markets, unburdened by outmoded regulations or excessive regulatory red tape. Restrictions on the use of the Internet, if any, should only be very narrowly tailored to address a proven problem, not a perceived one.

None of us on this panel or I suspect anyplace else likes spam, but each of us probably define it somewhat differently. Any Congressional action here really should very carefully balance the legitimate commercial benefits of e-mail against the consumers' need to exercise control over what he or she receives through a computer.

We think the most effective way to achieve that balance would be to pass legislation that reduces the incentive to send misleading and/or fraudulent e-mail. Such legislation will address the spam problem while preserving the many benefits of electronic communication.

Three Members of this Committee—Representatives Goodlatte, Smith and Boucher—have introduced H.R. 1017, a bill which we believe achieves these critical goals. H.R. 1017 would establish Federal criminal penalties for those who intentionally and without authorization initiate defective unsolicited e-mail messages, as well as those who design computer software that facilitates this conduct.

The other pending bill before this Committee, H.R. 718, also attempts to criminalize behavior that results in false or inaccurate e-mail, but it also contains provisions that go far beyond what we believe is necessary. And our three principal objections to H.R. 718 are that it would, one, inhibit the growth of the Internet; secondly,

give certain Internet service providers policies which would have the force of law; and three, it would expose businesses to the threat of wide-ranging and potentially open-ended litigation.

H.R. 718 does not stop with fraudulent or misleading commercial e-mail. It seeks to restrict and preclude legitimate commercial communications between businesses and their customers or prospective customers.

In addition, H.R. 718 would give certain ISP policies the force of law, and that's—that's unprecedented. If that should happen, the contracts entered into between a firm and its customers will be disrupted, and an ISP that cuts off e-mail after more than a certain number of bulk e-mails may well prevent a customer from receiving communications they are entitled by law to receive.

Nothing would chill the continued expansion of the Internet faster than the very real threat of wide-ranging and potentially open-ended litigation.

Mr. Chairman and Members of the Committee, the Internet is in its infancy. It has already produced a myriad of new opportunities for consumers. We share your concern over the abuse of unsolicited commercial e-mail, but we believe enacting legislation that frustrates the innovative use of the Internet would be bad and misguided public policy. Moreover, it would constitute a severe overreaction to a problem that can be addressed far more narrowly along the lines of H.R. 1017.

Mr. Chairman, SIA appreciates the opportunity to share our colleagues—to share our views with you this morning and we're eager to work with you and your colleagues.

Thank you very much.

[The prepared statement of Mr. Lackritz follows:]

PREPARED STATEMENT OF MARC E. LACKRITZ

Mr. Chairman, my name is Marc E. Lackritz, and I am President of the Securities Industry Association (SIA), the national trade association for the broker-dealer industry. SIA coordinates the shared interests of more than 680 securities firms nationwide and SIA member-firms (including investment banks, broker-dealers, and mutual fund companies) are active in all domestic and foreign markets and in all phases of public finance. Collectively, the U.S. securities industry directly manages the accounts of approximately 50 million investors and tens of millions more indirectly, through corporate thrift and pension plans. The industry contributes more than $300 billion annually to the U.S. economy and employs some 700,000 people.

Technological innovation has spread worldwide with lightning speed, reordering and reshaping the global economy. The leading edge of the powerful new wave of innovation is the information revolution, which has been essential to improving the world's productivity. The speed of the Internet's development and adoption are incomparable with any other communications technology—ever. Radio existed for 38 years before 50 million people tuned in; television took 13 years to reach that benchmark. Sixteen years after the first personal computer came out, 50 million people were using one. Only 61 million people worldwide were connected to the Internet in 1996; during the first decade of this century, more than a billion people will be using the Internet worldwide.

The Internet has also been a powerful force in the democratization of the financial marketplace. In 1983, for example, less than 20 years ago, an estimated 42.4 Americans owned stocks directly or through mutual funds. In 1999, that figure grew by 85.6 percent, to over 78 million, and average daily trading volumes increased 12 times over 1983's level. Investors now have unprecedented access to markets, instantaneous trading data, and extensive information once available only to securities professionals. Customers and clients can bypass a broker altogether to buy or sell stocks, gather research, track their own investment portfolios, or participate directly in initial public offerings from their computers.

Technological advances such as the Internet have brought many benefits to investors, issuers, and the securities industry. Information is more ubiquitous, more products and services can be offered with greater efficiency and lower costs, and larger, more competitive markets can be created. From customer service to automated clearance and settlement of trades to the very concept of what constitutes an exchange, technology has re-engineered the nation's financial marketplace. Vast amounts of information, increasing exponentially every day, are driving the markets, the industry, and the economy. Brokers communicate with their clients using email and graphically rich, information-packed Web pages.

In the United States—where half of all households have Internet access—investors have embraced the Internet to manage their finances. In 1995, online trading had just begun with just one firm offering trading capability over the Internet. Five years later, in 2000, there were more than 200 online trading firms, 19 million accounts, and $1.1 trillion in invested assets. By 2003, that figure could rise to $3.1 trillion as assets shift from older heads-of-households to younger generations and as Internet access increases. In 2000, 42 percent of all retail trades were entered over the Internet. And just last year, Congress enacted the E-Sign Act, which gave legal standing to electronic signatures. As a result, many financial services firms began offering their customers subscription-based products via electronic mail that allow their customers to request delivery of trade confirmations, monthly statements, prospectuses and other customer communications mandated by the securities laws. These communications may number in the hundreds of thousands per day for any particular firm. The passage of the E-Sign Act (as well as strong customer demand) encouraged the proliferation of these products by ensuring that the terms and disclosures made by firms when registering customers on line would be as enforceable under Federal and state law as any paper contract.

For the new cyber-economy to flourish, the government, market operators, and regulators must allow electronic commerce to grow in an environment driven by markets, unburdened by outmoded regulations and excessive regulatory red tape. Any restrictions on the use of the Internet should be very narrowly tailored to address a proven problem, not a perceived one. None of us likes "SPAM," or unsolicited email, but each of us probably defines it somewhat differently. As this hearing demonstrates, few of us can readily provide a consensus definition of SPAM. Congressional action should carefully balance the legitimate commercial benefits of email against the consumer's need to exercise control over what he or she receives through a computer.

The most effective way to achieve that balance is to pass legislation that reduces the incentive to send misleading and/or fraudulent email. Such legislation will address the SPAM problem while preserving the many benefits of electronic communication. Three members of this Committee, Representatives Bob Goodlatte, Lamar Smith, and Rick Boucher, have introduced H.R. 1017, a bill we believe achieves these critical goals. H.R. 1017 would amend title 18 of the U.S. Code to establish federal criminal penalties for those who "intentionally and without authorization" initiate defective unsolicited email messages, as well as those who design computer software that facilitates this conduct.

Importantly, Reps. Goodlatte and Boucher, in their roles as the House co-chairs of the Congressional Internet Caucus, are extremely well versed and knowledgeable on Internet-related public policy issues. Having immersed themselves in these issues, they—as well as several other members on this Committee who also serve on the Internet Caucus—may be more sensitive to the need to exercise caution when considering legislation that imposes restrictions on the use of the Internet.

The other bill pending before this Committee, H.R. 718, also attempts to criminalize behavior that results in "false or inaccurate" email (section 4). But it also contains provisions that go far beyond what we believe is necessary. Our three principal objections to H.R. 718 are that it would: 1) inhibit the growth of the Internet; 2) give certain Internet Service Provider (ISP) policies the force of law; and, 3) expose businesses to the threat of wide-ranging and potentially open-ended litigation.

H.R. 718 WOULD INHIBIT THE GROWTH OF THE INTERNET

As currently written, this bill does not stop with fraudulent or misleading commercial email. It seeks to restrict and preclude legitimate commercial communications between businesses and their customers or prospective customers. In so doing, it fails to take into account whether such email is indeed burdensome to consumers. It also fails to address the extent to which unsolicited email enters this country from abroad. In section 3(15) of the bill, "unsolicited commercial electronic mail message" is defined in such a manner as to encompass *any* email message which is 1) sent without the affirmative consent of the recipient and 2) falls outside the narrow defi-

nition of "pre-existing business relationship" contained in section 3(13). Section 3(13), in turn, provides that businesses would fall under the SPAM restrictions in H.R. 718 unless, over a five-year period *prior* to the issuance of a commercial email message, businesses (including their affiliates) had engaged in a "business transaction" and the recipient, at the time of that transaction or at the time the email was sent, was provided an opportunity to "opt-out" of receiving any "further messages."

SIA believes this language is overly broad and unnecessary. Title V of the *Gramm-Leach-Bliley Act* (GLB) recognized the value of the relationship between businesses (including their affiliates) and their customers. In that legislation, Congress only placed an "opt-out" obligation on the sharing of customer information with third parties. Absent a showing that the legitimate use of email by businesses has been abused, and we are unaware of any such showing, we believe this opt-out obligation, and its broad application to "the initiator and any affiliates of the initiator" (section 5(a)(1) and 5(a)(2)), is unwarranted. It is also contrary to the expressed goals of the Internet to promote, rather than deter, electronic commerce. The "opt-out" regime anticipated by H.R. 718 could well have the unintended and counterproductive effect of stifling the ability of businesses to market their products and services effectively to both consumers and other businesses. In turn, consumers would be deprived of the use of accurate and beneficial information about those products and services.

H.R. 718 WOULD GIVE CERTAIN ISP POLICIES THE FORCE OF LAW

Subsection 5(b)(1) prohibits the transmission of unsolicited commercial email that violates an ISP's policy *or* results from the receipt by that ISP of "a significant number of complaints" from its subscribers—an open invitation to litigation. In addition, section 5(d) provides ISPs with immunity from *all* liability—including both criminal and civil liability at either the state or federal level—for any "good faith" effort to block the transmission of unsolicited commercial email messages. This immunity has no limits and should be dropped. Moreover, the language in subsection 5(c) appears to give ISP policies even more authority than they already have in the balance of the section. Notwithstanding what is said elsewhere in the bill, this subsection apparently would allow ISPs to adopt wide-ranging policies "regarding commercial or other electronic mail" and enforce them "under any other provision of . . . law." The inconsistency over how this authority interacts with the power to construct policies relating to unsolicited commercial email provided elsewhere in section 5 certainly deserves the Committee's very close scrutiny.

If each Internet Service Provider's email policy is given the force of law, the contracts entered into between a firm and its customers will be disrupted. An ISP that, for example, refuses to accept more than a specified number of "bulk" emails originating from the same location, regardless of its content, may prevent a customer from receiving communications they are entitled by law to receive. Further, the company sending the required communication might not even be aware that the customer did not receive it. An ISP's failure to do so hurts consumers, interferes with a company's ability to communicate with its customers and is a large step backwards from the progress made in the area of e-commerce.

H.R. 718'S ENFORCEMENT PROVISIONS ARE OVERLY BROAD AND POTENTIALLY ONEROUS

Nothing will chill the continued expansion of the Internet faster than the very real threat of wide-ranging and potentially open-ended litigation. The ISP policies outlined in section 5 of the bill all suggest a strict liability standard of proof when a violation is alleged. No intent, or even knowledge, is necessary to prove a violation. Violations can be accidental. If the obligations imposed on businesses regarding unsolicited commercial email are violated, the conduct that brought about that violation, however motivated or even known, is deemed "unlawful." This phrase is repeated throughout the section and, while an alleged violator is allowed to raise an affirmative defense that the "violation was not intentional," that defense is only available *after* the charge has been leveled and the public onus has attached. Moreover, the affirmative defense is only available for allegations flowing from violations of subsection 5(a). If a business is alleged to have violated subsection 5(b), in which unsolicited commercial e-mail is prohibited in accordance with ISP policy or as a result of "a significant number of complaints," there is no such defense, and the business may be subject to a wide range of litigation. For example, the business could be subject to administrative enforcement by the FTC (subsection 6(a)), civil causes of action by an ISP or the recipient of an unsolicited commercial email (subsection 6(b)) at either the state or federal level, *as well* as State Attorneys General (subsection 6(c)). In addition, the civil causes of action, which, as mentioned previously,

may be the subject of strict liability standards of proof, are then subject to liquidated damages of $500 per violation, with a total of $50,000 (subsection 6(b)(B)). The prospect of litigation in 50 states and the federal courts is a daunting one, especially when the resulting case law will inevitably be confused and uncertain. The safer choice might be to disengage entirely in the use of commercial email.

Mr. Chairman and members of the Committee, the Internet is in its infancy as a medium, yet it has already produced a myriad of new opportunities for consumers. The securities industry is dedicated to providing outstanding customer service and to ensuring that broker-dealers abide by the highest standards of professionalism. Indeed, we routinely administer rigorous policies and procedures to ensure that the clients' interests come first. We share the Committee's concern over the abuse of unsolicited commercial email, but we believe enacting legislation that frustrates the innovative use of the Internet would be bad and misguided public policy. Moreover, it would constitute a severe over-reaction to a problem that can be addressed with a narrowly tailored solution along the lines of H.R. 1017.

Mr. Chairman, SIA appreciates the opportunity to share our views with you this morning, and we are eager to work with you and your colleagues to craft legislation that addresses the SPAM problem while preserving the many benefits of electronic communication.

Mr. GEKAS. We thank the gentleman and we turn to Mr. Misener.

STATEMENT OF PAUL MISENER, VICE PRESIDENT FOR GLOBAL PUBLIC POLICY, AMAZON.COM, REPRESENTING AMAZON.COM AND THE NATIONAL RETAIL FEDERATION

Mr. MISENER. Good morning, Chairman Gekas and Members of the Committee.

As you indicated, Mr. Chairman, my name is Paul Misener. I'm from Amazon.com. I'm also fighting a bit of laryngitis, so please pardon my voice.

Today I am pleased to testify on behalf of the National Retail Federation, an association to which Amazon.com belongs. Thank you very much for inviting me to appear before your Committee.

Amazon.com is the Internet's leading retailer and the National Retail Federation is the world's largest retail trade association, with membership from all retail formats and distribution channels. NRF represents an industry with over 1.4 million U.S. retail establishments employing more than 20 million people.

Mr. NADLER. Do you have your mic on?

Mr. MISENER. Yes, sir, it is. You still can't hear me?

Mr. NADLER. No.

Mr. MISENER. How now? Can you hear me now? How is this? Okay. Good. Thank you. I'm sorry about that.

The NRF represents retail establishments that employ roughly one out of every five American workers.

Mr. Chairman, the National Retail Federation supports efforts to eliminate abusive marketing practices, including the use of fraudulent return addresses in correspondence. But before I address the details of our positions, Mr. Chairman, I thought it might be helpful for the Committee to hear how my company, Amazon.com, uses electronic mail to communicate with its customers.

Amazon.com strives to be Earth's most customer-centric company. To be so, we must provide our customers the very best shopping experience. Bombarding our customers with excessive or irrelevant e-mail obviously would not provide the best experience. On the other hand, Amazon.com also strives to be the place where consumers can find and discover anything that they may want to buy

online. E-mail is one way we help our customers discover products and services they otherwise would not know are available. The challenge, therefore, is to meet our customers' desire to discover products and services without bothering them with excessive or irrelevant e-mail.

Amazon.com's solution is to give our customers meaningful choice and personalization. Please allow me to explain.

At Amazon.com's Web site, the page entitled "Your Account" enables customers to choose the kinds of e-mail they want to receive from us. This choice is not just a binary yes/no decision to receive or not receive Amazon.com e-mails; rather, this is a user-friendly and highly flexible means for customers to personalize precisely what kinds of e-mail they want, if any.

For example, the Customer Communications Preferences feature allows our customers to choose what sort of general e-mails they would like to receive from us. My own settings tell Amazon.com to send me e-mails telling me about special offers and new products but not about research surveys.

And the "Amazon.com Delivers" feature allows customers to receive specifically tailored e-mail recommendations, reviews, and interviews on any of over 150 topic areas. Currently, I have my preferences set for Amazon.com to e-mail me periodically about history books and jazz CDs among other topics. I have chosen not to receive information, for example, about pop music and video games.

Mr. Chairman, as I noted earlier, the National Retail Federation supports efforts to eliminate abusive marketing practices. We believe, however, that legislation should be narrowly tailored to address such abuses without hindering legitimate business practices. Indeed, NRF believes that any Federal law should not burden online communications and commerce when such burdens are not imposed on the offline world; should not establish mechanisms that enable private lawsuits over mere unintentional transgressions; should not unnecessarily restrict the ability of companies and their affiliates to communicate and transact online with their customers; and should clearly preempt State laws so that national standards will develop.

Mr. Chairman, we have been asked to provide our specific views on two bills before the House, H.R. 718 and H.R. 1017. Both bills admirably seek to address abusive marketing.

H.R. 718 is an excellent effort to prohibit egregious e-mail practices. Unfortunately, we believe this bill goes too far. Specifically, we do not support the provisions in H.R. 718 that would give Internet service providers the right to set e-mail policies for other commercial entities. It would be virtually impossible for online retailers to know, much less comply with, the policies of thousands of ISPs across the country, and it seems anomalous at best for corporate entities to be setting policies with the force of law.

Moreover, many ISPs also have retail operations that compete with NRF member companies. Government must not establish a regime in which such ISPs can use their market power over e-mail to restrain consumer communications from their retail competitors.

Further, we also do not support H.R. 718's provisions that would, one, burden online communications and commerce when such burdens are not imposed in the offline world; two, foster unwarranted

lawsuits by establishing broad private rights of action and damages having little relation to harm; three, shift the burden of proof to defendants for inadvertent transgressions; four, inhibit consumer choice by impairing corporate affiliate relationships; and five, not clearly articulate Congress' intent to establish a regulatory ceiling and preempt inconsistent State law.

NRF favors the more measured approach taken in H.R. 1017. Our more limited concerns with this bill include the lack of provisions to preempt additional or inconsistent State laws.

Mr. Chairman, on behalf of Amazon.com and the National Retail Federation, let me thank you again for inviting us to testify. We support your Committee's efforts to curb abusive marketing practices and look forward to working with you on legislation that would narrowly target such practices while not restricting the marketing activities of legitimate businesses.

I welcome your questions.

[The prepared statement of Mr. Misener follows:]

PREPARED STATEMENT OF PAUL MISENER

Chairman Sensenbrenner, Mr. Conyers, and members of the Committee, my name is Paul Misener. I am Amazon.com's Vice President for Global Public Policy. Today I am pleased to testify on behalf of the National Retail Federation, an association to which Amazon.com belongs. Thank you for inviting me to appear before your Committee.

A pioneer in electronic commerce, Amazon.com opened its virtual doors in July 1995 and today is the Internet's leading retailer, with well over 30 million customers in more than 160 countries. The National Retail Federation is the world's largest retail trade association, with membership from all retail formats and distribution channels. NRF represents an industry with year 2000 sales of $3.1 trillion, and over 1.4 million U.S. retail establishments, employing more than 20 million people—about one out of every five American workers.

Mr. Chairman, the National Retail Federation supports efforts to eliminate abusive marketing practices, including the use of fraudulent return addresses in correspondence, and the transmission of inappropriate materials to children. But before I address the details of our positions, I thought it might be helpful for the Committee to hear how my company, Amazon.com, uses electronic mail to communicate with its customers.

Amazon.com strives to be Earth's most customer-centric company. To be so, we must provide our customers the very best shopping experience, which combines convenience, personalization, privacy, selection, savings, and other factors. Bombarding our customers with excessive or irrelevant e-mail obviously would not provide the best experience.

On the other hand, Amazon.com also strives to be the place where consumers can find and discover anything they might want to buy online. E-mail is one way we help our customers discover products and services they otherwise would not know are available. The challenge, therefore, is to meet our customers' desire to discover products and services, without bothering them with excessive or irrelevant e-mail.

Amazon.com's solution is to give our customers meaningful choice and personalization. Allow me to explain.

At Amazon.com's website, the page entitled, "Your Account"—which is directly accessible via a link on every page on the site—enables customers to choose the kinds of e-mail they want to receive from us. This choice is not just a binary, yes/no decision to receive or not receive Amazon.com e-mails beyond those related to transactions. Rather, this is a user-friendly and highly flexible means for customers to personalize precisely what kinds of additional e-mail they want, if any. There are five principal customization features:

- *Customer Communications Preferences* allow our customers to choose what sort of general e-mails they would like to receive from us, if any. As we say on this page, "We want to stay in touch, but only in ways that you find helpful." My own settings tell Amazon.com to send me e-mails telling me about special offers and new products, but not about research surveys.

- *"Amazon.com Delivers"* allows customers to receive specifically tailored e-mail recommendations, reviews, and interviews on any of over 150 topic areas. Currently, I have my preferences set for Amazon.com to e-mail me periodically about History books and Jazz CDs, among other topics. I have chosen not to receive information about, for example, pop music and video games.
- *"New for You"* offers our customers broad-based e-mail recommendations based on their purchase history and expressed preferences. I have this feature turned on and, thus, every week or so, I receive an e-mail with some purchase suggestions, such as an early Stephen Ambrose book or a Caphelon cooking pot that I have not already purchased.
- *Amazon.com Alerts* notifies customers about very specialized subjects. I have set my alerts to notify me of any new Rolling Stones CDs or Jan Karon books.
- *Special Occasion Reminder* sends our customers e-mail reminders about important events. I have mine arranged to send me e-mails one month in advance, and then one week in advance, of both Mother's Day and Father's Day.

Mr. Chairman, as I noted earlier, the National Retail Federation supports efforts to eliminate abusive marketing practices. We believe, however, that legislation should be narrowly tailored to address such abuses without hindering legitimate business practices. Indeed, NRF believes that any federal law:

- Should not burden online communications and commerce when such burdens are not imposed in the offline world;
- Should not establish mechanisms that enable private lawsuits over mere unintentional transgressions;
- Should not unnecessarily restrict the ability of companies and their affiliates to communicate and transact online with consumers; and
- Should clearly preempt state laws so that national standards will develop.

Mr. Chairman, we have been asked to provide our specific views on two bills before the House, H.R. 718 and H.R. 1017. I note first, however, that because Amazon.com sends marketing e-mail communications only to existing customers, we do not send "unsolicited commercial e-mail," as defined in these bills. That said, we still have serious reservations.

Both bills admirably seek to address abusive marketing. H.R. 718 makes a good effort to prohibit egregious e-mail practices. Unfortunately, we believe this bill goes too far to limit such practices and would inadvertently constrain legitimate business activities.

Specifically, we do not support the provisions in H.R. 718 that would give Internet service providers the right to set e-mail policies for other commercial entities. It would be virtually impossible for online retailers to know—much less comply with—the policies of thousands of ISPs across the country, and it seems anomalous at best for corporate entities to be setting policies with the force of law. Moreover, many ISPs also have retail operations that compete with NRF member companies. Government must not establish a regime in which such ISPs can use their market power over e-mail to restrain consumer communications from their retail competitors.

Further, we also do not support H.R. 718's provisions that would (1) burden online communications and commerce when such burdens are not imposed in the offline world, e.g., applying legal force to opt-out choices; (2) foster unwarranted lawsuits (in state and federal courts) by establishing broad private rights of action and damages having little relation to harm; (3) shift the burden of proof to defendants for inadvertent transgressions, especially when reputable companies have strong market incentives not to make such mistakes; (4) inhibit consumer choice by impairing corporate affiliate relationships; and (5) not clearly articulate Congress' intent to establish a regulatory ceiling and preempt inconsistent state law.

NRF favors the more measured approach taken in H.R. 1017. Our more limited concerns with this bill include the lack of provisions to preempt additional or inconsistent state laws.

Mr. Chairman, on behalf of Amazon.com and the National Retail Federation, let me thank you again for inviting us to testify. We support your Committee's efforts to curb abusive marketing practices and look forward to working with you on legislation that would narrowly target such practices while not restricting the marketing activities of legitimate businesses.

I welcome your questions.

Mr. GEKAS. Thank you.

And the panel's final witness, Wayne Crews.

STATEMENT OF WAYNE CREWS, DIRECTOR OF TECHNOLOGY STUDIES, CATO INSTITUTE

Mr. CREWS. Good morning, Mr. Chairman. My name is Wayne Crews, I'm Director of Technology—can you hear me? I'm Director of Technology Studies at the Cato Institute. I appreciate the opportunity to appear today.

In the debate over the outpouring of unsolicited bulk e-mail, or spam, it's important to remember that the optimal—a little closer? Yes, it's pushed. Can you hear me? It's important to remember that the optimal amount of unsolicited of unsolicited commercial e-mail isn't zero. Sometimes commercial e-mail is unsolicited, yet it's welcome. It resembles spam, but it's something else.

It's not apparent that businesses selling legal and legitimate products have any less right to use e-mail than anyone else. Unsolicited commercial mail is annoying, but it probably tops out as a vice rather than a crime except in specific instances when the seller is peddling fraudulent or phony merchandise or impersonates someone else in the message's header information, or perhaps a sender might be breaking a bulk mailing contract he has with an Internet service provider.

Besides, for targeting the most egregious spam, laws simply will not be enforceable. Perpetrators will go offshore and the law will simply create legal and regulatory hassles for mainstream companies even as they're increasingly embracing permission-based opt-in e-mail.

Estimates say spam accounts for anywhere from 10 percent to one-third of all e-mail; yet a recent study by the EC seems to indicate that spam has declined since its heyday between 1995 and 1998.

The basic instructions to Internet users still apply: read the fineprint; don't post your e-mail address; set up a junk e-mail account; don't respond to spam; join services like Removeyou.com that get you off of mailing lists. But increasingly, e-mail filtering is changing the default from today's everything comes in unless you say no to nothing comes in unless you say yes. This is particularly useful for children's accounts. Passwords and postage are emerging. One company called MailCircuit offers a Handshake system that totally blocks spam. When an e-mail comes to the recipient, the sender is sent a message by the system asking for a unique reply. Upon replying——

Mr. BARR. Excuse me. Mr. Chairman, could we ask the witness to not move the microphone away. It's hard to hear up here. If you could, keep it closer to your mouth so we can hear better.

Mr. CREWS. I'll try.

Mr. BARR. Thank you.

Mr. CREWS. Upon replying, they are added to the friends list.

Mr. BARR. Excuse me. You have to move the microphone closer to where you're speaking. It's hard to hear.

Mr. CREWS. Oh. It was just moved away from me. Okay.

Mr. BARR. No, you just moved it away. But try and—that way, we can hear you better.

Mr. CREWS. How's that? Okay.

Upon replying, they are added to the friends list. Since spam is automatized, this process stops it. And ISPs increasingly can shift

some of the costs of commercial e-mail back to the sender. ChooseYourMail charges advertisers a delivery fee which is shared with the ISP. That represents steps toward Internet postage and reducing load.

As the market moves toward solutions, a legislative cure can be worse than the disease. It's not entirely clear what ultimately will count as unsolicited or commercial e-mail, and the definitions may expand. Many informational newsletters link back to for-profit Web sites or contain imbedded ads and may not have received explicit permission to do so.

Other questions might include the status of political e-mailings, chain letters, and even forwarded jokes. Even the proliferation of pop-up ads on the Web in the wake of the failure of banner ads might become suspect in the aftermath of spam legislation. They are not e-mail, yet they're unsolicited and they're commercial.

Recall that at bottom, what's being proposed with spam legislation is the further regulation of business communications. It's risky because marketing will surely be required for proliferation of new services, like instant messaging and eventual wireless Web communications.

Legislation and a flurry of litigation should not come between what are complex relationships between companies, users and well over 5,000 ISPs. It's certainly appropriate for consumers and ISPs to effect commercial block-outs from spammers if they like, but ISPs are given Federal powers to decide what is spam and to unilaterally block it with good-faith immunity. They will undoubtedly block legitimate transactions consumers want that resembles spam or even block out smaller competing ISPs.

Also, financial remedies that exceed the actual harm done by the typical spam create incentives to go on spam hunts, looking for evil imbedded within every e-mail. That will keep many businesses out of Internet marketing all together.

There are also problems with establishing what will qualify as clear and conspicuous identification of spam. The intent seems to be to aid filters, but filtering technologies might be moving in other directions that could conflict.

Moreover, identifiers may fail to distinguish between XXX and, say, flower seeds. That needlessly stigmatizes unsolicited mail generally.

Finally, legislative bans on false return e-mail addresses as well as software capable of hiding such information have significant implications for free speech. Anonymous speech is a cornerstone of our republic. It just happens to be the case that the very technologies that facilitate spam can also protect individuals' identity. As strange as it may sound, spam and the use of spam-ware are means by which individuals create the anonymous leaflet of today.

Legislation that impedes anonymity and efforts to protect privacy would be taking away with one hand what the Government claims to be offering with the other in the privacy debate. So in trying to make life difficult for unsolicited mail, it's all too easy to make it difficult for solicited mail, legitimate commerce, emerging Internet communication methods and free speech.

I thank the Chairman for the opportunity to speak today.

[The prepared statement of Mr. Crews follows:]

PREPARED STATEMENT OF WAYNE CREWS

I would like to thank the committee for the invitation to discuss H.R. 718, the "Unsolicited Commercial Electronic Mail Act of 2001," introduced by Rep. Wilson, and H.R. 1017, the Anti-Spamming Act of 2001, introduced by Rep. Goodlatte. My name is Wayne Crews, and I am Director of Technology Studies at the Cato Institute.

OVERVIEW

In the heated debate over the outpouring of unsolicited bulk email, otherwise known as "spam," it's important to remember that not every unsolicited message is evil incarnate. Despite the hysteria, the optimal amount of unsolicited commercial email is not zero. Sometimes, commercial email is friendly or otherwise welcome—yet unsolicited.

Unsolicited commercial mail can be annoying, but it probably tops out as a vice rather than a crime except in rather specific instances, such as when the sender is peddling fraudulent or phony goods, or is impersonating someone else in the message's header information. Or perhaps a sender might be breaking a bulk-mailing contract he has made with an Internet Service Provider (ISP).

Laws supposedly designed to halt spam can do more harm than good, especially on an Internet that has yet to even hit on a successful marketing model. That is not to say that spam is the road to success: rather, legislation can have unintended consequences that otherwise harm commerce regardless of any impact on spam. Notably, a recent report expects eighty percent of San Francisco's remaining dot-coms will fail over the coming months. Banner ad click-thoughs are down, as is the money spent on such marketing. Unsolicited email may be an annoyance to many of us, but it's also a part of a larger picture in which companies and entrepreneurs are groping for ways to keep the Internet's services and options growing while making a profit.

It's not apparent that businesses that are selling legal and legitimate products have any less right to use email than anyone else. The Internet as it exists today is a public, open system and none can legitimately claim a right to exclude others and have the medium regulated on their behalf. However the government must protect citizens against force and fraud.

As this testimony argues, with solutions available and improving on the sender, ISP and user side and even hints that the spam problem is stabilizing, legislation is not wise, especially when it's considered that Internet communication itself is still a moving target; email is just one manifestation. Government should not use the novelty of the technology to justify intervention, especially when there's plenty of novelty to come. Conditions are changing every day. We don't have all the answers to the spam problem, and interference now can impede superior solutions to the dilemma that are emerging.

Besides, if the idea is to target the most annoying kinds of spam (LOSE WEIGHT FAST!; MAKE MONEY AT HOME!; XXX!), spam laws simply will not be enforceable. The bad guys will just go offshore, out of the reach of legislation, and the effect of a spam law will simply be to create mischief and regulatory hoops for mainstream companies who typically are not the greatest offenders. Legitmate companies will end up being targeted, with small business likely taking a lot of the brunt of the rules. As will be described, reputable companies are embracing opt-out—and often opt-in—policies of their own accord, and the phenomenon of "permission-based" email—which looks a lot like spam but is actually friendly fire, so to speak (with enviable click-through rates!) is on the rise.

Not all unsolicited commercial email is created equal. Nor are ISPs, who would be given legislative immunity for "good faith" efforts blocking and policing what they believe to be spam, even in the absence of customer consent, and in spite of what might otherwise have been negotiated privately. That will create confusion and a legislative nightmare. As noted, the market is already embracing permission-based emailing. It'll resemble spam to many ISPs for sure. Government should enforce private contracts regarding the delivery of such bulk mail, not dictate what the terms should be or allow one party to set the terms unilaterally.

Spam is just marketing. And there are different levels of spam "guilt." Spam is much less invasive than door-to-door selling, but we don't outlaw that. It's best to allow people to decide for themselves whether or not to entertain sales pitches. To the extent unsolicited communication is responsible for growth of the Internet and future communications options, hindering unsolicited mail could hamper access for many; a government created digital divide.

HOW BIG IS THE SPAM PROBLEM?

It certainly easy to see why spam is widely used by the unscrupulous. It's as easy to send a million emails as it is to send one. Some organizations like CAUSE find that spam accounts for about 10% of all email. Others have estimated it to be up to one-third of traffic. A recent and frequently cited study by the EC seems to indicate the problem isn't as big as it used to be, that "It is safe to say the spam phenomenon is now in decline," and that spam had its "heyday between 1995 and 1998."[1]

Spam clearly remains problem but it's one ripe for political mischief, as legislation proposed can be more problematic than spam itself. The debate thrives on loaded language, like the word "spam" itself, or in the description of marketers collecting emails as "harvesting." Some seem to detest Internet commerce as a worldview. But commerce and a commercialized Internet are critical to expanding online services, and access itself.

PRIVATE MEANS OF COPING WITH SPAM

It is worth reviewing some of the means of coping with spam in play today and on the horizon, because they help illustrate why legislation is unneeded and also highlight some of the problems that legislation can create by changing the rules midstream in an adapting marketplace.

Individuals' Tools to Attack Spam:

The basic instructions to Internet users still apply: Read the fine print before filling out forms; don't post your email address on Usenet posting or in chat rooms (even "munging" the address with an insert like NOSPAM won't protect an email for long[2]); try to avoid posting your email on your website. If need be, set up set up separate "junk" email account to use in online interactions. Finally, don't respond to spam, even to ask to be removed since this is often just a trick to assure that an email address is live. Instead, report and send the spam, either your ISP (which reports it to the spammer's ISP and which might help since most ISPs have "no spam" stipulations as part of their terms of service) or to a service like SpamCop.

There are other preemptive strikes that can be taken against unwanted mail. For example the Direct Marketing Association runs a list (at *http://www.e-mps.org/en/*) that Web surfers can visit and sign into to have their names removed from emailing lists. DMA member companies must abide: "All DMA members who wish to send unsolicited commercial e-mail must purge their e-mail lists of the individuals who have registered their e-mail address with e-[Mail Preference Service]." The service is even capable of blocking business-to-business email, not just consumer email.

Of course, legitimate businesses that are part of the DMA aren't the chief culprits. Most spam comes from companies that are by no means DMA members.

Beyond such pre-emptive moves, email filtering is a common tactic. Email filters can do a number of things: They can block by sending to a separate folder, or even delete emails altogether. They can block based on the sender's email (called "blacklisting"), or they can block based on words in the subject line or body. Online email services will often send email to a "bulk folder" if the email is not specifically addressed to you, but instead contains numerous addressees. The Hotmail email system, for example, makes spam easy to deal with, even though the system is quite susceptible to spam. Bulk mail goes into a special folder and is held there for two weeks and then automatically deleted. During that time, the user can open the folder and scan for legitimate mail that shouldn't have been sent there. Rather than reading any of the spam, a user need only note legitimate messages and click the "This is not bulk mail" button. Those messages will never be sent to the bulk bin again.

Increasingly, consumers can configure email to accept only some addresses (whitelisting). If consumers so choose, the default can increasingly evolve from today's "everything comes in unless you say 'no'" to "nothing comes in unless you say 'yes.'" Spamcop, for example, offers white lists or safe list filters, and these can be integrated with existing email accounts.[3]

---

[1] Maureen Sirhal, "Experts Struggle to Gauge Impact of 'Spam'," *National Journal's Technology Daily*, May 7, 2001, p. 4.

[2] See *http://www.antionline.com/features/jargon/spamblock.html*

[3] See, for example, David P. Hamilton, "You've Got Mail (You Don't Want)," *Wall Street Journal*, April 23, 2001, p. R 21.

Email tools for kids, such as that provided by email-connection.com, can be set up so that a child can send only to parent-approved recipients. Of course, problems of children's unattended use of the Internet go well beyond email. But even here there are solutions, and some have opted to join private networks altogether, such as eKids Internet and JuniorNet, where only members of the network itself, not the public Internet, participate—yet many of the features of the public Internet are duplicated through partnerships.

Aside from standard filtering, there are two main methods to block spam that could emerge, and already have to certain extent: passwords and postage. These tools are truly novel, removing even the argument for opt-out requirements. While filtering will zap some innocent emails, password and postage systems hold the promise of getting around that problem. One programmer offers a system for Unix users by which the sender gets an autorespond message containing a password when he sends an email, if he is not listed in the recipients "privileges database." He must then respond with the password in the message. The initial autorespond states, "Spam foiling in effect. My email filter autoresponder will return a required email password to users not yet in the privileges database."[4] That blocks spam, which is automatized.

One company called MailCircuit offers spam-free email services on what it calls its "Handshake System" to assure that "If you don't want it, you do not have to receive it—Our Mail Verification Program stops unwanted mail period."[5] By this unique method, when an email comes to a recipient, the sender is sent a message by the system asking for a unique response. If they reply, they are added to the friends list and future messages go through. Again, since spam is automatized, this process usually stops it.

As seen in the next section, techniques for ISPs to share "postage" with legitimate emailers is on the rise. There could also be mechanisms by which individuals are paid postage for receiving unsolicited mail (remindful of the often seen notice from sellers on eBay: "I accept PayPal."), and could waive the fee in certain cases, particularly if the system were to expand beyond commercial email to encompass all "unknown" emailings.[6] What an innovation it would be for individuals rather than the USPS to collect postage! As they are now starting to do with commercial mailers, ISPs may be able to help facilitate postage for individuals.

ISP Tools to Attack Spam:

Paralleling those used by consumers, various ISP filtering options are in play (XXX; For Immediate Release!; Earn Money Fast!). ISPs are also able to block bulk mails that come from dial up accounts, which many spammers employ in order to hide their header information.[7]

ISPs also block known spammer directories such as the MAPS "Realtime Blackhole List." Blacklisting can lead to problems, but it is a perfectly legitimate exercise of property rights. Disputes arise because some bulk mailers regard this as vigilante behavior. Legislation would likely have some impacts on this option; but it's by no means clear that legislation is a good substitute for it.

Increasingly there appear to be ways emerging for ISPs to shift some of the costs and inconvenience of spam back to the spammer. One option is for ISPs to develop ways to start charging for commercial emails. Already, a company called ChooseYourMail "charges advertisers a delivery fee which is shared with the ISP. This enables the ISP to defray rising mailserver costs and help keep monthly access fees low for their subscribers."[8] This fits in the vein of request marketing that is changing the commercial mailing industry. Such pay systems help shift the burden back where it needs to be and represent the first steps toward "postage" for commercial email.

ISPs and technology providers may need to "collude" to implement these systems on a wide scale, and they must be allowed to experiment.

---

[4] See *http://www.uwasa.fi/ts/info/spamfoil.html.*

[5] According to MailCircuit, "The way it works is simple: When you receive an unfamiliar message our Mail Verification Program checks to see if it is from a familiar address, if not it places the message on hold and sends a letter of introduction to the sender of the mail message asking them to reply in a unique way, if they reply as requested the senders message is allowed to pass through to your inbox and they are added to your list of Friends. If they do not reply to the message in a certain amount of user defined days then the message is deleted and the senders address is placed in your hostile list, thus not allowing that sender to send any email messages to your email account again." *http://www.mailcircuit.com/handshake.htm.*

[6] See, for example, Declan McCullagh, "Consuming Spam Mail," Contributors' Forum, The Library of Economics and Liberty, February 12, 2001.

[7] Hamilton, p. R 21.

[8] *http://www.mailcircuit.com/cym.htm.*

Notably, privately owned networks like eKids don't experience significant shift-the-burden problems with spam. Commercial email policies would be spelled out to ISPs who join (or establish) such networks. And the question of who bore the costs, rather than being answered by legislation from Washington, D.C., would be resolved by contract. Some networks may disallow "spam" altogether. Of those that permit it, some may require spammers to pay fees to account for the strain they place on networks. Or, network owners could require that member ISPs maintain certain capacity.

"Peer Pressure" On The Bulk Mail Industry Is Addressing Spam

Permission-based email will grow, and it represents a mounting source of peer pressure on the commercial mailing industry to make mail less intrusive over time. The market needs to adjust to these new realities. Indeed, there is a cottage industry devoted to spelling out the difference between permission email and spamming.[9] Permission mailing is praised widely:

> Permission email has been identified as the next generation of Internet marketing. Enjoying significant click-through rates over banner ads and other forms of online marketing, it has experienced phenomenal industry growth and has led Jupiter Communications to predict that commercial email marketing will become a $7.3 billion business by 2005. Forrester Research reports email use accounts for over 35% of all time spent on the Internet and estimates that 50% of consumers will be communicating via email by 2001. Clearly, permission email has emerged as one of the most powerful Internet marketing mediums ever.[10]

Third party stamps of approval are on the rise as bulk mailers seek to legitimize themselves. As Removeyou.com head Thomas Brock to told the *Wall Street Journal*, "We are not here to kill the spam industry. We are here to save it. We are simply forcing the bulk-mail industry to do the right thing."[11] His group maintains a list of people who don't want to be spammed. When individuals forward a spam to Removeyou, they contact the spammer and invite them to join Removeyou.

PROBLEMS WITH GOVERNMENT REGULATION OF SPAM

Given all such developments, it's apparent that the market is moving toward solutions for a spam problem that may in fact have stabilized. The prospects are good, and legislation intended to target specific areas can have unintended effects that bleed over and hinder superior private solutions as well as online commerce and consumer access to growing online services. It's not enough just to have an aversion to spam, and then feel that's all we need to know. The legislative cure can be worse than the disease. And it can bring a lot of expensive enforcement and litigation costs in the areas covered below, in the bargain. It's not even clear that all the voices are being heard in the debate. Most small businesses are not on the Internet, and it's not clear that they would have an easy time meeting legislative hurdles.

Ironically, in fact, it is the government's mandate that cell phones incorporate 911 location capability that swung the door open to spam in that particular arena, which promises to be a real hot-button spam issue in the near future. The mandate is costly, and the best way for manufacturers to pay for it is to allow marketers access to customers. Nonetheless, the industry's trade association, sensitive to outrage and its impact on profits, is adopting an "opt-in" approach of its own accord that would assure no customer gets pitched unless he permits it. It's noteworthy that even when government "subsidizes" unsolicited mail, peer pressure kicks in to control it.

Most legitimate vendors are increasingly offering opt-out. Laws will be unenforceable as far as the most offensive material goes, as these relocate overseas. Much spam already originates from Pacific rim nations, for example.[12]

What Will Count As Spam?

Spamming used to refer to individual behaviors, in which users would post the same message to numerous newsgroups.[13] Will the definition of what counts as commercial spam change? It is conceivable that, in the wide universe that is the

---

[9] See, for example, *http://www.digitrends.net/marketing/13640—12335.html*
[10] http://www.yesmail.com/learn/
[11] Hamilton, p. R 21.
[12] Noted in McCullagh, February 12, 2001.
[13] Noted in James W. Butler III and Andrew Flake, "The Effective Control of Unsolicited Commercial Email," U.S. Internet Industry Association, Internet Policy White Paper, p. 1.

Internet, spam could come to mean not just "unsolicited commercial" email but other things unsolicited.

It is not clear what ultimately will count as "unsolicited commercial" email. What if a reputable company sends mail unasked, but provides return address and removes your name when you ask? That presumably will remain legal in the the legislation at hand. But that could easily change on the floor. And certain activists who hope to profit from "consulting" on email issues are pushing aggressively for opt-in laws that would outlaw initial contacts altogether—a clear constitutional problem, as well as a death sentence for electronic commerce (particularly for small firms). Mandatory opt-in for mail has serious free speech implications. Nonetheless some consumer groups in this round of hearings are reiterating the call for a "federally mandated 'opt-in' policy on commercial email."[14] That pressure will not go away, and legislation now is the camel's nose under the tent.

As it stands, the legislation defines a "commercial electronic mail message" as one that "primarily advertises or promotes the commercial availability of a product or service for profit or invites the recipient to view content on an Internet web site that is operated for commercial purpose." This is quite a loose definition. What counts as "primarily"? And most newsletters, which often are not primarily commercial, include links back to websites that are often run for profit. What about electronic newsletters from actual media services, such as the Industry Standard, whose emails contain advertisements and links between stories? It is unfair to treat ads differently just because they happen to be part of a news service, and someone will inevitably point that fact out. The media business is for-profit, after all.

What about organizations that are primarily informational in nature, perhaps even labors of love, say a gardening website, that allows sponsors to insert brief advertisements in email newsletters. Spam legislation could have a detrimental effect on such electronic newsletters. Given the penalties proposed in the legislation at hand, there are clearly incentives to go on "spam hunts," looking for evil embedded within every email.

In such an environment regulation could lead to even more spam, somewhat disguised. Spam legislation could lead to our receiving "public service announcements," that happen to include an offer for a product somewhere down the line. Other questions regarding spam include; what is to be the status of political emailings? Some may get more junk mail from their congressman than they do from spammers. Rep. Goodlatte mentioned "chain letters" in his testimony.[15] Would those be subject to legislation? What about forwarded jokes? Gartner has referred to such potentially nuisance mail as "occupational spam." So the broadening of what gets classified as spam may not be that remote a possibility.

Super-Contractual Immunity for ISPs Will Distort Emerging Internet Markets

Legislation proposes to allow blocking as well fines by ISPs "that establish a policy." ISP spamming policies are fine, but they should be private contractual matters, not set from above in federal law. This amounts to an unwarranted federalization of contracts. Besides, there are now well over 5,000 ISPs in operation, which could create a patchwork nightmare as they implement federal policy.

If ISPs are given too much power to decide what is spam and to unilaterally block it, with immunity, they will inevitably block legitimate transactions that consumers want. Many legitimate communications can easily be confused with spam. ISPs are given "good faith" immunity in the bill, but that gives them too much ability to simply reject forwarding messages when it suits their purposes (and the Internet already suffers from a separate class of related traffic-sharing problems that must be worked through by voluntary means). The legislation gives ISPs financial incentives to block spam since doing so helps them relieve pressure on their networks.

Legislation should not come between what are complex relationships between companies, ISPs and users. Government can't just rubber-stamp random ISP blockages that they otherwise would need to negotiate to secure, and then on top of that facilitate the blocked party's potentially being sued. And it's certainly not clear that consumers would even want ISPs to block, even on good faith, since it takes away the assurance that permission-based emails would get delivered. Indeed, an amendment to the version of H.R. 718 marked up in the House Energy and Com-

[14] Maureen Sirhal, "Anti-Spam Bills Debated at Hearing, In Letters," National Journal's Technology Daily, April 26, 2001.

[15] "Statement of Congressman Bob Goodlatte, Senate Communications Subcommittee—Spamming Hearing," April 26, 2001.

merce Committee gives a sweeping opt-out right to ISPs, allegedly similar to the one given consumers.[16]

As noting in recent testimony in the Senate with regard to related legislation, small ISPs and customers could get cut off without their knowledge:

> [W]e are concerned about reports that ISPs, in their eagerness to help their subscribers avoid receiving unwanted UCEs, may block emails that subscribers not only want, but have specifically contracted to receive as part of an electronic business relationship . . . [The bill] does nothing to prevent this from happening, and does nt even require ISPs to give notice to consumers that they intend to block, or that they have blocked, the transmission of e-mail either in general or from particular senders.[17]

Some marketers may favor this policy, but it also seems quite possible that this legislation could disrupt permission-based email alternatives just as they are emerging. Will the ISP know, care, or bother to keep track of the fact that a consumer signed up for information from Sears, Gap or Tower Records offline? Will an ISP block mailings from Scott's Lawn updating consumers on when to throw fertilizer and grass seed? Or another example; if by breaking the shrinkwrap and lid on software, I accept the software's agreement and it "phones home," that should be acceptable as consent for emails I later receive. It is not legitimate for ISPs to intervene (with immunity) in any private emails unless authorized. Especially as friendly commercial email traffic rises, regulation could create more problems than solutions. It's vital that emails that consumers have contracted to receive are never blocked. Often, these could contain critical or time sensitive information (such as financial data). Similarly other kinds of innocent bulk email, like letters sent from trade associations to members, could be captured in error.

Opt-in or opt-out arrangements already made in the offline world that customers seek to transfer to the Internet are plainly put at risk. If permission was granted offline (or even online), how would ISP know? Under the proposed legislation, they can block it, and not even let the intended recipient know they're doing it. The bill in this way interferes with the emergence of permission based marketing since, according Jerry Ceresale of DMA, it "doesn't account for prior relationships." The legislation doesn't make clear how ISPs will be aware of and honor prior relationships, and there's no sense that it appreciates the fact that such arrangements will increasingly be made routinely, and there appear to be no real incentives for an ISP to investigate or keep track.

Clearly the existence of a "pre-existing" relationship like that specified in H.R. 718 may not be as straightforward to obtain as supposed. And it could lead to a scramble by companies otherwise indifferent to collect personal data hastily that they otherwise may not have bothered to obtain. (H.R. 718, for example, would take effect 90 days after enactment.) There's nothing necessarily wrong with accumulating such information, but it seems counter to the spirit allegedly motivating this legislative push.

A better solution all around may be for ISPs to look for ways to charge for commercial emails that are not on a white list. Legislation could have the effect of shifting wealth artificially and permanently toward ISPs, when the market might otherwise move us toward a system whereby consumers get paid instead for each unsolicited commercial mail they accept. The consumer gets nothing if the ISP gets to reduce traffic unilaterally—and could even be harmed. This is not to say the consumer is entitled to such payment—merely that such an outcome is a logical resolution of the spam problem and a regulatory "solution" could foreclose what could be a tremendous opportunity.

And again, ISPs are not all created equal, and some are even spam-friendly. Clearly not all favor the federal granting of power to ISPs. Indeed, the good faith clause could allow an ISP to block out a smaller competing ISPs who may be accused, legitimately or illegitimately, of being a source of spam.[18]

Identification Requirement Creates Problems

There are also potential problems with establishing what will qualify as "clear and conspicuous" identification of spam. Spam is already usually immediately obvious to the recipient, a kind of background noise.

---

[16] Noted in Adam S. Marlin, "Anti-Spam Bill Approved By Panel Over Industry Objections," *CQ Daily Monitor*, March 29, 2001, p. 6.

[17] Jeremiah S. Buckley (General Counsel, Electronic Financial Services Council), *Testimony Before the Senate Commerce Subcommittee on Communications*, April 26, 2001, p. 3.

[18] See, for example, the February 17, 2001 letter from the U.S. Internet Industry Association to Rep. Heather Wilson.

The intent here seems to be to aid spam filters, but that might not be the result. Filtering technologies could move in directions that would be impeded by mandatory identifier information. There may be possible conflicts with other species of identifiers that may emerge for solicited commercial mail. It could also interfere with "preview screen technology used by many consumers to rapidly screen messages and their content."[19] Besides, it would likely require legal counsel to certify for a business what counts as clear and conspicuous, leading small or reluctant businesses to avoid email altogether.

Identifiers could hurt small businesses as well by unfairly stigmatizing unsolicited mail generally; Identifiers would likely fail to distinguish between XXX and, say, home gym equipment or flower seeds. Identifiers could also cause confusion where messages are only partly commercial.

Potential Impacts on Emerging Messaging Technologies

The desktop is only one means of accessing the Internet, and it is entirely conceivable that over time it will decline significantly in importance relative to mobile, remote, and other devices (handhelds, cell phones, the Carrier/GE thermostat, automobiles, etc.)

These are struggling industries, and marketing will be required for these devices to proliferate, and legislation impeding commercial email could stall them. Strategy.com, for example, one of the most prominent outfits whose business plan included offering targeted services to consumers over remote devices, is facing severe hard times in a skeptical venture capital environment. Artificial restrictions on commercial email are the last thing companies like this need.

Recall that, at bottom, what's being proposed with spam legislation is the further regulation of communications; email just happens to be the format of the day. It's unclear what the impact of legislation would ultimately be on services like Instant Messaging (since the compact nature of IM may not lend itself to opt-out and other messages), the eventual wireless Web, peer-to-peer interactions, and services like Fax4Free.com or eFax. Even the adoption of pop-up ads on the Web would be suspect under spam legislation. After all, no one explicitly asks for these. Spam legislation limiting emailing could unintentionally promote these in the short term—and then lead to yet another backlash.

Pathway for Ill-Considered Privacy Legislation

One of the worries is that spam violates privacy. Spam is not primarily a privacy issue in the sense of personally identifiable information about you being known. The real spammers who use data robots to harvest emails off newsgroups and websites typically don't know anything about you. But if legislation imposes opt-in and/or opt-out policies, it paves the way toward a broader privacy bill that could have several negative effects.

Tools to secure Internet privacy are improving all the time, with new browser technologies that police web sites according to user preferences just one of many options available to consumers. There is no one level of privacy preferences that consumers share, and no government rule capable of acknowledging that fact.

Levels of privacy protection are properly competitive features, therefore markets are necessary to provide the mix people desire. All government needs to do is enforce privacy contracts when they are violated.

Privacy legislation, particularly the "opt-in" variety that spam legislation seems to admire, also violates free speech: yet if corporate free speech is a target, will media speech also be in the crosshairs? Privacy is a key value and people want it protected. Ultimately, the question is, who provides the best discipline: markets or politicians?

Unintended Impacts on the Right to Anonymity and Free Speech

Free speech for the sender

Spam is, at bottom, merely advertising. And business speech is still just speech. There is a problem in saying that we shall enjoy the freedom to contact or visit companies anytime we like, but they can't contact us. Even the opt-out requirement in the legislation can be problematic: does it preclude all future contact from a company by email—or just contact about a particular subject or offering? It's certainly fine for consumers to effect complete blackouts from companies if they like. But implementing this with federal legislation appears to be overly heavy handed, and better left to emerging contractual relationships.

[19] James W. Butler III and Andrew Flake, "The Effective Control of Unsolicited Commercial Email," U.S. Internet Industry Association, Internet Policy White Paper, p. 7.

Plus, the precedent set would be troublesome: Could advertising restrictions pop up elsewhere, such as on the new Web pop up ads?

Free speech for the public

Goodlatte's H.R. 1017 would ban using false email return addresses in commercial email, as well as software capable of hiding such information. The requirement that valid header information be featured has significant implications for free speech.

It can be very simple, thumbnail-sized code indeed that forges the "from" line of an email.[20] Individuals should retain the right to safeguard their anonymity by such means.[21] It just happens to be the case that the very techniques that facilitate spam can also protect individuals' identity. It is a mistake to criminalize bulk messaging software. Yet H.R. 1017 could make such simple but critical software illegal.

Right now the Internet, especially as we sit on the cusp of a revolution in peer-to-peer networking, is one of the only unregulated, open-to-all forms of communication we have. The benefits of leaving it alone, despite problems with some of the "communicators" that populate cyberspace, vastly outweigh the potential costs.

In a way, the spam debate helps illustrate that the underlying crucial Internet debate is really not the one about privacy that gets all the media attention these days. Rather, the real question is whether government will allow individuals to remain anonymous when they actually have the technological means to do so. As strange as it may sound, "spam" and the use of "spamware" are means by which individuals can maintain a cloak of anonymity. For example, Spam Mimic is a Website that disguises a message by making it look like spam so that "sniffers" might be more likely to ignore it.

At the very time the concern is to enhance privacy on the Internet, it's unwise to criminalize uses of software that hide headers, or source and routing information. Consumers may seek these for privacy reasons. Spam legislation that impedes anonymity and individuals' attempts to protect their privacy would be taking away with one hand what government proposes to give with the other. Here, the federal government would be artificially harming privacy, and setting the stage for unnecessary privacy regulations.

This is the kind of unintended consequence that can emerge when governments try to leapfrog the fact that we still have a lot of learning to do.

Loophole Mess

Loopholes in legislation, which could easily emerge from the give and take that will characterize a spam bill on the floor, can have unintended consequences. What if a loophole explicitly permits certain kinds of bulk mail that emerging market institutions would have chosen to shut out?

Unreasonable Penalties

Rep. Chris Cox (R-California) has argued the fines stipulated in the Wilson bill are in excess of the actual harm done by the typical spam. And it seems that $500-per remedies (up to a $50,000 maximum) would be off-putting to small businesses, and essentially keep many of them off the Internet as far as trying to conduct email marketing is concerned. Besides, if people are going to get $500 for every unwanted email, why go to work anymore(!). Surely it's not this much of a burden to delete emails or otherwise take steps not to receive most of them at all. The level of federally specified remedies appears to go too far and create a lot of potential for mischief. Email has always been a phenomenon operating on the principle that not everyone has to grant explicit permission in order to be contacted—which is arguably the essence of the Internet revolution. If that premise is going to be reversed, with penalties besides, it represents a fundamental change with plenty of opportunity for mischief.

Ironically could end up with lawyers specializing in offering to help individuals lay claim to the $500 remedies they are "entitled" to. Would these solicitations qualify as spam?

WHAT SHOULD GOVERNMENT DO?

The Federal Trade Commission already has power to "prosecute fraudulent or misleading commercial emails."[22] States likewise have powers to prosecute fraud.

---

[20] See, for example, Declan McCullagh, "Use a Spam, Go to Prison," Wired News, March 24, 2001.

[21] See for example Jonathan D. Wallace, *Nameless in Cyberspace: Anonymity on the Internet Cato Institute Briefing Paper*, (December 8, 1999)

[22] Noted in Sirhal, April 26, 2001.

Otherwise, it's better to let existing and emerging market tools address the spam problem because of harmful impacts of legislation on legitimate commercial emails, emerging Internet communications methods and free speech.

Government should not grant ISPs a top-down right to block, with immunity. While private efforts to block spam do not constitute state action, government-sanctioned blockage arguably crosses that line and violates free speech.

Granted, ISPs may be going overboard in some instances when blacklisting sites that spam or that offer software potentially usable for spamming. But at least blacklisters are subject to market pressures and discipline. In an ongoing case, New Zealand's largest ISP (Xtra) is seeking to have itself removed from the Open Relay Behavioural Modification System blacklist as an accused source of spam. The operator of the list, however, says, "What [Xtra] doesn't seem to understand is that the internet is a cooperative of privately owned networks . . . No one has the right to send e-mail anywhere. It is a privilege that is granted by the owners of those networks."[23] Email marketers should be held accountable to the contracts they make with ISPs.

The government can't stop spam. In the final analysis, the market will have to do the heavy lifting. Regulation now is likely to simply harm legitimate commerce. In trying to make life difficult for unsolicited mail, it is all to easy to make it difficult for solicited mail, too.

Mr. GEKAS. We thank the gentleman.

Let the record reflect the attendance now of the gentleman from North Carolina, Mr. Watt; the gentleman from North Carolina, Mr. Coble; the gentleman from Georgia, Mr. Barr; the gentleman from Indiana, Mr. Hostettler; the gentleman from Wisconsin, Mr. Green; in addition to those already in attendance.

We will begin the period of questions with an allotment of 5 minutes to the Chairman.

It seems that the witnesses do seem to come up with a common theme as to how all of this should be addressed. Mr. Lane and Mr. Lackritz both use language saying that the market forces ought to be the final arbiter, so to speak, of the problems that are visited by these bills. Mr. Crews actually says we ought to let market tools do the work of regulating what happens with e-mail, and Mr. Misener says that this self-policing cannot work that is provided in one of the bills, that the providers cannot set the policy. And what's the specific reason for that, as you see it?

Mr. MISENER. Mr. Chairman, there are several problems with having ISPs set the policies that have the force of law, and the first is exactly that—having a commercial entity take on the role of the legislature in setting what is lawful and what is not.

But we have specific concerns because many of these ISPs have their own retail operations, and it would be unfair for them in their role as gatekeeper on e-mail to determine what e-mail from other competing retailers can get through to our customers.

Mr. GEKAS. And Mr. Lackritz, you said that some of the language contained in the Wilson bill would inhibit, actually inhibit the growth of marketing on the Internet. Is that by reason of too many deterrents present in the Wilson language?

Mr. LACKRITZ. Well, it's both the deterrents, but also the additional obligations imposed on everybody that does—sends out e-mail on the Internet. I mean, our firms, as I said, conduct millions of e-mails a day, some of them, to the customers, and all the protections that are in the Wilson bill, plus all the legal obligations and liabilities that arise, would attend to all those communications

[23] Michael Foreman, "Xtra May Use Court to Get Off Blacklist," *The New Zealand Herald Online*, Tuesday, May 1, 2001. *http://www.nzherald.co.nz/storyprint.cfm?storyID=184372.*

potentially; plus all the enforcement—the extraordinary, overbearing enforcement mechanism that's contained would also create a deterrent to expanding e-mail use. In fact, it might cause people to move back from using e-mail because of all those requirements on there.

Mr. GEKAS. Mr. Lane, what is your take on allowing the market forces—what evidence do you believe exists that the market forces alone can handle most of these situations?

Mr. LANE. Well, in our testimony, as you know, we talked about going after the fraudulent e-mail, and market forces aren't going to take care of that. I think the incentive is on the other side for the bad actors.

Where we're talking about market force is in the use of commercial e-mail for legitimate marketing purposes, and as was mentioned earlier, an EU study showed that there is a decline because of the activities of consumers in retaliation to businesses who abuse the e-mail system in sending out a lot of e-mail. Amazon.com talks about how they use e-mail and they don't want to upset customers. So there is a reaction, a negative reaction, to businesses who send out tremendous amounts of spam and don't listen to their customers.

Now that customers have the ability to interact with businesses directly on line, they have the ability to say what they will accept and what they won't accept, and with a click of a button, they can go to a competitor who is willing to accept their needs.

Mr. GEKAS. Does the lady from New Mexico have a response to the prevailing theme here that the market forces can do what the lady wants to do in her legislation?

Ms. WILSON. Mr. Chairman, I wish that were true. If it were true, we wouldn't be having this hearing today and there wouldn't be a problem to be addressed.

With respect to the Internet service providers and the issue that the—that the retailers have raised, the reality is, under current law, Internet service providers can screen out e-mail from anyone because the Internet is not a common carrier, it is a private network, and they can do that under current law. So there is no change in this bill from what current law is, and—and we don't intend to change that part of the law. Internet service providers now can screen out anything coming over their network because it's their network and their business.

What will, I think, result from this bill is it will make it easier for things that are actually solicited e-mail and—and e-mail between a customer and a business that have a business relationship, for that to go on and not to have that be mistakenly filtered out.

Many of the things that are expressed as concerns about relationships between Amazon.com or the financial services industry and so forth have absolutely nothing to do with this bill because this bill is about unsolicited commercial e-mail, it is about marketing people that you don't have an existing business relationship with and never have opted into anything. And the fact is that it's as cheap to send one e-mail as it is to send a million. That's the problem. The cost has shifted to the consumer and the Internet service provider and consumers have absolutely no right to opt out even after they've had one bite of the apple. So the companies have

not taken care of it. The Internet service providers have that right under law now, and this bill doesn't change it.

Mr. GEKAS. The time of the Chair has expired.

The Chair recognizes the gentleman from California, Mr. Berman, for a period of 5 minutes.

Mr. BERMAN. Well, Ms. Wilson—thank you, Mr. Chairman—if current law gives them that right, then why do you feel a need to immunize the ISPs in your bill?

Ms. WILSON. The Internet service providers have the right to screen out any kind of e-mail. What this does is two things. First, it gives the consumer also the right to say no.

Mr. BERMAN. My question was why do the ISPs—why are the ISPs immunized for—from liability for making screen-out decisions under your bill if they have the unfettered right to do it now and are accountable for their decisions both in the marketplace and in the court?

Ms. WILSON. Because this bill gives a private right of action to a citizen. Right now, the complaints go to the——

Mr. BERMAN. A private right of action to a citizen for not screening out——

Ms. WILSON. Yes, not——

Mr. BERMAN. But you immunize them for—you immunize them for—from liability from a sender who didn't want their e-mails screened out.

Ms. WILSON. I can answer the question the—the bill gives a private right of action to consumers. Right now, consumers complain to America Online or whoever their Internet service provider is—"Why do you keep sending me this stuff?"—when it's not the Internet service provider, it's the company that's sending it. What this says is, if you end up getting an unsolicited commercial e-mail, it's not the ISPs fault that you're getting it.

Mr. BERMAN. But your immunity doesn't just speak to that issue. I think in the testimony from Mr. Lackritz, he points out you have a—you provide an unlimited immunity from liability from the, quote, spammers for decisions to screen out information that perhaps goes beyond what the law authorizes—your bill authorizes.

Well, I mean—I don't want to take all my time on that, but I just—I think there is an inconsistency between what you said and what—and what the bill does in the context of your immunity provision.

I would like to ask the supporters of the legislation, which I guess—well, from—on the intellectual property issue, I know there is concern in our Subcommittee about whether, under the bills now introduced, an e-mail notice sent by an intellectual property owner attempting to police his rights on the Internet could fall under the definition of spam if either of these bills is enacted into law. That's the concern, and the question is, would an exemption for legal notices make the anti-spam bills any less effective at stopping the type of spam that Ms. Wilson or Mr. Goodlatte are seeking to get at?

Mr. GOODLATTE. Would the gentleman yield?

Mr. BERMAN. I would be happy to.

Mr. GOODLATTE. As far as I'm concerned, I think that would be a fine provision to add to the bill. I mean, I think that Ms. Wilson——

Mr. NADLER. I can't hear you.

Mr. BERMAN. Mr. Goodlatte said that would be a fine provision to add to the bill, which maybe should be the last word on the subject, but——

Ms. WILSON. I have no objection to that, either. I think the bill—neither bill is intended to screen out that kind of communication, and if it makes it helpful to put it explicitly in there, that's—I have no objection.

Mr. BERMAN. And other than Mr. Crews, who might take the point of view the need for that amendment might show the problems of the bill, I'm wondering if any of the other witnesses have any objection to that amendment?

Mr. LANE. Well, if you have a narrower bill, you don't have to have that amendment because I doubt a copyright holder would be sending out misleading header information or fraudulent routing information. So you wouldn't have the need to have a provision in there dealing with sending information on violations of copyright.

Mr. BERMAN. But there is concern that under the bills in front of us now, the definition of spam may be vague enough that it could be interpreted to cover those kinds of notices.

Would you object to the amendment?

Mr. LANE. Oh, no, not at all. But it's only under one of the bills, not under both.

Mr. BERMAN. Pardon me?

Mr. LANE. That would only impact one bill, not both of them.

Mr. BERMAN. Ms. Wilson's bill?

Mr. LANE. Yes.

Mr. BERMAN. One last question here. I am pleased to—spammers can't survive without a plentiful supply of e-mail addresses. Businesses have sprung up to fulfill that need. They have a technology that intrudes on popular Web sites and automatically gathers thousands and thousands of e-mail addresses at a time. It's called e-mail harvesting. They then sell or rent those addresses to spammers. The result is someone who has posted a comment in a chat room or made a winning bid on an online auction gets on a spam list and is flooded with a lot of unwanted messages. Don't we need to do something about these e-mail address harvesters? Spam couldn't survive without them, but this bill doesn't address the subject of e-mail harvesting. Would an amendment to address harvesting make the anti-spam legislation any less effective at stopping spam? Would there be any problem with such an anti-harvesting amendment, to your way of thinking?

Mr. GEKAS. Without objection, the gentleman is granted an additional 30 seconds.

Mr. BERMAN. Thank you.

And I guess the three of you——

Mr. LANE. We would object to that.

Mr. BERMAN. You would.

Mr. LANE. Yes, we would. Strongly. We believe that this provision would make it for the first time illegal to collect information for purposes of contacting people, and that is part of the privacy

debate that we're having now on personally identifiable information, and how that information can be used for marketing purposes.

Also, it runs into our discussions that we have every Thursday at three between the two Committees on the database issue, and that may be the more appropriate place to address this type of issue.

Mr. BERMAN. Because you think—you believe that this conveys some kind of proprietary right in your list of names?

Mr. LANE. We believe so, yes.

Mr. BERMAN. And you think that's bad?

Mr. LANE. Well, under the *Feist* decision, a proprietary right over factual data is unconstitutional.

Mr. NADLER. Is what? What's that again? Say that again?

Mr. LANE. Under *Feist*, factual data—facts—the property right—or the copyright of facts is unconstitutional under *Feist*.

Mr. BERMAN. But what about the compilation of those facts?

Mr. LANE. As I mentioned, that's a debate that we're having every Thursday at three, so I don't want to pre-judge the outcome of that debate.

Mr. BERMAN. Well, I will renew the question at 3 o'clock.

Anyone else comment on the anti-harvesting amendment?

Mr. LACKRITZ. Congressman Berman, our Members are—we're looking at that provision now. I mean, my own instinct is that I would be very reticent to get into preventing harvesting of publicly available factual information because we have phone books out there right now and, you know, people get information out of phone books. It's one of the things that sometimes people don't like, and so we have ways of screening against, you know, unsolicited kinds of calls.

Mr. BERMAN. What about information that isn't publicly available?

Mr. LACKRITZ. Well, if it's not publicly—well, it depends, I guess, on what you mean by publicly available. I mean, if it's on the Internet——

Mr. BERMAN. If it's only available because some robot harvesting mechanism made it available in——

Mr. LACKRITZ. I guess that's the issue. Maybe that's the issue.

Mr. BERMAN. Okay. Thank you, Mr. Chairman.

Mr. GEKAS. The time of the gentleman has expired.

We will indulge in one more set of questions before we recess for the purpose of responding to the vote call on the floor. The Chair recognizes the gentleman from North Carolina for a period of 5 minutes, Mr. Coble.

Mr. COBLE. Thank you, Mr. Chairman.

I had four questions and Mr. Berman has asked two of them, so I will play with my other two.

Mr. Lackritz, let me ask you, H.R. 718 treats violations of commercial e-mail rules devised by Internet service providers as if they were violations of the Federal Trade Commission, quote, "trade regulation rule." Does this in effect allow the ISPs to write trade regulation rules, A, and B, do other private businesses have this power?

Mr. LACKRITZ. Thank you, Mr. Coble. That's a—the answer is, yes, this bill—that's exactly the point we're raising. Yes, this bill would allow Internet service providers to write rules and regula-

tions that have the force and effect of Federal trade regulations, and—and so as a result, that's—that's one of the problems.

No other business—this is unprecedented. No other business allows a private entity—no other policies and no other laws and no other regulations would allow a private business to write rules and regulations that would have the effect of law. I mean, that's obviously the business of the Congress and the administrative agencies and the courts.

Mr. COBLE. Let me ask you a second question, Mr. Lackritz. Does allowing the ISPs to in essence write trade regulation rules violate the principle of fairness and due process because there won't be an opportunity for notice and comment while the rules are being developed?

Mr. LACKRITZ. Absolutely. In fact, Mr.—Congressman Coble, that's the reason that you all enacted the Administrative Procedure Act, the APA, was to assure that every participant in a rulemaking had an ample opportunity to file notice and comment and get a fair hearing. By having a structure like this, you completely would eviscerate that and I would suspect it would be illegal or unconstitutional.

Mr. COBLE. I thank you, sir.

I thank the other panelists.

Mr. Chairman, I would yield back.

Mr. GEKAS. The gentleman yields back the balance of this time.

The Committee stands in recess until 10:55.

[Recess.]

Mr. GEKAS. The time of the recess having expired, the Committee will come to order. We will continue with questions from Members of the Committee.

The gentleman from Virginia, Mr. Scott, is recognized for 5 minutes.

Mr. SCOTT. Thank you, Mr. Chairman.

I guess my first question is to ask the witnesses a question about phone calls and mail, phone calls and faxes. Courts have differentiated them from mail because of their intrusive nature.

Where do e-mails fall on the scale? I mean, in faxes, you can prohibit all unsolicited faxes, you can prohibit a lot of phone calls, time of day, but mail is virtually unregulated. Where would e-mails fall on the scale?

Mr. LANE. Mr. Scott, we believe that would fall more on the mail side for marketing purposes because it doesn't bother you at a certain time of day, so to speak; it comes whenever you look at your e-mails.

In terms of the fax issue, unsolicited faxes, I remember when that bill was passed and thermal paper was being used on faxes, and I remember a miscalculation by those who were lobbying trying to stop that legislation by sending Members of Congress a lot of faxes and you had all these curly papers all over the place, which I think maybe went against them. So there was a difference there, especially for small businesses where some of them only had one phone line. We find that with our Members, when we would send them information to their fax machines and they would call us saying we're tying up their line with too much information.

So there is a difference e-mail is more linear, you can access it when it's convenient to you. So we look at it more on the mail side.

Mr. SCOTT. Yes, sir.

Mr. LACKRITZ. Yes, Mr. Scott, I would suggest—we would suggest that e-mail is far more like paper mail, frankly, than it is like either telephone calls or faxes. I mean, telephone calls are intrusive in the sense that, you know, they ring and you have to pick them up, fax—faxes tie up phone lines and, you know, snail mail basically just comes to your house and you dump it in the garbage can. E-mails, you know, it comes over the computer and you delete it, you know, if you don't want to read it.

Mr. SCOTT. Anybody else want to comment? Okay.

The—some—one of the bills designates anonymous e-mail as fraud, per se. How does that—anybody familiar with *ACLU* v. *Miller*, a 1997 case? Anybody want to comment on that?

If not, in terms of—in terms of the abuses, what is the FTC doing now to curb abuses in spam e-mail, if anything?

Mr. LANE. If you're interested, they actually testified on the Senate side on this issue, so their testimony is over there for—for more details for your staff on that question, and they have a—15 pages of what they do in this area.

Mr. SCOTT. In your opinion, are they doing enough or too much, not enough? Anybody want to comment?

Mr. CREWS. FTC and the States both have the—have the authority to go after fraudulent and deceptive——

and deceptive business practices, and that's what should be done in the—in the category of e-mail.

The risk is just saying that anonymous e-mail could—could be fraudulent because that's often not the case. I mean, as I had mentioned in the testimony, anonymous speech is a large part of our heritage. Thomas Paine signed Common Sense as an Englishman and the Federalist Papers were written under the name Publius. And so it has a long history and the Supreme Court has—has upheld that tradition.

So it's important in the legislation that you not penalize anonymous speech, but it's certainly appropriate for the—for enforcement against fraudulent and deceptive—you know, for example, if you're using—spoofing is using someone else's—setting up your bulk e-mail so that it looks as though it's coming from someone else who actually has—has an account, it actually looks like actual individuals, and, you know, of course, that's fraudulent. It also creates trademark problems that courts would have problems enforcing.

Mr. SCOTT. But just straight anonymous, how would that be any different than a caller ID block when someone is calling soliciting—unsolicited commercial phone call where the caller ID says that caller unknown or private number or whatever it says, how is that any different?

Mr. CREWS. Well, I'm—I'm no expert in the caller ID law there, but for the—for the e-mail purposes, the notion of being able to—it—e-mail in a way is our pamphlets of today, and—and caller ID is a different—different issue.

Mr. SCOTT. Does it bother anybody that there's no criminal intent standard in this that you can make a good-faith commercial—you meet somebody at a reception and offer to do business with

that person. Accordingly, this would be an unsolicited commercial e-mail. Should that be criminalized?

Mr. LACKRITZ. Mr. Scott, of course not. I mean, that's part of the problem. This is an incredibly over-broad, vague, over-reaching statute. I mean, the way that this tries to deal with a small problem on the Internet is to try and—it ends up fouling up the whole rest of the Internet. I guess the—the best way of describing it would be this is kind of like a fly buzzing around in the room, this—you know, the problem of spam, and do you want to go after the fly with a fly-swatter or do you want to sort of foul the whole room with a stink bomb to sort of clear it up? And this—that's why we favor a much more narrow focused kind of approach.

Mr. CREWS. The legislation doesn't outline that initial contact. That first commercial unsolicited mail is presumably okay, but it puts in—puts in place enforcement mechanisms and gives ISPs powers with immunity to block what they believe to be bulk e-mails that could cause some real problems down the road.

Mr. GEKAS. The time of the gentleman has expired.

Mr. Crews, was Publius Hamilton, Madison or Jay? Which one was——

Mr. CREWS. It was all three.

Mr. GEKAS. All three.

The gentleman from Texas, Mr. Smith, is recognized for 5 minutes.

Mr. SMITH OF TEXAS. Thank you, Mr. Chairman.

Mr. Lane, in your testimony, you made the legitimate point, I think, that legislation regulating the use of commercial e-mail must be narrowly targeted to focus on the clear abuses without interfering with the development of legitimate uses of electronic mail for marketing purposes. You also mentioned that legislation should center around combatting the sending of fraudulent and deceptive e-mail.

Mr. Lackritz, you made the same point, but added that Congressional action should carefully balance the legitimate commercial benefits of e-mail against the consumers need to exercise control over what he or she receives through a computer.

Mr. Misener, you said that Amazon.com really didn't get into unsolicited commercial e-mail, but you had some of the same concerns.

Mr. Crews, you mentioned that unsolicited commercial mail can be annoying, but it probably tops out as a vice rather than a crime. You pointed to some I thought very good examples of where individuals could use certain tools to combat spam, and you might have noticed that Mr. Sensenbrenner in his prepared remarks also suggested some ways that spam could be combatted without necessarily going to the extent that is proposed by Representative Wilson in her bill.

But I've really got two general questions. I was—I'm going to ask a question of Representative Wilson, but I will get to that in a minute.

For you all and from her point of view, and to touch a little bit more upon what Mr. Scott was just referring to, from a consumer's point of view, why is it that if a consumer can say to the telemarketing firm, take me off your list and don't solicit me anymore,

and under current laws, that solicitor is required to do so, why shouldn't consumers have the same right when it comes to e-mail, just say, I want to opt out, don't bother me anymore?

And maybe just Mr. Lane and Mr. Lackritz could answer that, and then I'll go into the next question.

Mr. LANE. The difference in—in having a broad bill is the provisions of what is required to be contained in that e-mail in terms of notice and choice and opt out and the mechanisms of opting out, which are incredibly burdensome. You don't have, even in the telemarketing scenario, a notice requirement; it's just law that says, if they ask, you must respond to that.

Our focus is to ensure that consumers have the ability, either through a reply button or through other mechanisms contained in the e-mail, to contact the legitimate sender of that e-mail so that they can request to be taken off.

The mechanisms of trying to do that, whatever the rules of the law—I mean rules of the road in terms of what are you actually opting out of—are you opting out of the affiliate, are you opting out of the corporate, and so forth—becomes incredibly complex. And so those issues need to be resolved before we have a situation where you don't know exactly what you're opting out of——

Mr. SMITH OF TEXAS. Right. Mr.——

Mr. LANE [continuing]. And the requirements of the business to do so.

Mr. SMITH OF TEXAS. Thank you.

Mr. Lackritz.

Mr. LACKRITZ. Well, I think that we sort of have a different kind of situation. I think your analogy to unsolicited telephone calls and unsolicited e-mails—first of all, the unsolicited telephone calls are vastly more intrusive than an unsolicited e-mail. Secondly, it's really—there's a very strong commercial incentive for legitimate businesses like our—our firms to not send unsolicited e-mail to people who don't want to receive it. I mean, the last thing in the world you get, I mean, as—as Amazon.com has talked about, you've got to be very careful in terms of marketing that you don't send things to people they don't want to receive, particularly on e-mail, because it's a different kind of medium.

In addition to that, the administrative complexities that, in fact, that Mr. Lane has discussed would also make it much more complicated and much more difficult in terms of affiliates and affiliates of other organizations and existing customers and non-customers and people that have given you permission and people that haven't given you permission. It creates—it would create a rather bit structure when already there is a strong incentive not to do that.

Mr. SMITH OF TEXAS. Right.

One of the reasons I may sponsor Mr. Goodlatte's bill is because I think we need to reach a better balance. In my remaining time, and Representative Wilson isn't here, I was going to ask her in what way she would be willing to change her legislation.

But my question now is, what suggestions do you have for her—and I'm sure her staff is present—as to how she might change her bill to address some of the concerns you might have about unduly and I'm sure intentionally restricting legitimate e-mail commerce? And I am sure she doesn't intend to do that.

Mr. LACKRITZ. We would urge her to become a co-sponsor of the bill that you and Congressman Goodlatte are——

Mr. SMITH OF TEXAS. No, no. That may be asking too much. But do you have specific areas, and maybe they're the three areas you mentioned in your testimony where you would like for her to go back and revisit her legislation; is that correct?

Mr. LACKRITZ. Yes.

Mr. SMITH OF TEXAS. Okay.

Lastly, and I'm going to sneak this in real quickly, because I'm Chairman of the Crime Subcommittee, I have a particular interest in cyber-crime, and also an interest in a subject that many of you all have mentioned in your testimony, and that is pornography.

Do you have any suggestions as to what we on the Crime Subcommittee might do to reduce the incidence of pornography?

Mr. GEKAS. Without objection, the gentleman is granted an additional 30 seconds to elicit an answer.

Mr. SMITH OF TEXAS. Thank you, Mr. Chairman.

Mr. LANE. Mr. Smith, we are willing to sit down with staff to—to work on that issue, because as we mentioned in our testimony, the sending of pornography does hurt legitimate e-mailers because it makes customers fearful of opening up an e-mail that they haven't asked for. So we are interested in working with you in that area.

Mr. SMITH OF TEXAS. Okay. Thank you, Mr. Chairman.

Mr. GEKAS. The time of the gentleman has expired.

The gentleman from New York, Mr. Weiner, is recognized for 5 minutes.

Mr. WEINER. Thank you, Mr. Chairman.

I think the correct issue analogy is not the intrusive phone call, but the intrusive or the excessive solicitation of third-class mail from a catalogue company or the like, and unlike the industry that you gentlemen represent—the issue was very similar. There was a point in time where it became very popular in the late '70's and early '80's where people were complaining about this, and the big retailers got together and formed something called the Direct Marketing Association, and now, with a phone call or a letter, you can have your name removed from the list. They have taken that proactive step. Need, or desire, even, for Congressional intervention receded.

It doesn't seem to me that the industry is taking similar steps in this area, unlike in the area of privacy, where there have been little indicias at the bottom of your—of your—of Web sites saying that we're part of this privacy consortium; security of credit cards, which was once a big concern—now there are industry-wide standards and little indicia that go at the bottom; filtering software, for example, that gets offered across different Web sites.

It seems to me this issue goes away tomorrow if the gentleman sitting here and others in the industry announce: You know what we're going to start doing? We're going to start having a single-click opt-out for consumers.

It is not as complicated as the witnesses—as you have made it sound. You know, you can opt out of, as I was mentioning to Mr. Lackritz during the break, you can opt out of getting J. Crew solici-

tations. That doesn't mean J. Crew can't send notice saying, you owe us 15 bucks for your last sweater.

I think it's relatively easy to do, and I think that for those of us who are Internet libertarians, it would show that you recognize that there is some concern, recognizing, of course, that probably the worst of the offenders of this spamming are not the so-called legitimate types that are—that are represented here.

I think that if—that if you all would say, we're going to start doing that, I think it's a relatively easy solution that will restore this body's confidence that you take the issue seriously and I think it would help consumers, too.

I have to tell you that a lot of the solicitations, the unsolicited solicitations that I get usually have a one-click at the bottom that just say "put unsubscribe" in the reply line or whatever it is and we'll take you off. Why not just do that kind of stuff, take that kind of step, from a—you know, from an industry perspective, because somewhere between the fraudulent e-mails, which obviously we're all against, or most of us are against, and the all unsolicited e-mails, I think there is a solution here the industry can tackle, and I'm not sure if any or all of you want to comment on that.

Mr. LANE. Congressman, I think, I believe, and I don't want to speak on behalf of another association, but I believe the DMA actually does that and has ground rules for the sending of e-mail, and I would be happy to contact them to have them contact you, and they may actually be here somewhere.

Mr. WEINER. Let me ask the gentleman from Amazon.

Mr. LANE. Those steps are already being taken.

Mr. WEINER. All right. Let me ask the representative from Amazon.

Are you a member of any industry-wide organization that helps people remove their name from a list in a global way or remove—I mean, just help manage this type of thing, or is that type of communication in violation of some antitrust provision that I'm not aware of? Is there any kind of industry-wide effort to make it easier for people to remove themselves from these lists?

Mr. MISENER. Mr. Weiner, thank you for your question.

Amazon.com is not a member of those kinds of associations, as you've asked; however, Amazon.com does not send unsolicited commercial e-mail as defined in either of these bills. The only e-mails we send are to our existing customers. We do not send it to customers—or to consumers, rather, who are not already Amazon.com customers.

Mr. WEINER. If I buy a book in March, you send me a solicitation in April for a similar type of book.

And by the way, I find most of these solicitations, and this might be an unpopular thing to say, usually helpful because, I mean, Amazon knows me better than my girlfriend does.

But the—— [Laughter.]

Mr. WEINER. But do I have a one-click at the bottom that I can say, do me a favor, I don't want to get another solicitation in June?

Mr. MISENER. Absolutely.

Mr. WEINER. And in your experience, do most of the major e-tailers do that kind of thing?

Mr. MISENER. Yes, that's correct.

Mr. WEINER. So—so in most of the definitions that have been bandied around about spam, it's not really an Amazon kind of thing; it would be—it would be someone trying to sell their individual book or something like that?

Mr. MISENER. Well, I can speak to my personal experience.

Mr. WEINER. Yes.

Mr. MISENER. I receive the same sorts of e-mails that everyone else does, and I simply delete them. It's not a long process. When we send out these unsolicited commercial e-mails from our perspective, they are not the same as defined in these bills, as I mentioned. We are sending them only to existing customers, and everyone has an opportunity to opt out. Our principal concerns with the way that H.R. 718 is constructed is that there could be liability attached to the inadvertent sending of an e-mail again to that same customer. Currently if a customer opts out of receiving further e-mails and we send them one, it may annoy them and they may not want to buy anything from us again, which——

Mr. WEINER. Right.

Mr. MISENER [continuing]. Is something that we take to heart, but if we inadvertently do so, to have FTC regulatory liability associated with that action——

Mr. WEINER. And I—and I share that concern. What I'm trying to find is a way to kind of find some kind of middle voluntary way that consumers, you know, can have—I mean, I think much more importantly than having Congress weigh in on the side of consumers here, if the industry kind of gets together and says, we're going to have some unified standards——

Mr. GEKAS. Would the gentleman yield? Would the gentleman yield?

Mr. WEINER. Certainly, Mr. Chairman.

Mr. GEKAS. In line with that, we understand that there is this e-mail preference service. Doesn't that answer some of the questions raised by the gentleman from New York? Maybe somebody could fill in with that.

Mr. CREWS. There's a—I would just add to this that there is—there is coming to bear on the bulk-mailing industry a lot of third-party pressure to kind of clean up its act. The DMA example is one. If you're a member of the Direct Marketing Association and someone asks to be taken off, you have to take them off. But there is another outfit out there, too, called Removeyou.com that consumers can send spam to. Removeyou then goes to that spammer, basically harasses them and tries to get them to clean up their act and join Removeyou and remove customers who ask to be taken off.

So there's that kind of third-pressure being brought to bear, and companies are offering—you know, in response to that, the whole request marketing phenomena is emerging now. There's Yesmail.com and lots of others——

Mr. WEINER. Well, I think——

Mr. CREWS [continuing]. That are trying to pressure——

Mr. WEINER. I think, just to conclude, Mr. Chairman, maybe we can reach a point of mutually assured destruction that if you get spammed, you have the ability to send a million letters back to the spammer and we'll just—anyway, thank you, Mr. Chairman.

Mr. CREWS. No, that wouldn't help.

Mr. GEKAS. The time of the gentleman has expired. We now yield 5 minutes to the gentleman from Virginia, Mr. Goodlatte.

Mr. GOODLATTE. Thank you, Mr. Chairman. Gentlemen, I appreciate all of your kind words about our efforts here. The reality, however, is that while my bill is significantly different than Ms. Wilson's, I am a supporter of Ms. Wilson's general efforts and voted for her bill, as did virtually everybody in this room who served in the last Congress last year. Her bill has passed the Commerce Committee. This Committee has limited time and limited jurisdiction in which to act on making improvements. So I think that all roads here lead through Ms. Wilson's ofFeist and we've got to work out a way to try to accommodate your concerns while recognizing that something is going to be done in this area, and soon.

So first of all, I would like you to comment in general about the private right of action issue from a couple of standpoints. The first—the first is, what kind of precedent is there for that? I think that's the major bone of contention here. There are other things that we can change and I think she would be amenable to talking about changing, but she indicated today a strong support for her private cause of action.

In the—in the area of postal mail, in the area of faxes, in the area of unsolicited telephone calls, in the area of unsolicited—people knocking on your door, what kind of private rights of action exist in those areas, at either the State or the Federal level, and what has been the experience with them if they do exist in any of those areas?

Mr. Lackritz, you have anything to say about that?

Mr. LACKRITZ. I was afraid you were going to ask me that question and I was just trying to get some more facts.

First of all, the whole concept of private rights of action is very rare and very unusual in the law. Secondly, one of the biggest problems that businesses faced over the last number of years has been the incredible proliferation of lawsuits and in terms of dealing with a phenomenon like this, what we've come to understand is that technology is a vastly more effective means of dealing with a lot of these issues than a series of rights, obligations and lawsuits.

Mr. GOODLATTE. I agree with everything that has been said about using technology to block these things out. I will also tell you that the technology doesn't completely work. I've had my own frustrations with trying to stop unsolicited commercial e-mail and unsolicited commercial faxes as well, in fact. I'm a participant in a situation right now where the FTC has fined an entity of more than a million dollars for sending repeated unsolicited commercial faxes. I don't know of anything I can do personally about that, but I'm wondering if you are aware of anything in any of those areas where there is a law that allows private cause of action, and, if so, what has been your experience with that? Has that caused too much litigation, too much abuse, too many frivolous private causes of action?

Mr. LACKRITZ. Under section—I mean, first of all, almost every—all 50 States have many FTC acts that prohibit fraudulent or deceptive practices.

Mr. GOODLATTE. Do they allow the——

Mr. LACKRITZ. In some cases——

Mr. GOODLATTE [continuing]. People to——

Mr. LACKRITZ. In some cases, you can also bring a private right of action under some of those statutes, but I don't have a catalogue of which ones they are and which ones they're not, and as a result, I can't give you the facts that you have asked and obviously deserve. I can get that back to you before the record closes.

Mr. GOODLATTE. Great.

Yes, Mr. Crews.

Mr. CREWS. It is the case that in California, under California law, that—that a person who had received spam from Cosmo.com, which just shut down, as you probably know, sued in small claims court and prevailed. Didn't do much good since Cosmo was out of business, but——

Mr. GOODLATTE. Just under general California statutes?

Mr. CREWS. Yes.

Mr. GOODLATTE. Not a specific——

Mr. CREWS. Right.

Mr. GOODLATTE [continuing]. Anti-spam statute.

Mr. CREWS. So there's that ability, and she—and, of course, she got a high profile for taking that case.

But the cases like that can become nuisances because one way of looking at her particular case was she got the spam, she complained, and the company made a stupid mistake of sending her back an e-mail acknowledging that they had gotten her notice and wanted her—and that she would be cut off, so that is what triggered her and made her sue.

Mr. GOODLATTE. Before my time expires, let me ask you all, is there a way to—to take this private right of action that she has in her legislation and modify it so that it only applies to egregious cases, cases involving obscenity, cases involving gross numbers of repeat violations? Is there a way to—to give the truly frustrated individual some private cause of action without causing the kinds of misery that I agree that you described could ensue with simply one or two unsolicited commercial e-mails resulting in—in litigation that your industries would have to defend.

Mr. LANE. Congressman, you can't say private right of action without the Chamber commenting. It's part of our history. Obviously we have strong concerns about having the precedent as well as the proliferation of litigation that is occurring to American businesses across the board, and we don't want to add to that.

We saw it with the cellular telephone industry and the lawyer out of Baltimore suing on proposed——

Mr. GOODLATTE. But the reality is that you may very well have that unless we find a common ground.

Mr. LANE. You may, but you don't want to give them the exact law to be able to do that when there are other remedies available.

Mr. GOODLATTE. That law is heading down the track very fast right at you with a bill that's about to go to the floor of the House of Representatives that passed the last Congress with an overwhelming majority. She said 427 to 1 or something. Maybe it won't be quite that overwhelming, but it's likely to pass.

Is there something that we have that we can do that would be acceptable to you that would make it far fewer of those types of lawsuits that you confront?

Mr. GEKAS. The gentleman's time——

Mr. GOODLATTE. Am I extended for another——

Mr. LACKRITZ. Mr. Chairman, can I respond?

Mr. GOODLATTE. I would ask unanimous consent——

Mr. GEKAS. Extended 1 minute to allow answers, yes.

Mr. GOODLATTE. Thank you.

Mr. LACKRITZ. Could I respond?

Mr. Goodlatte, I think that your question about trying to figure out a way to narrow that funnel in private right of actions is a great idea, and we—and we certainly favor that, but it's only one part of the problem with the liability provisions of this bill.

The bill also contains a strict liability standard. It doesn't—you know, and that in and of itself—and one with liquidated damages, along with a minimum of 5—I think it's $500 per violation per consumer. I mean, this is—you might look at this as sort of the trial lawyers' relief act in some respects——

Mr. GOODLATTE. And I'm sympathetic to your concern about that, and I want to help in that regard, but I'd also suggest that if we need to accommodate a private right of action, we ought to be looking to find ways to narrow it considerably.

Mr. LANE. Congressman, regarding your comments on the Commerce Committee, they have made great strides. They've moved it dramatically and they have been working and trying to improve the bills. So we agree with you in terms of working with the Committee and trying to narrow this down, but, it's still the problem of a private right of action, and I don't know if language can be drafted that would be satisfactory, but we're willing to look at anything.

Mr. GOODLATTE. I think Mr. Misener wanted to say something.

Mr. MISENER. Yes, Mr. Goodlatte. Thank you.

I do appreciate your—your admonition to us that we ought to be engaged on this particular issue and offer solutions as opposed to just completely pushing back.

There are some avenues, and you've suggested a few, extraordinarily egregious behavior, perhaps the linking with pornography, things that the companies represented by the entities at this table certainly do not subscribe to. So absolutely so and we will work with you and your staff.

Mr. GOODLATTE. Thank you, Mr. Chairman.

Mr. GEKAS. The time of the gentleman has expired.

The lady from California, Ms. Lofgren, is recognized for 5 minutes.

Ms. LOFGREN. Thank you, Mr. Chairman.

I guess I've been thinking about the vote last year and really been rethinking our reflexive yes votes on that. It was on the suspension calendar, as I recall. I don't recall that we had extensive analysis or hearings, and I think many Members, as we do with suspension votes, just thought it was motherhood and apple pie and cast a yes vote, and I—that's why I think this hearing is especially important.

You know, I was thinking, 5 years ago, I used to get complaints a lot from my constituents about spam, but I don't think I've gotten an e-mail complaining about spam for several years, and I think

it's because people know how to deal with it now. We have a delete button.

This morning, as a matter of fact, I got an unsolicited e-mail, too, actually, from Wolf Cameras, which I've now blocked, so I'm not going to be getting any more unsolicited e-mails from Wolf Camera, and I think the ability to just block what you don't want has really resolved much of the anxiety that people had. So I guess I'm questioning whether this is an appropriate area for legislation at all.

One question I guess I have is to the extent that there are fraudulent solicitations, wouldn't those fraudulent solicitations be proscribed under existing fraud statutes? Do we need another statute to fight fraud in addition to the anti-fraud laws of the States and the Federal Government?

Mr. LACKRITZ. No. Ms. Lofgren, you're absolutely right. Section 5 of the FTC Act already proscribes fraud and fraudulent or deceptive acts, and a fraudulent e-mail certainly would come under the aegis of section 5 there.

Ms. LOFGREN. Let me ask you. The one thing I think that is disturbing to people is unsolicited e-mail that is lewd coming to adults, and especially to kids. I mean, it's very upsetting to people. It may not be something that violates an obscenity statute, but it's not appropriate for children and it's—it's yucky and you don't want your kids being exposed to that.

Is there existing law that would protect or proscribe that particular form of spam?

Mr. LACKRITZ. Not that I'm aware of. There is—there is that—an ability under the FCC law to stop the transmission of obscene material, but that's because that governs common carriers, and currently the ISPs are not deemed to be common carriers, and so they're beyond the reach of the FCC at this point.

Ms. LOFGREN. I guess the final question I have is, looking at both bills, the ability—the wisdom of involving the FTC in a more vigorous regulatory role. I mean, is that what we want to do, number one? And number two, in terms of criminal law enforcements, you know, I—I look at what U.S. Attorneys are doing around the country, and we can't get filings on egregious copyright violations on the laws that we've already passed. I'm just sort of wondering where in the whole panoply of our arsenal would spam fit relative to the prosecution for other activities, where should this fit. Anyone who wants to answer that.

Mr. LANE. In terms of, the copyright, obviously there needs to be more resources put into both the Department of Justice and the FTC to go after those who are violating copyright law. That's a priority for us at the Chamber.

In terms of the resources to go after fraud and abuse and misleading header information at the FTC, we'd have to look at the balancing—of were resources available, and do we need to increase that to build consumer confidence on the use of—or to look at commercial e-mail, because that is what this is all about, it's about consumer trust, and even just having the law on the books may help stem the tide of bad e-mail. That helps legitimate businesses in using this incredible new tool.

Ms. LOFGREN. I guess the final thing I'd like to say is that if we—and if you have some suggestions on this, I would be eager to

get them. In the case of an unsolicited e-mail that is—has sexual content but is not so disgusting that it would violate an obscenity statute, is there a narrow remedy that you could recommend when such material was received by individuals who are minors? Do you have some ideas or suggestions on that? Either in addition to what's in either one of these bills or in lieu of these bills.

Mr. MISENER. Ms. Lofgren, I don't have any ideas right—for you right now. We certainly would be willing to work on that because none of the companies represented by——

Ms. LOFGREN. Certainly not.

Mr. MISENER [continuing]. These groups up here obviously support any of that kind of activity and so would be happy to try to draw that kind of a line.

Mr. LACKRITZ. Ms. Lofgren, I can just relate back to in the telecommunications are, there was a big focus in the mid '80's on the whole issue of dial-a-porn.

Ms. LOFGREN. Right.

Mr. LACKRITZ. And I think this—this is a similar kind of issue, and my instincts would say that if we go back to some of the questions surrounding dial-a-porn and how to deal with that, they might be—might give us some constructive ways of dealing with this issue, too.

Mr. LANE. And there's also laws on the books dealing with the sending of pornography or obscene material through the mail that may also supply——

Ms. LOFGREN. And I understand that, but the problem is what is—you know, we all believe in the First Amendment. What's going to be obscene under the First Amendment is a different stand than what I think is really appropriate for my children to receive unsolicited. And if you have further ideas on that, I would be very interested in it, but absent that, I'm not at all sure we should be doing anything in this arena.

Mr. CREWS. It might be useful to look at——

Mr. GEKAS. The lady is extended an additional 30 seconds.

Ms. LOFGREN. Thank you, Mr. Chairman.

Mr. CREWS. It may be useful to look, if you have further hearings on this issue, for example, at some of these new technologies, because there are e-mail accounts now that will only—for a child, and for a child on the Internet, the problems go way beyond just e-mail, they're——

Ms. LOFGREN. Good luck on getting your 16-year-old to comply with that.

Mr. CREWS. That's right. They're going to run into these problems everywhere.

But as far as e-mail is concerned, parents can set up with certain companies that will only accept e-mails from particular addresses, and separate from that, there is new technologies called Handshake technologies that virtually stop every spam, because any e-mail that comes in gets an auto-responder from the service provider, it goes back, and the person who sent the e-mail has to stick in the subject line a password that you sent, then it comes through and it can come down into your account. And the reason that stops spam is because spam is automated, and that kills it right there.

Ms. LOFGREN. Thank you, Mr. Chairman.

Mr. GEKAS. The time of the lady has expired.

The gentleman from Georgia, Mr. Barr, is recognized for 5 minutes.

Mr. BARR. Thank you, Mr. Chairman.

We have before us in H.R. 718 a piece of legislation that is as broad and heavyhanded and litigation-friendly as any that trial lawyers could have dreamed up, and, as Mr. Goodlatte indicated, here we are with that being sort of the piece of legislation that has a head of steam behind it, and we're going to have to work awfully hard to derail it, which I think we ought to.

I think it's going to take more than just sort of an academic exercise to come up with some alternative—alternatives. I would suggest a full court press initiated very, very quickly.

It's unfortunate that we've got to this point. I think all sides to this were sort of caught asleep at the switch last year when this thing—when this thing was slipped through under suspension of the rules. Hopefully we won't be faced with that tactical or procedural situation again and we can all take a closer look at it, because I think there are some—some terrible precedent-setting provisions in H.R. 718.

As I understand it, with the exception possibly of Mr. Crews, you are all in support of H.R. 1017. Is that correct?

Mr. MISENER. With some minor modifications which I mentioned in my testimony.

Mr. BARR. Okay.

And Mr. Crews, I think your position probably would be that neither piece of legislation is essential; there are some other alternatives short of enacting new criminal and civil liability——

Mr. CREWS. That's right.

Mr. BARR [continuing]. Statutes that could address this problem.

Mr. CREWS. That there are some alternatives and you may get some unintended effects—just sending a lot of this mess overseas and things of that sort. So you really end up with the penalties just hurting legitimate companies that are starting to embrace this—these new marketing procedures.

Mr. BARR. With regard to the other—you all's organizations and memberships, are your members engaged in this? Are they contacting Members of Congress, particularly key Committee and Subcommittee and leadership Members?

Mr. LANE. I wouldn't be allowed to be up here if my members weren't contacting us to be up here to testify on our positions, and they are heavily engaged.

Mr. LACKRITZ. Mr. Barr, our members are now aware and active with respect to this legislation. I think you're right, last year I think we were all a little bit asleep at the switch in the sense that we—it was toward the end of the session, and I don't think anybody thought that the bill had a chance of getting enacted into law. Now that we've had a chance to reflect on it and look at some of the provisions and their implications, I think we've become engaged and active and we are very focused on trying to slow this train down.

Mr. BARR. I appreciate that and——

Mr. LANE. Mr. Barr?

Mr. BARR. Yes?

Mr. LANE. I would just say, I want to clarify that. We haven't endorsed either bill at this point. We're looking at it and we think that we can reach some compromise in trying to bring all the parts together, as Mr. Goodlatte articulated earlier.

Mr. BARR. But your organization does not support H.R. 718?

Mr. LANE. We stated in our letter to the Commerce Committee that we had some concerns and we would like to see some changes to it. We think we can make some——

Mr. BARR. See, that's the kind of thing that I'm not sure will get you where you want to be if you just—if you're afraid to come forward and say, we do not support H.R. 718. That's what our people need to hear, that this is bad legislation, it sets very bad precedent that could come back to haunt you and the American consumers and businesses in a lot of different areas. You start monkeying around with exempting certain types of proceedings from the—from the APA, you start opening the floodgates for private causes of action very vaguely defined but very broadly worded.

I think—I think you all need to be a little bit bolder, perhaps, in—I certainly can't tell you how to run your organizations, but if the attitude is, well, you know, we're not going to say we're opposed to H.R. 1017, we'd like to see a few changes, probably what you'll get is H.R. 718 with a few minor changes, and I'm not quite sure that that will get you where we need to be. So I'd—I'd take off the gloves. That would be my suggestion. No surprise there, I'm sure.

Thank you.

Mr. GEKAS. The time of the gentleman is yielded back.

The Chair now recognizes the gentleman from North Carolina, Mr. Watt, for 5 minutes.

Mr. WATT. Thank you, Mr. Chairman. I try to use these opportunities as—hearing as an opportunity to learn more about the bills, and this one has certainly been helpful, although I have been kind of in and out.

I'm not sure that I come down quite where Mr. Barr comes down on this, however; probably a little bit closer to Mr. Goodlatte. It does seem to me that if you are taking substantial steps to reduce spam, which it sounds like the industry is, that the people who are engaging in it will be ultimately the worst actors, not people who really have the best of intention, and that ultimately, it's not necessarily a good public policy to leave all enforcement activities to big brother government. So one could make the argument that a minimalist approach that gives individuals a private cause of action to enforce their rights against egregious conduct is a much, much better and wiser public policy course than criminalizing more things which the Government really doesn't have the resources to enforce.

And so I'm not sure where I come down, I'm not taking a position on this, but I was surprised to hear Mr. Lackritz' comment that somehow private causes of action to enforce what are essentially rights that we recognize for people not to be interfered with, receive something, is something that's revolutionary. That is not revolutionary; that is—that's the way we—we enforce our rights in this country. And in the absence of those private causes of action, I'm not sure—I don't believe that the Government will just con-

tinue to grow and grow and grow and we'll get more and more and more criminal laws on the—on the books, which, in a commercial context, really I don't think is the appropriate way to deal with this.

Now, let me give you kind of a backdrop for where I come down on this. I mean, I just came back from Brazil and met with a bunch of Afro-Brazilian members of their legislature, and we got into a discussion about the substantial disparities in education, in income, in job opportunities, between Afro-Brazilians and other Brazilians. And as I probed and continued to probe, they finally told me that there is no private cause of action for racial discrimination in Brazil. It is criminal, they said, it is a criminal law, they said, against racial discrimination in employment, and, of course, the government never considers that criminal, they never have brought a criminal action against anybody, and probably rightfully so. I'm not sure that racial attitudes or racial motivations are criminal. We have set up a set of standards that we think are the norm in our country and we leave it to private individuals to enforce those standards.

Now, the question then becomes, what is the appropriate standard in this context? And I don't think—I'm kind of close to Mr. Goodlatte, I think.

Could I have 30 additional seconds?

Mr. GEKAS. The gentleman is accorded an extra 30 minutes—30 seconds.

Mr. WATT. I think you are doing yourself a disservice to stick your head in the sand and say we oppose any private cause of action, without some kind of constructive response on this issue.

Mr. LACKRITZ. Could I respond, Mr. Watt?

Mr. WATT. Yes, sir.

Mr. LACKRITZ. Mr. Chairman, could I have a couple minutes—seconds to respond?

I think the point that you're raising is a very valid point, but I'd just draw your attention, in this legislation, to the scheme that's set up. The scheme that's set up here is not Congress enacting rights to protect individuals; the scheme that's set up is Congress giving Internet service providers the right on their own to set rules and regulations that have the force of law and then provide a private right of action.

Mr. WATT. I understand that and I have problems with that.

Mr. LACKRITZ. Okay. But then the other piece of that, Mr. Watt, is that in addition to the private right of actions, in this case, we also have enforcement authority to the FTC and also to 50 State attorney's general that also have enforcement authority. So what we——

Mr. WATT. You may find in my comments a minimalist approach on that, too, but you—you know, the letter you all sent out that's signed by all these organizations that—that signed off on it say you oppose private cause of action, but you don't have any—and then you say, "We agree that a strong enforcement provision is needed to deter illegal and unwanted spamming." Well, what is it? If it's not a private cause of action, if it's not FCC—FTC, if it's not criminal, which I don't think is necessarily appropriate, what is the—what is the enforcement mechanism?

Mr. LACKRITZ. That's where we come back to dealing—to agreeing with you and Congressman Goodlatte. We agree with you. That's why Congressman Goodlatte—Goodlatte's approach is the right approach, if any, to take in this particular area.

Mr. WATT. Thank you, Mr. Chairman.

Mr. GEKAS. The time of the Chairman and the gentleman from North Carolina has expired.

We now recognize Mr. Cannon for 5 minutes.

Mr. CANNON. Thank you, Mr. Chairman.

I apologize to the panel for not having been here the whole time, but there are a number of issues that I—that I think are quite important. And part of this is the fact that in my own family, my 14-year-old son is probably more sophisticated than my wife about some of these issues, but it's my wife who draws to my attention the fact that she gets e-mails from women who haven't seen me or seen her, whatever the case may be, since high school, and—and then when you click through, you get sometimes some unpleasant things.

But if I can direct a question to Mr. Misener, Mr. Lackritz, and Mr. Lane, as I understand it, database protection is about protecting the intellectual property rights of creators, owners, and maintainers of databases. On the other hand, preventing spammers from getting my name so as to prevent them from sending families ads for pornography or other kinds of offensive things seems more like consumer protection than it does database protection.

Are you saying that you would rather allow spammers to send children fraudulent or pornographic ads so the database debate won't be prejudiced? And what if there's explicit language in the amendment that created a—no new property interest in the e-mail address explicitly, taking it out of the realm of database?

Mr. LANE. Well, if I can respond to that, it's sort of like saying that this pen, no one can touch it, only I can use it, but I have no property right over that pen. I mean, just because you say it doesn't make it fact, and so that's one of the concerns that we have by just having a line in there does not resolve our concerns.

But we are concerned that—the precedent that this would set in terms of the use of factual data for marketing purposes, and we don't believe that this is a good precedent to set as there are ongoing database discussions on the use of factual data, which includes names, addresses, phone numbers, as well as discussions on the privacy debate is what is the appropriate use of personally identifiable information, and how that information is gathered.

Mr. LACKRITZ. Mr. Cannon, I don't—I hope that we are not being—that you don't think of us as defending individuals that send pornographic messages to children.

Mr. CANNON. Thank you.

Mr. LACKRITZ. We have no—we have no truck with them, and as far as we're concerned, they should be, you know, prosecuted and locked up, because they just foul the space for everybody else.

I think the real issue is how do—you know, there's a difference between marketing activities and providing opportunities for individuals and consumers versus dealing with fraudulent and pornographic perpetrators over the Internet, and that's where we're try-

ing to draw a distinction, that I think that's the important kind of distinction to draw.

Putting—putting limitations on individuals exercising their freedom to use publicly available facts to exercise business activities and market products and services, legitimate products and services to people I think is a very dangerous road to go down, and it's fraught with peril from the standpoint of the first amendment on the one hand, and just from the standpoint of interfering with legitimate businesses on the other.

Going after, you know, pornographers and people that are sending that kind of stuff to children, as Ms. Lofgren raised, is something we oppose and will work very strongly with you to try and stop that.

Mr. CANNON. Looking for some ideas, frankly.

Mr. LACKRITZ. Okay.

Mr. CANNON. Thank you.

Mr. Misener.

Mr. CANNON. Mr. Cannon, we certainly agree that this issue has to be raised and our question is one of venue, not of the issue itself. We don't feel as strongly as some other companies do about the harvesting of e-mail addresses in public places, but we're certainly willing to talk about it. Our only concern in this context is where that discussion takes place. We believe it is more appropriately addressed in the context of copyright and perhaps privacy, but not in the context of spam.

Mr. CANNON. Thanks.

Can I just follow up, Mr. Misener, with another question?

Mr. MISENER. Certainly.

Mr. CANNON. Amazon pledges to protect your customers' information, including e-mail addresses. Why would you want to allow predatory marketers like mass-spammers to violate the very principles you institute to protect your customers?

The Direct Marketing Association pledged in their best practice policy never to harvest e-mails. How can we protect Americans from irresponsible marketers who don't follow those best practices?

Mr. MISENER. Well, Mr. Cannon, we absolutely do protect our customers' e-mail addresses. They are safe and not public. As to addressing that issue more broadly, again, it's one of, we believe, of just the venue of the discussion. This is a discussion about spam. We felt that that issue was sufficiently distinct from the issue of anti-harvesting. I would be happy to have that discussion with you in the context of copyright and these other venues where this is being discussed.

Mr. CANNON. Great. Thank you.

If the Wilson bill became law, would this be the first major Federal regulation of commerce over the Internet; and if so, would you advocate a go-slow approach to the regulation of online commerce?

Mr. LACKRITZ. Absolutely. I mean, I think the other—the other bill that Congress passed last year affecting commerce on the Internet was E-Sign bill, and that was a very positive and good contribution to the development of commerce over the Internet because it legitimized, you know, e-signatures and that kind of thing. That actually helped to promote commerce and promote the use of the Internet.

This legislation, on the other hand, would be the first bill that it would actually restrict commerce on the Internet. It would also—it would also discriminate, if you will, against commerce that's not on the Internet.

Mr. GEKAS. The time of the gentleman has expired.

Mr. LACKRITZ. It would discriminate against commerce that's on the Internet versus commerce that's not.

Mr. CANNON. Could I ask unanimous consent to be given an additional 1 minute so we——

Mr. GEKAS. Without objection, the time is extended for 1 minute.

Mr. LANE. Our approach on all Internet-related issues is to ensure we narrowly target or have legislation that narrowly targets the harm, the real harm that we can address. We feel that way on the privacy debate. Instead of having overly-broad restrictions on the use of information because of the negative implications that it could have on businesses and consumers, let's find the specific harms and narrowly target legislation to fill those gaps.

We feel that way on the database issue, which is let's find what are the specific harms and narrowly target that gap. And so we feel the same way on the unsolicited commercial e-mail legislation—what are the specific harms, and let's narrowly target the legislation toward those gaps which we believe right now is going after the misleading header information, pornography and some of the other abuses that are out there.

Mr. CANNON. Great.

Thank you, Mr. Chairman. I yield back.

Mr. GEKAS. The time of the gentleman has expired.

We recognize the lady from Texas for 5 minutes.

Ms. JACKSON LEE. Thank you very much, Mr. Chairman. I thank the witnesses for their discussion and you can see that Members are truly quarreling with the best approach.

Let me associate myself with hopefully a good-faith compromise, because I think that there is a concern here that needs to be addressed, and I would suggest to you that when Members legislate, there is some good will and good intent behind trying to address a problem that they have probably heard about over and over again.

I would equate what is attempted here by the old antiquated phone solicitation, and I say that because it probably is declining. But if anyone has any chance to be at home during the day, and that, of course, is probably a fluke, the constant ringing of the phones is a huge annoyance. And so I think the distinction here is that the intrusion on the Internet is silent to a certain extent and may not raise the ire of individuals as much as the ringing telephone; but nevertheless, I think the intent of the authors of the legislation are behind the fact that either consumers are misrepresented to or they are, if you will, inconvenienced. And so I'm going to raise my questions along these lines.

First of all, I raised similar questions about protection of children, and it would appear that children are enticed to buy any- and everything, and so I'm going to ask you again to restate some of the more commercial options that consumers have as it relates to children.

The other thing that I will be looking at is fraudulent sales or cruel sales. And what do I mean by that? There is legislation that I think has recently passed in the State of Texas that prohibits the sale of either the items of the criminal perpetrators, such as Manson was trying to sell a lock of his hair. Heinous things like that are occurring on the Internet, believe it or not, but—or either the victims' items that may be—that someone is attempting—the victim of a particularly heinous crime and if the victim is deceased.

But in any event, that has come to my attention, and so there are some extremes that we find occurring on the Internet, and so my line of questioning will follow some of my colleagues.

I think that—and I'm—Mr. Goodlatte is not here; I'm going to ask him how does he—how does he view the meshing of his legislation to the legislation of Congresswoman Wilson. I'd like you to answer that question first, and I'll ask each gentleman, how do you see those legislative initiatives meshing? And you need to say where you don't see them meshing, meaning that, I'd rather go with the Goodlatte. I'm not forcing you to say that, but if we're in a moment of compromise, that may be what occurs, and I think that the major point that most of us have been making, we're asking you as experts, you'd better speak up now as to what won't work, meaning, no, they won't mesh, or, I'm really for only this one. That helps us.

My second question would be to restate again how children can be helped or how consumers can be helped when it relates to children, and particularly fraudulent or the excessive buying or enticing to buy or enticing to do things, in quotes, "unbecoming" to children.

And then Mr. Lane, I'm going to pointedly ask you a question because it appears that you have said in your testimony that you would be supportive of legislation, but you yield or you would lend yourself, associate yourself to Federal legislation because you are concerned about duplicative and overlapping State legislative initiatives. Clarify that point for us so that we can at least understand your position today, though it may be emerging and changing. I'm going to go to you on that point, and the gentlemen, if you can answer my other questions more particularly.

Mr. Lane.

Mr. LANE. Starting with the States' problems, and I don't know if this is a full list, but right now, there are approximately twelve States—California, Connecticut, Delaware, Idaho, and several others—that have laws on the books dealing with unsolicited commercial e-mail or e-mail.

My understanding is on this——

Ms. JACKSON LEE. How many States?

Mr. LANE. I could count them.

Mr. LACKRITZ. We counted twelve.

Mr. LANE. Fourteen States that I have here. There may be others on the book.

Ms. JACKSON LEE. Okay.

Mr. LANE. And so—and they all have different provisions of definitions of what is unsolicited commercial e-mail.

Ms. JACKSON LEE. Right.

Mr. LANE. My understanding is that the California law has been struck on the dormant commerce clause.

Ms. JACKSON LEE. So what you want to do is to get rid of the confusion.

Mr. LANE. I want to get rid of the confusion so we have a standard in place for e-mail that's fraudulent or the commercial—or the header information is fraudulent or the routing information is fraudulent.

On the other question you had dealing with the selling of awful things, I would call it, on the Internet, that's a problem obviously, and it's of concern; but I don't know if you can stop it under the first amendment.

There's currently a case taking place here in the U.S. when Yahoo France was being fined by the French Government for selling Nazi memorabilia because it was against French law. Obviously that's a horrible thing, but can we stop it under the first amendment? We get into those problems, and I don't know how you address that.

Mr. GEKAS. Does the lady require an additional 30 seconds?

Ms. JACKSON LEE. I would appreciate it if the distinguished Chairman would give me an additional minute so that these gentlemen could answer my two questions.

Mr. GEKAS. Without objection.

Ms. JACKSON LEE. I thank the Chairman very much.

And I would just say, Mr. Lane, you prefer, if there is legislation, that it be Federal legislation. Is that my understanding?

Mr. LANE. Yes.

Ms. JACKSON LEE. Thank you.

Mr. LACKRITZ. Following up on that, we would support the Goodlatte approach here rather than the Wilson approach. It—it seems to us that the whole preemption is very important here. You don't want to have 50 separate State laws that are going to create—going to throw sand in the wheels of the Internet, basically. When we—when we've had, you know—when we've delegated these things to States in certain circumstances—here, we've got a national issue, you've got an Internet, it's global, and to have 50 separate State authorities setting these standards would be—would be very foolish.

One of the reasons we like the Goodlatte approach more than the Wilson approach is that what he does is, at the Federal level, articulates a definition of what's wrong and what's criminal or what's, you know, what's fraudulent. That's a much easier mechanism to go through than setting up this scheme of delegating to Internet—Internet service providers the right to write regulations that are going to have the force of law, creating private rights of actions, State attorney generals with enforcement powers, and the FTC. So that's why we favor the Goodlatte approach.

With respect to the good taste issue, I'm not sure we can ever legislate against bad taste. I really wish we could. And from the standpoint of what to do with children, my sense is now that there are filters that are available now where you can put the filters onto the computers and only allow e-mails in that you want to have come in, and my sense is that for parents, that's the best way of

approaching this, not by creating new rights responsibilities or lawsuits.

Ms. JACKSON LEE. Mr. Misener.

Mr. MISENER. Ms. Jackson Lee, very briefly, your two questions—first our principal problems with H.R. 718. In our view, the principal problems really have to do with the applicability of this statute to relationships with existing customers.

Amazon.com, as I mentioned before, does not send out any kind of e-mail to consumers with whom they do not have a prior business relationship, and therefore we're very concerned when the law starts to apply to existing business relationships.

The second is the involvement of ISPs in the establishment of rules that have the force of law.

Your second point had to do with kids and content. My strong plea is to you that this be dealt with in the context of content, not a specific medium. I don't want child pornography arriving at my house via the mail, by carrier pigeon, or any other means. It—it should be addressed, I think, I believe, in the area of content, not the medium.

Mr. CREWS. Just briefly on the children and content issue. There are risks that go along with the benefits of the Internet and parents have to be extremely vigilant, and this is one that goes beyond just e-mail because the kinds of offerings you are talking about show up on eBay and other Web sites that auction this material off. So it's completely outside of the e-mail question, but it's one that—that we're trying to address, too.

But parents need to know their options. I mentioned the Handshake options on e-mails, but even beyond that, believe it or not, there are companies—there's one in particular called E-Kids Internet that is working with Hewlett-Packard for servers and Cisco for routers and Abovenet for fibers that has actually set up a separate Internet all together that subscribers join. There are thousands of subscribers to this now, and it's a completely safe environment for kids. In other words, you cannot get there from here, you cannot get information off of the worldwide Web to E-Kids Internet; it's a separate network for kids. And I think in the future, you're going to see more of that kind of innovation adapting to what people want.

Ms. JACKSON LEE. Thank you, Mr. Chairman.

Mr. GEKAS. The time of the lady has expired.

Ms. JACKSON LEE. And I assume, Mr. Chairman, you've allowed us to put our opening statements in the records. I ask to do so.

Mr. GEKAS. Without objection.

Ms. JACKSON LEE. Thank you.

Mr. GEKAS. The gentleman from California, Mr. Issa, is recognized for 2 hours. [Laughter.]

Mr. GEKAS. But we'll reduce that to 5 minutes.

Mr. ISSA. Thank you, Mr. Chairman. I'll use revise and extend to get the other hour and 55 minutes.

As some of you at the desk know, I come from the electronics industry, and as a result, I'm expected to be one of your best friends, and I am, but I also am here today to be one of your worst nightmares.

Lee Iacocca was well known late in his career for saying, lead, follow, or get out of the way. These two bills are before us today because you didn't lead; the States are inappropriate to lead and that leaves only the Federal Government to take a lead. And although I share what some of you have been saying very diplomatically that Heather Wilson's bill has some good in it, Mr. Goodlatte's bill has more good in it, but none of you are thrilled with them 100 percent, and I have expressed that to my colleagues, too.

My frustration here today is that I—and I apologize for not being here for the entire time, but I've heard a tone that doesn't have enough answers coming from industry, and I appreciate that Amazon.com and the other what we would call big players or deep pockets if we think of it in a trial lawyer's stance are very good and very sensitive to the problems. But many of the proposed solutions, many of the things you say are becoming available, even the filters, have been clearly insufficient to meet the ingenuity of all the people out there in this ubiquitous Internet.

And so I would ask that when you revise and extend, when you look at—at giving me answers, and there's been plenty of questions to allow you to give these answers, that, in fact, you give us the guidance to modify this legislation, and it will be probably more Mr. Goodlatte's than Ms. Wilson's, but it's clear that we're going to do something and we're going to move the bastion of authority to the Federal Government and lead, that you give us additional guidance, and if there are out-clauses that you think need to be there, that you prescribe how we can give an out-clause—because of self-regulation, or because of adherence to other standards—and if there's going to be a public/private entity, that you describe it in some detail such that the Federal Trade Commission can understand that this is possible.

You know, there—there is no question that the gentlewoman from California, for example, Ms. Lofgren, she makes a very good point. When I receive junk mail, it's in an envelope. If I received a nude picture on a postcard, we would have already been having hearings on that years ago. I don't receive eight-by-ten glossies as junk mail; I do receive eight-by-ten glossies as e-mail that are clearly an open letter. And so there are some things that are going to have to be done.

I think Mr. Goodlatte has thoughtfully given you the best first effort, and I would—I'm not going to ask you a lot of questions, but I would ask that you use your ability to supplement to give us back some additional specific guidance, and that you be less diplomatic than you have been here today.

The—probably the only question I ask you all is, is the ISP the right entity—I don't know the number today, but some of—one of you must know. How many ISPs are there?

Mr. MISENER. Thousands.

Mr. LACKRITZ. Five-thousand. More than——

Mr. ISSA. Five-thousand. Okay. And that's in the U.S., right? Clearly this is standing a long way down the answer, and when you start looking and saying, well, there's got to be an alternative and we want to stay away from private action, I would ask you to answer two questions a little bit here today, but the rest of it in

paper, or e-mail, that, one, if the FTC—or if we're going to avoid private action, what is the alternative first place to go to?

If someone wants to make a sex discrimination or race discrimination case in California, they must first go to a body and that body must release them to sue, and then they're allowed to sue, and I would think the model that would happen would be similar to that in this case if we allow a private action.

And secondly, do you have some sort of a proposal of a universal third party that an e-mail could be forwarded to and I'm done with it, rather than trusting the benevolence of some organization that sends you unsolicited e-mail that may or may not have complied with the law, and when you try to send it back, often, as you know, the recipient is not accepting or it asks you to fill out a form and tell more about your life in return for turning off.

I would ask that you seriously consider an industry solution. There are great minds within what used to be our industry, and I believe that you can do that, and the more you give us sooner, the better our legislation would be. And I would leave time for oral answers.

Mr. LANE. We look forward to working with you on suggestions as we move forward.

The first entity that we believe that a customer should go to to be taken off is the business itself and reply in some manner—that you have a legitimate reply mechanism or legitimate connection to a Web site so that you can contact them before you go running to another entity.

If that cause—if that doesn't work, the FTC has been collecting over the years spam e-mails and they've been looking into them, especially from the fraudulent side, to make sure that customers are not harmed.

In terms of technology being able to be circumvented because of the ingenuity of folks out there, amazing as it may sound, they're pretty clever in terms of circumventing laws as well, and that's also a concern, where they go offshore to avoid U.S. law, and the ones who are actually harmed are U.S. businesses. So we need to make sure that we don't do something that harms U.S. businesses and drives the bad guys off shore, because they are incredibly clever, as we know.

Mr. LACKRITZ. If I could just address your question very briefly——

Mr. ISSA. Very briefly.

Mr. LACKRITZ. I think——

Mr. ISSA. I'm out of time.

Mr. LACKRITZ. I appreciate that.

I think your point is very well taken. I would only note that I know in the securities industry, the rush to get into the Internet space has been so—so intense that the focus has been on creating opportunities and not yet on eliminating abuses. For us, our legitimate businesses, obviously these spammers are not good for any of us, and I think that we're just beginning to focus on eliminating the abuses because everybody has been focusing on creating opportunities, which we think is what the new technology really enables.

So we're happy to work with you.

Mr. ISSA. Thank you, Mr. Chairman.

Mr. GEKAS. I thank the gentleman.

The Chair wishes to comment that this has been, in my experience, one of the finest hearings held in the Judiciary Committee on a very complex and tense subject, and I wish personally to thank the witnesses and to ask them to be poised to answer new questions or old questions by written interrogatories, some of which are piling up already, and you will help us a great deal to serve you and to serve the public.

This hearing stands adjourned.

[Whereupon, at 12:10 p.m., the hearing adjourned.]

APPENDIX

STATEMENTS SUBMITTED FOR THE HEARING RECORD

PREPARED STATEMENT OF THE HONORABLE GEORGE GEKAS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF PENNSYLVANIA

A quorum being present, the Committee will come to order.

Today, the Committee holds a legislative hearing on two related bills - H.R. 718, the "Unsolicited Commercial Electronic Mail Act of 2001," introduced by Representative Heather Wilson, and H.R. 1017, the "Anti- Spamming Act of 2001," introduced by Representative Goodlatte.

H.R. 718 and H.R. 1017 both propose to address problems raised by unsolicited commercial e-mail, also known as spam. Today's hearing will address the various questions that arise regarding unsolicited commercial e- mail and what role the federal government, state attorneys general, and the trial bar should be in addressing these issues.

The debate about spam is often complicated because policy makers often confuse or don't understand what constitutes spam. Often, the term spam is used to encompass a number of different practices, some criminal, some annoying, and some benign. Often, e-mail fraud, e-mail pornography, and e-mail marketing all lumped into the same category and referred to as spam. They are demonstrably different, and the amendment adopted by the Committee recognizes those differences.

Fraudulent messages, that is e-mail messages whose content is intended to deceive, cheat, defraud, or swindle consumers, is already illegal. Since 1994, the Federal Trade Commission has brought 173 law enforcement actions against more than 575 defendants to halt online deception and fraud. I am greatly concerned about unscrupulous scam artists who take advantage of the uneducated, naive, and gullible. Furthermore, the proliferation of fraudulent e-mail poses a threat to consumer confidence in online commerce.

Another related type of e-mail fraud is known as technical fraud. Technical fraud includes forging or falsifying header and return information, thereby concealing the sender's identity. Those who engage in content fraud often use technical fraud to conceal their true identities. Furthermore, technical fraud is used to defeat Internet service providers' and computer users' e-mail filters, preferences, and other technologies designed to block unwanted e-mail. Both the Wilson bill and the Goodlatte bill attempt to address the issue of technical fraud. The amendment adopted by the Committee clearly and directly addresses this particular issue.

A third problem is e-mail pornography. Rep. Wilson has stated repeatedly that the reason she became interested in this issue is because she received an unsolicited pornographic e-mail several years ago. Neither bill does anything to directly address this issue although commercial pornographers who send unsolicited e-mail would be placed under the same legal strictures as mainstream companies under the Wilson proposal. The Hart amendment, adopted by the Committee, clearly and directly addresses this issue.

The last issue addressed by the Wilson bill, and the most controversial component of this debate, is the regulation of e-mail marketing. The Wilson bill sets up an elaborate enforcement system to regulate unsolicited commercial e-mail. Violators of the bill could have the FTC, state attorneys general, ISPs, and recipients of the e-mail filing various legal actions against them. This raises several concerns.

First, the Wilson bill, if passed, will be the first major federal regulation of online commerce. Marketing, no matter how annoying, is integral to the success of commerce, including electronic commerce. Congress has supported and encouraged Internet commerce in several ways. The E-signatures bill and Internet access tax moratorium were affirmative signals that Congress wanted the efficiencies of the Internet to bring choices, competition, and needed information to consumers. Electronic commerce is still in its infancy. Business models are constantly changing to

find the right formula for success over the Internet. For example, banner ad revenue has fallen almost as much as the stock prices of many dot-coms. The Committee should seriously consider the ramifications of regulating e-mail marketing and its impact on the growth of commerce.

Another concern about the regulation of e-mail marketing has to do with proportionality. Assume for a moment that an established company were to send you an e-mail advertisement every day for a month peddling its newest line of ugly polyester ties. You wouldn't buy them and would be annoyed at receiving the messages. However, most established companies offer some sort of permission based marketing, and at a minimum the vast majority offer recipients the opportunity to opt out of receiving future messages. Furthermore, the recipient could sign up with the Direct Marketing Association's e-mail preference service to discontinue the unwanted marketing messages. The receiver of the messages could also establish an e-mail preference to discard the messages automatically. Finally, the recipient can do the equivalent of throwing junk mail in the trash by merely hitting the delete key. I am concerned about making a federal case out of a mere annoyance. The Justice Department, FTC, and state attorneys general likely have more pressing matters to deal with than annoying commercial e-mail. Congress should carefully consider proposals to unleash the FTC, state attorneys general, and the trial bar on U.S. businesses for sending unsolicited commercial e-mail.

Lastly, the Internet's greatness and potential lies in its decentralized configuration. The lack of centralized control mechanisms and the international nature of this global medium raises concerns about the efficacy of any regulatory regime. Established and small U.S. companies are not likely to move operations off shore and will be subject to the long arm of the law and to a plaintiff's attorney's subpoena.

The bad actors—scam artists and porn spammers—may merely move their operations off shore out of the reach of the federal government.

I believe we should do what we can to address fraudulent and pornographic e-mail, but also believe we need to be careful and cautious about regulating e-mail marketing. Congress should avoid falling victim to the law of unintended consequences, particularly at a time where Internet commerce is struggling to survive.

I also look forward to hearing the views of the witnesses and now recognize Mr. Conyers for his opening statement.

PREPARED STATEMENT OF THE HONORABLE BOB GOODLATTE, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF VIRGINIA

Thank you Mr. Chairman for holding this very important hearing. I appreciate the opportunity to hear from today's witnesses about the need for legislation to address the growing problem of mass unsolicited e-mail, also known as "spam."

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

Marketers have learned to take advantage of this new capability to reach consumers. Many consumers choose to communicate via e-mail with their financial institutions, favorite retailers and other companies with which they form relationships. Millions of individuals and businesses opt to receive communications and notices by e-mail. In order for the Internet to continue to thrive and grow as a medium for commerce, legitimate businesses must be able to reasonably communicate with their customers or consumers who wish to do so.

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

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

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

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

E-mail fraud includes forging or falsifying header and return information, thereby concealing the sender's identity. Those who engage in content fraud and those who send pornographic e-mail often use such technical fraud to conceal their true identities. Furthermore, technical fraud is used to defeat ISPs' and computer users' e-mail filters, preferences, and other technologies designed to block unwanted e-mail.

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

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

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

Because of the complexity surrounding all e-commerce issues like spam, legislation must be carefully balanced to ensure that enforcement mechanisms address real harms without causing damage to the unique advantages provided by the Internet. Legislation should be narrowly targeted to provide law enforcement with the tools they need to combat abuses without opening the floodgates to frivolous litigation or interfering with legitimate uses of e-mail for marketing purposes. In this vein, I would suggest that spam legislation should include strong monetary penalties, however, we should proceed with caution regarding the inclusion of a private right of action in that it could have the unintended consequence of discouraging the use of electronic commerce.

Legislation addressing the problem of unsolicited commercial e-mail is greatly needed during this legislative session to protect consumers and Internet Service Providers from victimization by spam.

I commend you, Representative Wilson, on your tireless efforts to address this issue. You should be commended for your role in bringing the problem of spam to the forefront of public debate. I look forward to continuing to work with you to achieve our common goal of reducing the burden of unwanted e-mail on consumers and Internet Service Providers.

Again, I thank you Mr. Chairman for holding this important hearing and I look forward to the testimony of our witnesses.

PREPARED STATEMENT OF THE HONORBALE JOHN CONYERS, JR., A REPRESENTATIVE IN CONGRESS FROM THE STATE OF MICHIGAN

At the outset, I would like to congratulate the Chairman for protecting our Committee's jurisdiction on this issue and holding this timely hearing.

Spam is not a trivial issue. Anyone who uses the Internet can tell you it's no fun being constantly bombarded with unsolicited e-mails. And any parent can tell you they don't want their young children exposed to fraudulent or pornographic spam.

And spam can be costly, as well. It takes time to delete and block unwanted e-mails, and ISPs must have extra server capacity to handle the flood of e-mails. I'm not entirely surprised that the worldwide costs of spam have been estimated at $9.4 billion per year, and that America Online believes spam accounts for 30% of its e-mail traffic.

At the same time, though, I hope we can approach the problem reasonably. The Majority always promotes federalism and talks about how congressional action

erodes states' rights in the areas of hate crimes and civil rights, but then it promotes legislation that imposes Federal criminal penalties for sending e-mails. On this issue, I have to support the federalists because I'm just not convinced we want people sitting in Federal penitentiaries for sending e-mails.

First, we should take a hard look at the feasibility of criminal sanctions—the most severe penalty available to Congress. Our U.S. Attorneys are busy—as they should be—fighting violent crime and gun offenses. And our Federal judges, including Chief Justice Rehnquist, have complained that Congress is federalizing too many crimes and overloading the court system. We should instead consider a graduated approach, by which we seek injunctive relief against an offending party before we devote Federal resources to incarcerating them.

Second, we must be sensitive to civil liberties and free speech rights. The First Amendment clearly applies to the Internet, so any government regulation would have to be "no more extensive than necessary" to achieve a "substantial government interest."

Finally, we shouldn't duplicate existing legal protections. State laws already provide for actions against deception and fraud. At the Federal level, both the FTC and the SEC prosecute fraudulent activity. Before we write a new law, we should know how it would fit with current laws.

I hope to work with the Chairman to craft a balanced bill that provides for a real and viable means of controlling spam while respecting our free speech rights.

PREPARED STATEMENT OF THE HONORABLE HOWARD L. BERMAN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Mr. Chairman,

Thank you for calling this hearing and putting together a panel of witnesses who can knowledgeably address the issue of unsolicited commercial e-mail.

Unsolicited commercial e-mail, or "spam mail," is a problem for all of us. Spam drives up the costs for Internet Service Providers. Many feel it is an invasion of privacy and are concerned that their personal information is being shared, resulting in lowered confidence in e-commerce.

I support the need for anti-spam legislation. At the same time, I am concerned that we do not limit the rights of legitimate businesses to advertise their products, police their intellectual property and protect their consumers.

The bills that our witnesses will be testifying about today contain many interesting provisions. I believe that these bills get us on the right track by focusing the dialogue on how best to protect consumers from unwanted commercial e-mail without infringing on First Amendment and other rights.

Again, thank you, Mr. Chairman, for calling this hearing. I look forward to hearing from the witnesses.

PREPARED STATEMENT OF THE HONORABLE SHEILA JACKSON LEE, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS

Thank you Mr. Chairman.

Mr. Chairman, these legislative initiatives before us today, H.R. 718 and H.R. 1017, both seek to deal with the very serious problem of unsolicited email messages, also known as "spamming."

H.R. 708 and H.R. 1017 address spamming by providing criminal penalties. However, H.R 718 also provides additional penalties not directly related to fraud and deceptive practices. This problem is widespread. In recent years spamming has reached all levels of society and government. According to a report by the Congressional Management Foundation, the Congress of the United States received more than 80 million pieces of electronic mail last year. Most of these were unsolicited bulk mailings that interfered with congressional communications and the overall operations of congressional ofFeists.

A Gartner survey released last month found that U.S. employees spend 49 minutes or ten percent of each workday managing mail. This is probably much higher for congressional staff.

In order to solve this problem we must confront two hurdles: (1) understanding that unsolicited electronic mail is legal and is protected as speech under the First Amendment; and (2) we have yet to define what the term "unsolicited commercial email" actually means.

However, in our haste to stop the most egregious forms of spamming, criminally harassing advertising, we run the risk of silencing individuals and businesses across this nation who selectively and responsibly use e-mail simply as a means of speech.

For example, some organizations offer services to eliminate spam, whether legitimate or criminal, and indiscriminately damage legitimate businesses and individuals in the process. Such "Spam-busters" usually operate as filters for large groups by simply blacklisting the domain alleged to be the source of the spam. This is wrong, and can be damaging to the reputation and commerce of a firm that has been erroneously singled by the spam-buster.

Mr. Chairman, there are measures that we can take to eliminate harassing or illegal spam while not frustrating the efforts of legitimate e-mail users. In a recent Senate Commerce Committee hearing on this very issue, it was estimated that over 90 percent of spam today is fraudulent. Technical measures and public policies should be pursued that prevent and/or prohibit the use of fraudulent headers to send unsolicited commercial email messages.

Additionally, standard-setting institutions need to continue to search for technical standards and specifications in order to assist users in controlling incoming email. Fortunately, Internet Service Providers (ISPs) offer the option of filtering commercial e-mail ("opt-out") or bypassing the filtering so that they receive all or part of the stream of mail ("opt-in").

Importantly, while we must continue to monitor and vigorously prosecute those who stalk the Internet, we must take care to protect what is greatest about the Internet and about this nation: our freedom.

The development and implementation of technical tools and public policies that support the kind of innovation that allows for filtering spam without absolute censorship makes good sense, and is imperative for free and robust speech to continue. These technologies put the consumer in control, so government doesn't have to.

I look forward to hearing testimony on these important matters of public policy. Thank you.

PREPARED STATEMENT OF LAURA W. MURPHY, DIRECTOR AND MARVIN J. JOHNSON, LEGISLATIVE COUNSEL, AMERICAN CIVIL LIBERITIES UNION

Mr. Chairman and Ranking Member Conyers:

Thank you for this opportunity to present our views on H.R. 718 and H.R. 1017, two efforts to legislatively address spam, often referred to as "unsolicited commercial electronic mail" or UCE. We urge you to oppose this legislation because it infringes on First Amendment rights.

The ACLU believes this is an area in which current law already provides adequate remedies, and, therefore, the government should not engage in further legislation. However, if this Committee believes action is necessary, there are problems in both bills that must be addressed to avoid constitutional issues. With regard to H.R. 718, this Committee should:

1. Amend the bill to apply only to bulk unsolicited electronic mail, and specifically define "bulk mail."
2. Amend the definition of unsolicited commercial electronic mail to clarify that it applies only to those messages that are predominantly concerned with commercial transactions.
3. Delete the provision requiring accurate routing information. It is destructive of anonymity and punishes innocent speech.
4. Delete the provision regarding "identifiers." This is a form of prior restraint and compelled speech.
5. Remove provisions allowing Internet Service Providers to set their own policies and have them enforced as federal law. The overall effect of this provision may effectively ban unsolicited commercial electronic mail.

With regard to H.R. 1017, this Committee should:

1. Amend the bill to specifically define "bulk" mail.
2. Amend the bill to apply solely to commercial transactions.
3. Delete the provision requiring accurate routing information. It is destructive of anonymity and punishes innocent speech.
4. Delete the provision prohibiting dissemination of software designed to protect privacy.

THERE IS NO SUBSTANTIAL NEED FOR GOVERNMENT INTERVENTION IN THIS AREA.

Initially, we question whether government regulation of truthful unsolicited commercial electronic mail is appropriate at all. Where the communication is truthful, it is generally preferable to let the marketplace control, rather than government intervention.

Clearly, the government may have a role in regulating such mail where it is fraudulent, but current law already provides a remedy. The Federal Trade Commission currently pursues such cases.[1] The Securities and Exchange Commission rules prohibit certain kinds of stock promotions, and various state laws closely regulate contests and sweepstakes. Thus, fraudulent electronic mail can be attacked using current laws.

Sending spam by misappropriating another's domain name has already been successfully prosecuted. Last year, America Online used trademark and unfair competition laws to pursue a spammer who sent 73 million e-mail messages for his adult web sites using an "aol.com" address. The address was nonexistent. The federal magistrate found the use infringed on America Online's trademark and recommended that the spammer pay damages of more than $1.5 million.

Many Internet Service Providers (ISPs) expressly prohibit their users from sending spam. For example, Earthlink's current "Acceptable Use Policy" prohibits subscribers from sending "any unsolicited commercial email or unsolicited bulk email" or using its services for activities "that have the effect of facilitating unsolicited commercial email or unsolicited bulk email whether or not that email is commercial in nature." Those who breach such contracts may find their service terminated. Because ISPs rely on customer service and satisfaction to keep their customers, and the performance of their servers is an integral part of that satisfaction, they are not reluctant to pursue customers who violate the contract.

Where the spammer is not a customer, ISPs have successfully sued spammers on various theories, including trespass and by making claims under the Computer Fraud & Abuse Act.

Many ISPs employ spam "filters" and consumers have filtering options available as well.

Because current law, the marketplace and software options such as filters already deal with spam, there is no overwhelming need for further federal legislation, particularly where that proposed legislation raises constitutional concerns.

ANY SPAM LEGISLATION SHOULD ONLY APPLY TO BULK COMMERCIAL EMAIL, WHICH SHOULD BE SPECIFICALLY DEFINED. FAILURE TO DO SO SUBJECTS THE BILL TO CHALLENGE UNDER *CENTRAL HUDSON GAS* V. *PUBLIC SERVICE COMMISSION* AND *44 LIQUORMART INC.* V. *RHODE ISLAND*.

The Supreme Court has recognized that the First Amendment applies to the Internet. *Reno* v. *ACLU, 521 U.S. 844, 117 S. Ct. 2329 (1997)*. Any restriction on speech on the Internet must therefore be scrutinized for its First Amendment implications.

H.R. 718 applies solely to commercial speech in the form of unsolicited commercial electronic mail. Commercial speech is protected under the First Amendment to the United States Constitution. In *Bigelow* v. *Virginia*, 421 U.S. 809 (1975), the United States Supreme Court held that "speech is not stripped of First Amendment protection merely because it appears" as a commercial advertisement. *Id.* at 818. In 1976, the Court reaffirmed that speech that "does no more than propose a commercial transaction" is protected by the First Amendment. *Virginia State Board of Pharmacy* v. *Virginia Citizens Consumer Council, Inc.*, 425 U.S. 748, 762 (1976).

In order for the government to regulate commercial speech, it must have a "substantial governmental interest." Furthermore, the regulation must be no more extensive than necessary to achieve the government's interest. *Central Hudson Gas* v. *Public Service Commission*, 447 U.S. 557 (1980).

The Supreme Court strengthened commercial speech protections in 44 *Liquormart Inc.* v. *Rhode Island*, 116 S. Ct. 1495 (1996). In 44 Liquormart, the Court invalidated a regulation banning the advertisement of liquor prices. Justice Stevens, writing for a plurality, noted that when scrutinizing restrictions on truthful commercial speech, "there is far less reason to depart from the rigorous review that the First Amendment generally demands." 116 S. Ct. at 1507. The plurality further noted

[1] On April 26, 2001, the Federal Trade Commission testified before the Senate Subcommittee on Communications of the Committee on Commerce, Science and Transportation regarding their efforts to address fraudulent UCE. The FTC first filed an enforcement action against deception on the Internet in 1994. Since then, the FTC has brought 173 enforcement actions against more than 575 defendants.

that commercial speech restrictions on truthful information are only justified where there are "no less onerous alternatives." With these words, the plurality veered toward a strict scrutiny approach. Thus, to regulate truthful commercial speech, the government must have a substantial government interest, and the regulation must be narrowly tailored and the least onerous of the alternatives.

While H.R. 718 declares a substantial government interest, it fails to narrowly tailor the regulation to achieve that asserted interest.[2]

Section 2(a), subsections 4 and 5, focus on the shifting of costs from the sender to the recipient or the ISP. This appears to be the primary governmental interest articulated. In testimony on this bill's predecessor in the 106th Congress, the rationale for regulation of UCE was not the isolated unsolicited commercial electronic message, but the sheer volume of *bulk* commercial electronic mail. On the Internet, it costs virtually the same to send one message or one thousand messages. The testimony suggested that flooding the Internet with *bulk* unsolicited electronic mail caused servers to crash, and costs to mount for the Internet service providers. Recipients were inundated with messages on how to "get rich quick." Thus, the harms discussed in the testimony were directly related to *bulk* unsolicited commercial electronic mail, rather than unsolicited electronic mail in general.

H.R. 718 does not discuss bulk electronic mail. It prohibits *any* unsolicited commercial electronic mail. For example, suppose you met someone on an airplane who you thought might be a good business prospect. You exchanged business cards, and she had her e-mail address on the card. When you get back to your office, you send her an e-mail proposing a business transaction. According to H.R. 718, you have now sent an unsolicited commercial electronic mail message, and may have violated the policies of an Internet service provider.[3]

The net cast by H.R. 718 is therefore far too broad and is likely to run afoul of *Central Hudson* and 44 *Liquormart*. The bill should define bulk mail and apply the regulations to those who send such mail. Bulk mailers are often far more likely to have the resources to comply with these rules. The average small business-person sending out a couple of e-mails here and there to drum up business is unlikely to have the same resources.

H.R. 1017 applies to *all* email, whether commercial or private. While it refers to "bulk unsolicited electronic mail," the term "bulk" is never defined. Because this bill broadly applies to all email, it is not entitled to analysis under the "relaxed" commercial speech standard. It therefore, is even less likely to withstand constitutional scrutiny than H.R. 718.

THE DEFINITION OF COMMERCIAL ELECTRONIC MAIL IN H.R. 718 MAY SWEEP TOO BROADLY.

The definition of "commercial electronic mail message" in H.R. 718 is also troublesome. "Commercial electronic mail message" is defined as a message that "primarily advertises or promotes the commercial availability of a product or service for profit or invites the recipient to view content on an Internet web site that is operated for a commercial purpose."

In the case of a message asking the recipient to view a web site, what level of "commercial purpose" suffices to bring the message within the ambit of the definition? For example, if a non-profit organization runs a web site primarily to educate the public about its issue, but also sells products through the web site (books, t-shirts, etc.), does an unsolicited email directing the recipient to the web site become "commercial?"

The bill uses the word "primarily" earlier in the sentence, to modify "advertises or promotes." "Primarily" should also be added before the words "operated for a commercial purpose." This would make it clear that web sites with an incidental commercial purpose will not be swept into the ambit of the bill.

BOTH BILLS PROHIBIT CONSTITUTIONALLY PROTECTED ANONYMOUS SPEECH BY REDEFINING IT AS "FRAUD."

"Fraud" is normally defined as "a false representation of a matter of fact, whether by words or by conduct, by false or misleading allegations, or by concealment of that

---

[2] It is not clear there is a substantial government interest in regulating truthful unsolicited commercial electronic mail. The bill declares that interest based on its findings, but never quite delineates what that interest may be.

[3] H.R. 718 notes in its findings that "Unsolicited commercial electronic mail can be an important mechanism through which businesses advertise and attract customers in the online environment." After recognizing this beneficial aspect to UCE, the bill then proceeds to ban it. According to House Report 107–41, dated April 4, 2001, the purpose of H.R. 718 is to "prohibit the initiation and transmission of unsolicited commercial electronic mail messages."

which should have been disclosed, which deceives and is intended to deceive another so that he shall act upon it to his legal injury." *Black's Law Dictionary*, Sixth Edition. Both H.R. 718 and H.R. 1017 expand the definition of fraud to include anonymous unsolicited e-mails, regardless of the intent to induce action to the detriment of the recipient.[4] Mere concealment of one's identity becomes the crime. Fraud is thus transformed in this context from a specific intent crime to one of general intent; the government need no longer prove any intent to defraud the recipient, only the act of concealing one's identity.

Anonymous speech is protected under the First Amendment. *Talley* v. *California*, 362 U.S. 60 (1960); *McIntyre* v. *Ohio Elections Commission*, 115 S.Ct. 1511 (1995). This right of anonymity has also been applied to speech over the Internet, *American Civil Liberties Union* v. *Miller*, 977 F.Supp. 1228 (N.D. Ga. 1997) and *American Civil Liberties Union* v. *Johnson*, 4 F.Supp.2d 1029 (D.N.M. 1998), and even to commercial speech. *NLRB* v. *Midland Daily News*, 151 F.3d 472 (6th Cir. 1998).[5] By requiring accurate information, H.R. 1017 in one fell swoop destroys all anonymous communication on the Internet, while H.R. 718 has the same effect for *commercial* electronic mail.

A similar provision[6] was challenged in *American Civil Liberties Union* v. *Miller*, *supra.*, and a preliminary injunction was granted.

> [B]ecause "the identity of the speaker is no different from other components of [a] document's contents that the author is free to include or exclude," McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 340–42, 115 S.Ct. 1511, 1516, 131 L.Ed.2d 426 (1995), the statute's prohibition of internet transmissions which "falsely identify" the sender constitutes a presumptively invalid content-based restriction. See *R.A.V.* v. *St. Paul*, 505 U.S. 377, 382, 112 S.Ct. 2538, 2542–43, 120 L.Ed.2d 305 (1992). The state may impose content-based restrictions only to promote a "compelling state interest" and only through use of "the least restrictive means to further the articulated interest." *Sable Communications of California, Inc.* v. *FCC*, 492 U.S. 115, 126, 109 S.Ct. 2829, 2836, 106 L.Ed.2d 93 (1989).

The court noted that fraud prevention was the asserted state interest, but the statute was not narrowly drawn to achieve that end.

> [B]y its plain language the criminal prohibition *applies regardless of whether a speaker has any intent to deceive or whether deception actually occurs.* Therefore, it could apply to a wide range of transmissions which "falsely identify" the sender, but are not "fraudulent" within the specific meaning of the criminal code. [Emphasis added.]

The court found that the ACLU was likely to prevail upon its claim of overbreadth, because the statute swept protected activity within its proscription. Specifically, the act prohibited "such protected speech as the use of false identification to

---

[4] Section 4 of H.R. 718 as reported from the House Commerce Committee makes it a crime to send a message with "knowledge that any domain name, header information, date or time stamp, originating electronic mail address, or other information identifying the initiator or the routing of such message, that is contained in or accompanies such message, is false or inaccurate." Section 5(a)(3)(C) requires messages have a "physical mailing address of the initiator." Using the term "with knowledge" would include any anonymous UCE message, regardless of the reasons for wanting anonymity, and even if the information contained in the message was entirely truthful. Requiring a valid physical postal address in the message has obvious implications for anonymity. H.R. 1017 prohibits "intentionally and without authorization" initiating "the transmission of a bulk unsolicited electronic mail message to a protected computer with knowledge that such message falsifies an Internet domain, header information, date or time stamp, originating e-mail address, or other identifier." Although use of the term "without authorization" would seem to limit the reach of the statute, it is unclear in some of the instances who could give such authorization.

[5] In keeping with the Supreme Court's rulings providing less protection for commercial speech, the court applied the test enunciated in *Central Hudson*.

[6] The challenged law in *ACLU* v. *Miller* was not limited solely to commercial electronic mail, similar to H.R. 1017. Although H.R. 718 limits its regulation to commercial electronic mail, it does not escape constitutional scrutiny. As noted previously, *Central Hudson* applies to commercial speech regulations, and also requires a narrow tailoring between the "substantial governmental interest" and the challenged regulation. Additionally, 44 Liquormart requires the government use the least onerous alternative. Here, there is no narrow tailoring or use of the least onerous alternative. For example, an unsolicited commercial electronic mail message could be entirely truthful, but illegal, under both bills by knowingly using inaccurate header information.

avoid social ostracism, to prevent discrimination and harassment, and to protect privacy . . . "[7]

Both bills suffer from the same infirmities. With no compelling justification, they prohibit anonymous speech, and punish anonymous speech even where there is no intent to deceive regarding the offer or information transmitted.

The provision requiring "identifiers" in H.R. 718 should be deleted. It is a form of prior restraint and compelled speech.

H.R. 718 additionally requires a conspicuous identifier be placed on unsolicited commercial electronic mail. The bill makes it unlawful to send UCE without the identifier. The ACLU opposes this provision because it is a form of prior restraint and "compelled speech."

A prior restraint consists of a government regulation that restricts or interferes with speech prior to its utterance. The Supreme Court has said that "[a]ny system of prior restraints of expression comes to this Court bearing a heavy presumption against its constitutional validity." Bantam Books v. Sullivan, 372 U.S. 58, 70 (1963).

Fundamental to the issue of labels or identifiers is that the First Amendment's protections include "both the right to speak freely and the right to refrain from speaking at all." *Wooley* v. *Maynard*, 430 U.S. 705, 714 (1977). It is a "fundamental principle that the coerced publication of particular views, as much as their suppression, violates the freedom of speech." *Herbert* v. *Lando*, 441 U.S. 153, 178 n.1 (1979)(Powell, J., concurring). The protections of the First Amendment encompass "the decision of both what to say and what not to say." *Riley* v. *National Federation of the Blind*, 487 U.S. 781, 797 (1988). "The First Amendment mandates that we presume that speakers, not the government, know best both what they want to say and how to say it." *Id.* at 790–791. By requiring an "identifier" on certain electronic mail, this bill forces senders to say something they may not wish to say, which is constitutionally suspect.

As noted above, a regulation of commercial speech must be narrowly tailored to achieve the asserted substantial government interest. Where the harm comes from the sheer volume, and inability to opt-out from receiving any further messages, this provision is not narrowly tailored to achieve the asserted substantial interest.

THE OVERALL EFFECT OF H.R. 718 MAY BE TO MAKE COMMERCIAL MAIL SO BURDENSOME IT OPERATES AS AN EFFECTIVE BAN ON SUCH COMMUNICATION. A BAN ON COMMERCIAL ELECTRONIC MAIL IS UNLIKELY TO BE UPHELD BY THE COURTS.

Section 5 (b) allows Internet service providers (ISPs) to set their own UCE policy and it gives those policies the force of federal law. A violation of any such a policy is subject to action by the Federal Trade Commission, as well as a civil action by the ISP.

There are approximately 6,000 Internet service providers in the United States. Under H.R. 718, *each* can set its own, different, policy and pricing scheme. Anyone who sends unsolicited commercial electronic mail will be faced with a nearly insurmountable burden to read and comply with each policy. A violation of even one policy can result in liability. The end result is that it will significantly chill protected speech—it will be too difficult, and the potential liability too great, to afford sending such mail.

Because H.R. 718 effectively bans UCE, it is likely a court would find it fails to narrowly tailor its solution as required by *Central Hudson* and *44 Liquormart*. Additionally, the result conflicts with Section 2 (a)(3) of the findings: "Unsolicited commercial electronic mail can be an important mechanism through which businesses advertise and attract customers in the online environment."

H.R. 1017 UNCONSTITUTIONALLY LIMITS FREE SPEECH BY PROHIBITING DISSEMINATION OF COMPUTER PROGRAMS THAT ENHANCE PRIVACY.

H.R. 1017 prohibits *any* unsolicited electronic mail, commercial or non-commercial, which knowingly and without authorization contains a false "Internet domain, header information, date or time stamp, originating e-mail address, or other identifier." It then further prohibits intentionally selling or distributing any computer program designed to protect the privacy of one sending email by falsifying that information.

---

[7] By subsequent agreement of the parties, the preliminary injunction was converted into a permanent injunction. No appeal was taken from the injunction. *American Civil Liberties Union of Georgia* v. *Barnes*, 68 F.3d 423 at 426 (11th Cir. 1999).

As noted above, there is a constitutional right to anonymous communication. H.R. 1017 clearly violates that right. But here, it goes even further, outlawing speech that may be used to guarantee that right.

Computer source code and software is protected expression under the First Amendment. *Junger* v. *Daley*, 209 F.3d 481 (6th Cir. 2000). The First Amendment affords broad protection to speakers, allowing even speech which advocates violation of the law. *Brandenburg* v. *Ohio*, 395 U.S. 444 (1969) ("[T]he constitutional guarantees of free speech and free press do not permit a State to forbid or proscribe advocacy of the use of force or of law violation except where such advocacy is directed to inciting or producing imminent lawless action and is likely to incite or produce such result.")

To outlaw speech because it may advocate or make possible a violation of the law flies in the face of constitutional precedent and turns the First Amendment on its head. Additionally, it sets a bad precedent. If something may be prohibited simply because it may be used to commit a crime, Congress and state legislatures *could* outlaw cars, guns, hammers, computers, and anything other item that could be used in the commission of a criminal offense.

CONCLUSION

While unsolicited commercial electronic mail, like paper junk mail, may be unwanted and annoying, the "short, though regular, journey from mail box to trash can . . . is an acceptable burden, at least so far as the Constitution is concerned." *Bolger* v. *Young's Drug Products Corp.*, 463 U.S. 60 (1983).

There is a considerable question of whether regulation of truthful unsolicited commercial electronic mail should be the subject of legislation, and whether new laws are needed to deal with such mail at all. H.R. 718 assumes the answer is in the affirmative, and attempts to ban unsolicited commercial electronic mail, while H.R. 1017 goes even further in regulating *all* unsolicited electronic mail. As H.R. 718 notes in its findings, "In legislating against certain abuses on the Internet, Congress should be very careful to avoid infringing *in any way* upon constitutionally protected rights, including the rights of assembly, free speech, and privacy." [Emphasis added.] There are significant constitutional concerns in both bills that need to be addressed before that goal may be achieved.