REDUCTION IN DISTRIBUTION OF SPAM ACT OF 2003

HEARING

BEFORE THE

SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY

OF THE

COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS

FIRST SESSION

ON

H.R. 2214

JULY 8, 2003

Serial No. 42

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

88–203 PDF WASHINGTON : 2003

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

COMMITTEE ON THE JUDICIARY

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

HENRY J. HYDE, Illinois
HOWARD COBLE, North Carolina
LAMAR SMITH, Texas
ELTON GALLEGLY, California
BOB GOODLATTE, Virginia
STEVE CHABOT, Ohio
WILLIAM L. JENKINS, Tennessee
CHRIS CANNON, Utah
SPENCER BACHUS, Alabama
JOHN N. HOSTETTLER, Indiana
MARK GREEN, Wisconsin
RIC KELLER, Florida
MELISSA A. HART, Pennsylvania
JEFF FLAKE, Arizona
MIKE PENCE, Indiana
J. RANDY FORBES, Virginia
STEVE KING, Iowa
JOHN R. CARTER, Texas
TOM FEENEY, Florida
MARSHA BLACKBURN, Tennessee

JOHN CONYERS, JR., Michigan
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
LINDA T. SÁNCHEZ, California

PHILIP G. KIKO, *Chief of Staff-General Counsel*
PERRY H. APELBAUM, *Minority Chief Counsel*

SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY

HOWARD COBLE, North Carolina, *Chairman*

TOM FEENEY, Florida
BOB GOODLATTE, Virginia
STEVE CHABOT, Ohio
MARK GREEN, Wisconsin
RIC KELLER, Florida
MIKE PENCE, Indiana
J. RANDY FORBES, Virginia

ROBERT C. SCOTT, Virginia
ADAM B. SCHIFF, California
SHEILA JACKSON LEE, Texas
MAXINE WATERS, California
MARTIN T. MEEHAN, Massachusetts

JAY APPERSON, *Chief Counsel*
SEAN MCLAUGHLIN, *Counsel*
ELIZABETH SOKUL, *Counsel*
KATY CROOKS, *Counsel*
PATRICIA DEMARCO, *Full Committee Counsel*
BOBBY VASSAR, *Minority Counsel*

CONTENTS

JULY 8, 2003

OPENING STATEMENT

	Page
The Honorable Howard Coble, a Representative in Congress From the State of North Carolina, and Chairman, Subcommittee on Crime, Terrorism, and Homeland Security	1
The Honorable Robert C. Scott, a Representative in Congress From the State of Virginia, and Ranking Member, Subcommittee on Crime, Terrorism, and Homeland Security	4

WITNESSES

The Honorable Jerry Kilgore, Attorney General of Virginia	
Oral Testimony	6
Prepared Statement	8
The Honorable William Moschella, Assistant Attorney General, Office of Legislative Affairs, United States Department of Justice	
Oral Testimony	13
Prepared Statement	15
Mr. Joseph S. Rubin, Senior Director of Public and Congressional Affairs and Executive Director of Technology and e-Commerce, United States Chamber of Commerce	
Oral Testimony	19
Prepared Statement	21
Mr. Chris Murray, Legislative Counsel, Consumers Union	
Oral Testimony	25
Prepared Statement	27

LETTERS, STATEMENTS, ETC., SUBMITTED FOR THE HEARING

Prepared Statement of the Honorable Howard Coble, a Representative in Congress From the State of North Carolina, and Chairman, Subcommittee on Crime, Terrorism, and Homeland Security	3

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

Prepared Statement of the Honorable Bob Goodlatte, a Representative in Congress From the State of Virginia	53
Prepared Statement of the Honorable Sheila Jackson Lee, a Representative in Congress From the State of Texas	54
Letter and Corrected Prepared Statement from William Moschella, Assistant Attorney General, Office of Legislative Affairs, United States Department of Justice	55
Letter from the American Civil Liberties Union (ACLU)	65

REDUCTION IN DISTRIBUTION OF SPAM ACT OF 2003

TUESDAY, JULY 8, 2003

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON CRIME, TERRORISM,
AND HOMELAND SECURITY
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Subcommittee met, pursuant to call, at 10 a.m., in Room 2141, Rayburn House Office Building, Hon. Howard Coble (Chair of the Subcommittee) presiding.

Mr. COBLE. Good morning, ladies and gentlemen. The Subcommittee on Crime, Terrorism, and Homeland Security is conducting a legislative hearing on H.R. 2214, the "Reduction in Distribution of Spam Act of 2003."

E-mail has been the primary driver of Internet usage. It has revolutionized the way people and businesses communicate with each other. E-mail has been heralded as the so-called "killer app." Now that is a trendy term, and I am not a very trendy guy, but I think technologists would know what I am talking about, an application that every computer user wants, has and uses. The increasing problem of unwanted e-mail or spam is threatening, as one observer put it, to, quote, kill the killer app, close quote. Recent studies suggest that 40 percent or more of all e-mail in the system is spam. Not long ago, spam was a mere annoyance, but its exponential growth may now be clogging the lanes of the information superhighway. No one likes spam, but the vexing challenge is, what can we do about it without causing unintended harms to the Internet and e-commerce?

The increased use of the Internet and e-mail for electronic commerce is certainly desirable. In fact, the Congress has encouraged, through such measures as e-signatures and various e-Government initiatives, the full use of the Internet to conduct e-commerce. E-mail, more than anything else, has been the most common way to facilitate e-commerce between buyers and sellers on the Internet.

Businesses also use e-mail, much like the regular mail to market their products and services. In fact, e-mail marketing is viewed by many as a necessary and valuable component of electronic commerce. The market efficiencies that the Internet can provide consumers is facilitated by notices, specials, discounts and other offers that are immediately accessible to a large number of prospective customers unbounded by geography. Furthermore, new Internet technologies can better target offers to those potential buyers with the greatest likely interest while avoiding those with little or no in-

terest. We should not lose sight of all these benefits as we grapple with the downside.

Unfortunately, the same things that make e-mail a great tool of commerce can also lead to abuse by those who send spam. E-mail is instantaneous and virtually free. There are no stamps in cyberspace, no per-message costs like there are, for example, in bulk mail. There is really not even a post office. The costs of delivery are borne more by the recipient and the transmission network than by the sender. Because of that nature, there is little difference in the marginal cost to a spammer of sending a thousand e-mail messages, for example, versus several million.

E-mail, like other means of communication, can be used to deceive, cheat, defraud and swindle consumers, but with much wider distribution possibilities. Spam is also a tool for the distribution of computer viruses. Additionally, some mass commercial e-mailers send pornography to unwilling recipients. Many spammers have become adept at fraudulent practices that conceal their identity and the type and route of their messages in order to evade detection.

Many Internet users have always found any unwanted e-mail to be intrusive and annoying, but more recently it is the volume of spam itself that is generating complaints and very real problems for users. Internet service providers, who operate the networks over which e-mail flows, and legitimate businesses who rely on getting their messages through are also concerned about the cumulative effects of massive amounts of unwanted e-mail. AOL, the largest Internet Service Provider, now is blocking over 780 million junk e-mails per day. Recent studies estimate that spam will cost businesses who use e-mail more than $10 billion in lost productivity this year. Spam is undermining consumer confidence in the utility of e-mail and harming the ability of consumers and businesses to conduct legitimate e-commerce.

There are already efforts under way by the Federal Trade Commission, by States and by ISPs to curb spam, but all these efforts clearly have their limitations. The question before us today is whether the spam problem has risen to a level that merits Federal legislation and whether such Federal legislation or regulation can be effective without causing unintended harm to e-commerce.

H.R. 2214 was introduced by Mr. Burr, Mr. Sensenbrenner, Mr. Tauzin, Mr. Goodlatte, Mr. Upton, Ms. Hart and Mr. Stearns and Mr. Cannon on 22 May of this year. The bill is intended to curb the rising tide of unsolicited commercial e-mail—UCE—or spam by giving consumers more power to identify and decline unwanted commercial e-mail and by giving law enforcement and providers of Internet access service more tools to pursue and stop spammers.

Title II of the bill in particular amends title 18 of the U.S. Code to provide significant criminal penalties and civil fines for the most egregious senders of spam—those who intentionally falsify their identity and the source of their messages, attack protected computers, harvest the addresses of unsuspecting Internet users and send unwanted sexually explicit materials.

I look forward to hearing the testimony from our witnesses about the problem of spam and the potential help this legislation can provide.

I am now pleased to recognize the distinguished gentleman from Virginia, the Ranking Member Mr. Bobby Scott.

[The prepared statement of Mr. Coble follows:]

PREPARED STATEMENT OF THE HONORABLE HOWARD COBLE, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NORTH CAROLINA

Good Morning. Today the Subcommittee on Crime, Terrorism, and Homeland Security is holding a legislative hearing on H.R. 2214, the "Reduction in Distribution of Spam Act of 2003."

E-mail has been the primary driver of Internet usage. It has revolutionized the way people and businesses communicate with each other. E-mail has been heralded as the so called "killer app," an application that virtually every computer user wants, has, and uses. But the increasing problem of unwanted e-mail or "spam" is threatening, as one observer put it, to "kill the killer app." Recent studies suggest that 40% or more of all e-mail in the system is spam. Not long ago spam was a mere annoyance, but its exponential growth may now be clogging the lanes of the information superhighway. No one likes spam but the vexing challenge is what can we do about it without causing unintended harms to the Internet and E-commerce?

The increased use of the Internet and e-mail for electronic commerce is certainly desirable. In fact, the Congress has encouraged, through such measures as E-Signatures and various E-Government initiatives, the full use of the Internet to conduct "E-commerce." E-mail, more than anything else, has been the most common way to facilitate E-commerce between buyers and sellers on the Internet.

Businesses also use e-mail, much like the regular mail, to market their products and services. In fact, e-mail marketing is viewed by many as a necessary and valuable component of electronic commerce. The market efficiencies that the Internet can provide consumers is facilitated by notices, specials, discounts, and other offers that are immediately accessible to a large number of prospective customers unbounded by geography. Furthermore, new Internet technologies can better target offers to those potential buyers with the greatest likely interest while avoiding those with little interest. We should not lose sight of all these benefits as we grapple with the downside.

Unfortunately, the same things that make e-mail a great tool of commerce can also lead to abuse by those who send spam. E-mail is instantaneous and virtually free, there are no stamps in cyberspace, no per message costs like there are for bulk mail—there's really not even a post office. The costs of delivery are borne more by the recipient and the transmission network than by the sender. Because of that nature, there is little difference in the marginal cost to a spammer of sending a thousand e-mail messages versus 100 million.

E-mail, like other means of communication, can be used to deceive, cheat, defraud, and swindle consumers, but with much wider distribution possibilities. Spam is also a tool for the distribution of computer viruses. Additionally, some mass commercial e-mailers send pornography to unwilling recipients. Many spammers have become adept at fraudulent practices that conceal their identity and the type and route of their messages in order to evade detection.

Many Internet users have always found any unwanted e-mail to be intrusive and annoying, but more recently it is the volume of spam itself that is generating complaints and very real problems for users. Internet Service Providers, who operate the networks over which e-mail flows, and legitimate businesses who rely on getting their messages through are also concerned about the cumulative effects of massive amounts of unwanted e-mail. AOL, the largest Internet Service Provider, is now blocking over 780 million junk e-mails per day. Recent studies estimate that spam will cost businesses who use e-mail more than $10 Billion in lost productivity this year. Spam is undermining consumer confidence in the utility of e-mail and harming the ability of consumers and businesses to do conduct legitimate E-commerce.

There are already efforts under way by the Federal Trade Commission, by states, and by ISPs to curb spam—but all these efforts clearly have their limitations. The question before us today is whether the spam problem has risen to a level that merits federal legislation, and whether such federal legislation can be effective without over-regulating the Internet?

H.R. 2214 was introduced by Mr. Burr, Mr. Sensenbrenner, Mr. Tauzin, Mr. Goodlatte, Mr. Upton, Ms. Hart, Mr. Stearns, and Mr. Cannon on May 22, 2003. The bill is intended to curb the rising tide of unsolicited commercial e-mail ("UCE") or "spam" by giving consumers more power to identify and decline unwanted commercial email and by giving law enforcement and providers of internet access service more tools to pursue and stop spammers.

Title II of the bill in particular amends Title 18 of the U.S. Code to provide significant criminal penalties and civil fines for the most egregious senders of spam—those who intentionally falsify their identity and the source of their messages, attack protected computers, harvest the addresses of unsuspecting internet users, and send unwanted sexually explicit materials.

I look forward to hearing the testimony of the witnesses about the problem of spam and the potential help this legislation can provide.

I would now recognize Mr. Scott for an opening statement.

Mr. SCOTT. Thank you, Mr. Chairman. I want to thank you for holding the hearing on H.R. 2214, the Reduction in Distribution, or RID, Spam Act.

All Internet users experience the problem we call spam. There are many definitions. To a large extent it is in the eye of the beholder, ranging from passing around jokes and chain letters to our families, friends and associates to bulk commercial e-mail. The primary components of spam are that it is unwanted and unsolicited. Add to this the problem of volume, intrusiveness and adding such things as cookies to your computer and popping up while you are in the middle of using the Internet, the cost of taking up space as well as having to take the time to delete the e-mail, and we have a problem with spam.

Unsolicited and unwanted e-mails from families, friends and associates can be easily handled by gentle or not-so-gentle requests not to send it, so no law is needed to address that aspect of spam. The annoyance of such e-mail is simply part of the price we pay for an Internet-based principles for universal access and freedom.

The procedures for preventing or stopping unsolicited bulk commercial e-mail have been increasingly inadequate, while the volume has increased exponentially. It takes substantial time, energy, expertise and increasingly more sophistication to develop products to address it. The average Internet user is not able to address it and is spending a lot of time just simply erasing the bulk e-mail.

Estimates indicate that as much as 45 percent of e-mail traffic consists of this bulk unsolicited commercial e-mail. Moreover, much of this commercial e-mail contains either fraudulent, misleading or pornographic material. Increasingly, Internet users are defrauded of money or otherwise scammed by unscrupulous marketers. This is the type of spam the bill before us seeks to address.

I look forward to our witnesses and how this problem can be effectively and efficiently dealt with. While I support the effort to restrict spam on the Internet in a matter similar to the way we found effective in addressing abusive unsolicited commercial communications through mails and telephone, I am concerned about the superfluous provisions in the bill such as preventing class actions and restricting attorneys' fees and providing consumers with an opt-out rather than opt-in choice. Some of those may actually may hinder our efforts, rather than help. I am also not sure whether the bill before us rather than some other bills are the best way to address the issue.

I also want to take a close look at the bill as we mark it up to be sure that we define our narrowly targeted—that we define the problem narrowly tailored enough to make sure that we don't trample on the Constitution. Even commercially sponsored e-mail does have some first amendment protection. Just because e-mails come from a business doesn't mean that the content is unprotected. So

we want to make sure that what we are targeting is the unprotected speech under the first amendment.

So, Mr. Chairman, I thank you and look forward to the witnesses who will be testifying before us.

Mr. COBLE. I thank you, Mr. Scott.

We have an outstanding panel today, and Mr. Scott has requested the privilege to introduce his Attorney General. I am pleased to recognize Mr. Scott.

Mr. SCOTT. Thank you, Mr. Chairman.

Our first witness is the distinguished Attorney General from the Commonwealth of Virginia, Jerry Kilgore. He was elected Virginia's 42nd Attorney General on November 6, 2001, receiving more than 60 percent of the vote. Prior to his election as Attorney General, he served in the Cabinet of former Governor George Allen, as the Secretary of Public Safety.

He has served on the front lines of law enforcement as an Assistant Commonwealth's Attorney for Scott County, Virginia, and as Assistant U.S. Attorney for the Western District of Virginia. He received his law degree from the Marshall Witt School of Law at the College of William and Mary and is a graduate of the University of Virginia's college at Wise.

And, Mr. Chairman, it wasn't part of his official bio, but I would want to point out that he has done a lot of work in the problem of identity theft. It is one of the problems we are dealing with, and we may want to take advantage of his expertise in that area as well as in the future.

Mr. COBLE. Thank you, Mr. Scott; and, Attorney General, good to have you with us. Good to have all the witnesses, and permit me now to introduce the remaining members of the panel.

Our next witness is the Honorable William Moschella, Assistant Attorney General for the Office of Legislative Affairs for the U.S. Department of Justice. Attorney General Moschella is a familiar face to the Judiciary Committee as he most recently served as its Chief Legislative Counsel and Parliamentarian. He also served as Chief Investigative Counsel for the Committee from 1999 through 2001, as General Counsel for the House Rules Committee in 1999 and with the House Government Reform Committee. Assistant Attorney General Moschella received his juris doctorate from the George Mason University School of Law and his bachelor degree from the University of Virginia.

Good to have you back on the Hill, Will. I think I inadvertently promoted you to Attorney General, but don't tell Mr. Ashcroft that.

Our third witness will be Mr. Joe Rubin, the Senior Director for Public and Congressional Affairs and the Executive Director for Technology and E-commerce at the United States Chamber of Commerce. The U.S. Chamber of Commerce is the world's largest business federation, representing more than 3 million businesses of every size, sector and region in the country. Mr. Rubin serves as liaison between the U.S. Chamber of Commerce and the Administration.

Mr. Rubin, not unlike Mr. Moschella, is no stranger to this Committee. Prior to joining the Chamber, Joe was Legislative Director for Congressman George Gekas from Pennsylvania and Legislative Counsel for Congressman Steve Chabot of Ohio where he handled

Judiciary Committee issues. Mr. Rubin obtained his doctorate from the Emory School of Law and is a graduate of the University of Maryland.

Our final witness, Mr. Chris Murray, is the Legislative Counsel for the Consumers Union, with an expertise in technology, communications, media policy and intellectual property issues. Consumers Union, the publisher of Consumer Reports, is an independent nonprofit testing and information organization serving only consumers as a source of advice about products and services.

Before joining Consumers Union, Mr. Murray was a Ford Foundation Media Arts and Cultural Fellow for 2 years, focusing on broadband and telecommunications issues. Mr. Murray worked with the firm Leslie Harris and Associates for clients such as the American Library Association and America Online. Mr. Murray is a graduate of Florida Southern College and received his law degree from Georgetown University.

It is good to have all of you with us; and I will note at the outset that Attorney General Kilgore, although we are fortunate to have him—because I think you are scheduled to be in northern Virginia later, Mr. Kilgore, and I think you have to leave on or about 11 o'clock. So if we don't get to examine Mr. Kilgore as thoroughly as we would like to, I am sure you would be open to written questions submitted to you, Mr. Kilgore.

I am pleased to indicate that we have been joined by the gentleman from California, gentlemen from Florida, Ohio and Wisconsin. Good to have you with us.

Mr. SCOTT. Mr. Chairman, I am notified that Congresswoman Jackson Lee is unable to attend today's hearing because she is in Houston, TX, at the funeral of a constituent who died while serving his country in Operation Iraqi Freedom.

Mr. COBLE. Thank you, sir.

Mr. Kilgore, we will start with you; and, gentlemen, let me assure you, Mr. Scott and I try to operate on the 5-minute rule here. When you see that red light illuminate in your face, we will not send a U.S. Marshal after you, but you will know that the ice is becoming thin.

So, Mr. Kilgore, for 5 minutes.

STATEMENT OF THE HONORABLE JERRY W. KILGORE, ATTORNEY GENERAL OF VIRGINIA

Mr. KILGORE. Thank you, Mr. Chairman, and thank you, Mr. Scott, for that kind introduction. It is great to be before this Committee.

Virginia is the Internet capital of the world. More than half of all the Internet traffic in the world runs through Virginia, and more than half of all the Internet access to business and individuals is provided by Virginia companies. As you consider Federal anti-spam legislation, H.R. 2214, I am pleased to be able to address your Committee today on Virginia's anti-spam law that went into effect just 7 days ago.

It was not too long ago that none of us had heard of e-mail. But now we can't live without it. Anyone who has e-mail now knows about spam, that frustrating, unwanted e-mail that shows up everyday by the dozens or hundreds in your computer's in-box.

The proliferation of spam has becoming increasingly frustrating to both users and the Internet Service Providers, also known as ISPs. Spam is technically defined as unsolicited bulk e-mail, UBE, or unsolicited commercial e-mail, UCE. Spam aggravates the average user and costs businesses millions of dollars in lost revenues. Virginia is home to many ISPs. Each day these ISPs are forced to use expensive technology and commit countless manpower hours to combat the millions of pieces of spam that are transmitted through these services. This spam is not only annoying, sometimes it is obscene. Spam has a direct, negative impact on the efficiency and effectiveness of the free enterprise system and day-to-day operations of business.

We live in a world that relies more and more on technology. In my office, we rely on technology a great deal, especially when time sensitive information is of concern; and spam certainly throws wrenches into that technology.

Billions of pieces of bulk e-mail are sent every second of the day. While the Internet and technology are meant to improve the quality of our lives, many hours of stress are expended because of this problem. Deals can be lost and even jobs are lost because smaller ISPs simply cannot survive the toll spam provides.

Virginia has had laws that attempted to deal with the growing problem of spam since 1999. The Virginia General Assembly amended the statutes defining crimes such as computer fraud, computer trespass and theft of computer services in recent years. These revisions attempted to cover the sending of unsolicited bulk e-mail and created a civil relief section that gave both consumers and the ISP the right to sue spammers for actual or statutory damages. These laws have been effectively used by Internet Service Providers to sue spammers from all over the country for violations. In fact, my office has twice successfully defended the constitutionality of Virginia's anti-spam law and Virginia's long-arm statute that allows Virginia courts to exercise jurisdiction over out-of-State spammers.

Although the laws were somewhat effective, we recognized the growing need to toughen Virginia's computer crime laws in relation to the transmission of spam. We found that spammers were paying the civil damages or mere criminal fines assessed against them but were continuing with their destructive behavior. They chalked it up to the cost of doing business. The threat of civil lawsuits and misdemeanor convictions was not enough.

In our pursuit, we also examined the labeling laws many other States have enacted. Most of these laws require spammers to identify e-mail messages as containing advertisements, ADV, or adult material, ADT. These laws have shown to be somewhat ineffective as well in that they are based on the false premise that spammers are law-abiding advertisers.

After spending a great deal of work over the summer of 2002 working with both consumers and the Virginia Internet Service Providers Alliance, we were able to come up with legislation that punished spammers as felons when they employed such fraudulent means as forging and falsifying routing information. I am grateful that the Virginia General Assembly passed this important anti-spam legislation.

We give new provisions in the criminal code of Virginia which prohibits the forging or falsification of e-mail transmission and that is not unlike the Federal legislation that is before you. I am pleased that so many of our concerns and the concerns of my fellow attorneys general have been taken into account in this proposed Federal statute and preemption is no longer a concern and that you will no longer preempt State attorneys general and State general assemblies from passing tough laws against spam.

The majority of spam is transmitted using fraudulent means so that the recipient cannot determine where it came from and cannot ask to be removed from this mailing list. They sometimes also use special software that protects them from being tracked. Our law ensures that those spammers that joyride on accounts that don't belong to them will be held accountable for those acts. These tougher criminal penalties will serve as a deterrent to many spammers who considered the civil damages of the past a cost of doing business.

There are many conditions to charging felonies in Virginia, and those are included in Virginia's act, and they are included in my written testimony.

This new anti-spam law also includes new sections which provides for asset seizure and forfeiture for all monies and other income and proceeds earned as a result of the violation of this law and all computer equipment, all the software and personal property used in connection with this spamming operation.

Our new law went into effect just 7 days ago, on July 1; and my new Computer Crime Unit has already begun working with consumers and ISPs to investigate those who are violating Virginia's laws.

Thank you for allowing me to be with you this morning.

Mr. COBLE. Thank you, Mr. Attorney General.

[The prepared statement of Mr. Kilgore follows:]

PREPARED STATEMENT OF JERRY W. KILGORE

Mr. Chairman and members of this distinguished committee, I am Jerry Kilgore, Attorney General of Virginia. Virginia is the Internet Capital of the World. More than half of all Internet traffic in the world runs through Virginia, and more than half of all Internet access to business and individuals is provided by Virginia companies. As you consider federal anti-Spam legislation, HR 2214, I am pleased to be able to address your committee today on Virginia's Anti-SPAM law that went into effect seven days ago.

It was not too long ago that no one had ever heard of e-mail. But now, who among us can live without it? Anyone who has e-mail certainly knows about SPAM. It is that frustrating, unwanted e-mail that shows up every day by the dozens . . . or hundreds . . . in your computer's in-box.

The proliferation of SPAM has become increasingly frustrating to both users of the Internet and Internet Service Providers, also known as ISP's. SPAM is technically defined as unsolicited bulk email, "UBE," or unsolicited commercial email, "UCE." SPAM aggravates the average user and it costs businesses millions of dollars in lost revenue. Virginia is home to many Internet Service Providers. Each day, these ISP's are forced to use expensive technology and commit countless manpower hours to combat the millions of pieces of SPAM that are transmitted through their servers. This SPAM is not only annoying but often also obscene. SPAM has a direct, negative impact on the efficiency and effectiveness of the free enterprise system and day-to-day operations of business.

We live in a world that relies more and more on technology. In my office, we rely on technology a great deal—especially where time-sensitive information is of concern. But SPAM can throw a wrench into receiving this information. Even if I have

my Blackberry with me, SPAM makes the transmission cumbersome for the ISP—thereby slowing down the transmittal rate.

Billions of pieces of bulk e-mail are sent each second of the day. While the Internet and technology are meant to improve the quality of our lives—many hours of stress are expended because of this problem. Deals can be lost and even jobs are lost because smaller ISPs can't survive the toll SPAM exacts.

Virginia has had laws that attempted to deal with the growing problem of SPAM since 1999. The Virginia legislature amended the statutes defining crimes such as "Computer Fraud," "Computer Trespass," and "Theft of Computer Services" in recent years. These revisions attempted to cover the sending of unsolicited bulk email, and created a civil relief section that gave both consumers and the ISP's the right to sue the Spammers for actual or statutory damages. These laws have been effectively used by the Internet Service Providers to sue Spammers from all over the country for violations. In fact my office has twice successfully defended the constitutionality of Virginia's anti-SPAM laws and Virginia's long-arm statute that allows Virginia courts to exercise jurisdiction over out-of-state Spammers.

Although the laws that were in place had been somewhat effective, my office recognized the growing need to toughen Virginia's computer crime laws in reference to the transmission of SPAM. We found that Spammers were paying the civil damages, or mere criminal fines assessed against them, but were continuing their destructive behavior. They chalked up those damages or fines as a cost of doing business. The threat of civil lawsuits or misdemeanor convictions was not enough to deter them.

In our pursuit to further combat the problem of SPAM, my office studied the "labeling laws" many other states had enacted. Most of these laws require Spammers to identify the e-mail messages as containing advertisements, "ADV," or adult material, "ADT." These laws have been shown to be somewhat ineffective in that they are based on the false premise that most Spammers are merely law-abiding advertisers.

After spending a great deal of the summer of 2002 working with both consumers and the Virginia Internet Service Providers Alliance, which represents all of the ISP's located within Virginia, I sponsored legislation that would punish Spammers as felons when they employed such fraudulent means as forging and falsifying routing information. I am grateful that in this past session of Virginia's General Assembly, my ANTI-SPAM legislation was adopted.

The law, which has been touted as the toughest in the nation, provides a new separate provision in the criminal code of Virginia, which prohibits the forging or falsification of e-mail transmission information used to facilitate the sending of SPAM. This is not unlike the federal legislation before you. I am pleased that some of my concerns, along with many other Attorneys General, about the proposed federal statute's preemption of Virginia's criminal statute relating to SPAM have been addressed. The majority of SPAM is transmitted using fraudulent means so that the recipient cannot determine the sender or ask to be removed from the mailing list.

Spammers often use special software designed to protect them from being tracked. Our law ensures that the Spammer who joyrides on accounts that do not belong to him will be held accountable for that act. In fact, such a Spammer can now be punished as a felon when he uses such fraudulent means to send SPAM. This tougher criminal penalty will serve as a deterrent to many Spammers who consider the civil damages that they have been ordered to pay as a mere cost of doing business.

There are three conditions, which raise the violation of sending SPAM using fraudulent means to a felony. The conditions are triggered when the volume of SPAM transmitted exceeds 10,000 attempted recipients in any 24-hour period, 100,000 attempted recipients in any 30-day time period, or one million attempted recipients in any one-year time period; or when the revenue generated from a specific SPAM transmission exceeds $1,000 or the total revenue generated from all SPAM transmitted to any ISP exceeds $50,000; or if the Spammer knowingly hires, employs, uses, or permits any minor to assist in the transmission of the SPAM.

Another first in the nation in computer crime law was enacted with our new provision concerning fraudulent SPAM containing obscenity. It will also now be a violation of our Virginia Computer Crimes Act for Spammer to use a computer in spamming operations in connection with a violation of obscenity laws. An initial offense of this nature is a Class 1 Misdemeanor and a second offense is now a Class 6 Felony.

The new anti-SPAM law also includes a new section which provides for the seizure and forfeiture of all moneys and other income and proceeds earned as a result of violations of the law, and all computer equipment, all computer software, and all personal property used in connection with any violation of the law.

Our new law went into effect just seven days ago, on July 1st and my Computer Crime Unit has already begun to work with consumers and the ISP's to investigate

and prosecute violations. In fact, this new anti-SPAM law is one of many computer laws that my office has been authorized by the legislature to prosecute. I am certain that our law will benefit every Virginia resident who uses the Internet and has an e-mail account, and many Americans who benefit from Virginia's technology crescent.

Thank you very much and I am happy to answer any questions you may have.

ATTACHMENT

COMMONWEALTH OF VIRGINIA'S SPAM STATUTE

§ 18.2-152.3:1. Transmission of unsolicited bulk electronic mail (spam); penalty.

A. Any person who:
   1. Uses a computer or computer network with the intent to falsify or forge electronic mail transmission information or other routing information in any manner in connection with the transmission of unsolicited bulk electronic mail through or into the computer network of an electronic mail service provider or its subscribers; or
   2. Knowingly sells, gives, or otherwise distributes or possesses with the intent to sell, give, or distribute software that (i) is primarily designed or produced for the purpose of facilitating or enabling the falsification of electronic mail transmission information or other routing information; (ii) has only limited commercially significant purpose or use other than to facilitate or enable the falsification of electronic mail transmission information or other routing information; or (iii) is marketed by that person acting alone or with another for use in facilitating or enabling the falsification of electronic mail transmission information or other routing information is guilty of a Class 1 misdemeanor.

B. A person is guilty of a Class 6 felony if he commits a violation of subsection A and:
   1. The volume of UBE transmitted exceeded 10,000 attempted recipients in any 24-hour period, 100,000 attempted recipients in any 30-day time period, or one million attempted recipients in any one-year time period; or
   2. The revenue generated from a specific UBE transmission exceeded $1,000 or the total revenue generated from all UBE transmitted to any EMSP exceeded $50,000.

C. A person is guilty of a Class 6 felony if he knowingly hires, employs, uses, or permits any minor to assist in the transmission of UBE in violation of subdivision B 1 or subdivision B 2.

(2003, cc. 987, 1016.)

§ 18.2-152.12. Civil relief; damages.

A. Any person whose property or person is injured by reason of a violation of any provision of this article may sue therefor and recover for any damages sustained and the costs of suit. Without limiting the generality of the term, "damages" shall include loss of profits.

B. If the injury under this article arises from the transmission of unsolicited bulk electronic mail in contravention of the authority granted by or in violation of the policies set by the electronic mail service provider where the defendant has knowledge of the authority or policies of the EMSP or where the authority or policies of the EMSP are available on the electronic mail service provider's website, the injured person, other than an electronic mail service provider, may also recover attorneys' fees and costs, and may elect, in lieu of actual damages, to recover the lesser of $10 for each and every unsolicited bulk electronic mail message transmitted in violation of this article, or $25,000 per day. The injured person shall not have a cause of action against the electronic mail service provider that merely transmits the unsolicited bulk electronic mail over its computer network. Transmission of electronic mail from an organization to its members shall not be deemed to be unsolicited bulk electronic mail.

C. If the injury under this article arises from the transmission of unsolicited bulk electronic mail in contravention of the authority granted by or in violation of the policies set by the electronic mail service provider where the defendant has knowledge of the authority or policies of the EMSP or

where the authority or policies of the EMSP are available on the electronic mail service provider's website, an injured electronic mail service provider may also recover attorneys' fees and costs, and may elect, in lieu of actual damages, to recover $1 for each and every intended recipient of an unsolicited bulk electronic mail message where the intended recipient is an end user of the EMSP or $25,000 for each day an attempt is made to transmit an unsolicited bulk electronic mail message to an end user of the EMSP. In calculating the statutory damages under this provision, the court may adjust the amount awarded as necessary, but in doing so shall take into account the number of complaints to the EMSP generated by the defendant's messages, the defendant's degree of culpability, the defendant's prior history of such conduct, and the extent of economic gain resulting from the conduct. Transmission of electronic mail from an organization to its members shall not be deemed to be unsolicited bulk electronic mail.

D. At the request of any party to an action brought pursuant to this section, the court may, in its discretion, conduct all legal proceedings in such a way as to protect the secrecy and security of the computer, computer network, computer data, computer program and computer software involved in order to prevent possible recurrence of the same or a similar act by another person and to protect any trade secrets of any party and in such a way as to protect the privacy of nonparties who complain about violations of this section.

E. The provisions of this article shall not be construed to limit any person's right to pursue any additional civil remedy otherwise allowed by law.

F. A civil action under this section must be commenced before expiration of the time period prescribed in § 8.01-40.1. In actions alleging injury arising from the transmission of unsolicited bulk electronic mail, personal jurisdiction may be exercised pursuant to § 8.01-328.1.

(1984, c. 751; 1985, c. 92; 1999, cc. 886, 904, 905; 2003, cc. 987, 1016.)

§ 18.2-152.16. Forfeitures for violation of this article.

All moneys and other income, including all proceeds earned but not yet received by a defendant from a third party as a result of the defendant's violations of this article, and all computer equipment, all computer software, and all personal property used in connection with any violation of this article known by the owner thereof to have been used in violation of this article, shall be subject to lawful seizure by a law-enforcement officer and forfeiture by the Commonwealth in accordance with the procedures set forth in Chapter 22.1 (§ 19.2-386.1 et seq.) of Title 19.2, applied mutatis mutandis.
(2003, cc. 987, 1016.)

§ 18.2-376.1. Enhanced penalties for using a computer in certain violations.

Any person who uses a computer in connection with a violation of §§ 18.2-374, 18.2-375, or § 18.2-376 is guilty of a separate and distinct Class 1 misdemeanor, and for a second or subsequent such offense within 10 years of a prior such offense is guilty of a Class 6 felony, the penalties to be imposed in addition to any other punishment otherwise prescribed for a violation of any of those sections.
(2003, cc. 987, 1016.)

Source: ***Code of Virginia***

Mr. COBLE. Mr. Moschella.

STATEMENT OF THE HONORABLE WILLIAM MOSCHELLA, ASSISTANT ATTORNEY GENERAL, OFFICE OF LEGISLATIVE AFFAIRS, UNITED STATES DEPARTMENT OF JUSTICE

Mr. MOSCHELLA. Thank you, Mr. Chairman, Mr. Scott and Members of the Subcommittee. Thank you for inviting me to testify today about the Justice Department's views on H.R. 2214.

Like you, the Department has received an increasing number of letters and calls from citizens complaining about the number of unsolicited electronic mail appearing in their mailboxes and the potentially fraudulent, dangerous or obscene content of those electronic mails. We have been in discussions with Internet Service Providers who tell us that the amount of spam they are handling continues to increase. We are hearing clearly that people simply are fed up with the unwanted mail offering pornography, untested medications and shady financial deals clogging their inboxes.

When consumers throw up their hands at their electronic mailbox and when providers pass increased costs of spam onto their customers, the benefits of electronic commerce facilitated by the Internet will diminish. This would be unacceptable.

At the same time, Congress must be careful about adopting too much regulation in this area or instituting an inflexible regime which could threaten the openness and success of the Internet. Our policy toward the Internet from its significant commercialization in the early 1990's has been to encourage electronic commerce to grow in accord with the Internet's open architecture and have preferred technology-based and market-driven solutions. Accordingly, we support efforts that will target the problem of unsolicited commercial e-mail, particularly e-mail designed to facilitate consumer fraud or unwanted transmission of pornography while not harming legitimate marketers sending electronic mail that a customer wants to read. We encourage the Subcommittee and Congress as a whole to pursue these goals when drafting legislation in this area.

While we believe that the Department of Justice can play a supporting role in addressing the spam problem, we of course do not believe that the problem can be adequately addressed by a single approach or single agency. Indeed, it is not a problem Government can be expected to solve by itself. We believe strongly that criminal prosecution will be a very small part of a larger cooperative initiative. It is a backstop to the civil, administrative and market-based remedies that form a larger part of the solution. The role of the criminal justice system in addressing this problem should be appropriately limited to those offenders who are affirmatively hiding their identities and who are sending out unsolicited e-mail with unmarked sexually explicit content. Moreover, our prosecutions should focus on the most egregious violators who are involved in sending thousands of spam messages every day.

The Justice Department believes that it can play an important part in this broad response to the problem of unsolicited commercial e-mail. We believe that criminal sanctions are appropriate when a marketer has knowingly lied about his or her identity when sending out such e-mail. Spammers don't want to put true identifying information on its commercial mail because they don't want

to have their mail filtered, hear from irate recipients or lose their connection to their Internet because they have violated their contract with their provider. At worst, these marketers do not want to be contacted because they are actively engaging in fraud by advertising illegal items or schemes and want to hide from investigators and victims.

We believe that deterring the knowing use of fraudulent identifying information will assist both users and Internet Service Providers in fighting spam. With accurate identifying information, users can contact marketers to tell them that they no longer wish to receive the spam and they can tell whether those requests are being honored. Similarly, with accurate identifying information, providers can better identify and, when appropriate, filter traffic from persons who are crippling their networks or generating hundreds or thousands of complaints due to spam.

In fact, in testimony on May 21 of this year before the Senate Commerce Committee, Ronald Scelson, a self-proclaimed spammer who claimed responsibility for sending approximately 180 million spam e-mails per day, indicated that he intentionally forged headers precisely so that he would avoid being shut down by his service provider due to customer complaints. Creating a criminal offense to address the worst behavior will allow law enforcement in appropriate cases to work with providers to identify those responsible for this sort of activity and subject them to prosecution.

Similarly, we believe we can assist in deterring one of the most common and significant complaints about spam—people receiving unsolicited messages containing sexually oriented contact. Requiring marking of that sexually explicit content in unsolicited mail and enforcing that requirement with a criminal deterrent can help individuals and parents filter out electronic mail they are likely to find particularly offensive.

Mr. Chairman, the Department supports H.R. 2214's general approach to criminal penalties. We believe that criminalizing this egregious conduct that I discussed at the felony level is appropriate for several reasons.

First, it will help to ensure these cases will be investigated and prosecuted in the field as investigators and prosecutors simply lack resources or the incentives to spend weeks tracking down a spammer for a misdemeanor offense.

Second, it will provide prosecutors with the necessary tools to investigate these cases, as some Federal investigative tools are reserved solely for felony offenses.

Third, it places the United States in a position of being able to seek and receive international assistance in this area in the future as international treaties, law and practice often restricts certain types of assistance to cases in which both countries criminalize the conduct at the felony level.

Mr. Chairman, my written statement contains some specific suggestions for the criminal provisions which I will be happy to discuss; and I appreciate the opportunity to testify.

Mr. COBLE. Thank you, Mr. Moschella.

[The prepared statement of Mr. Moschella follows:]

PREPARED STATEMENT OF WILLIAM E. MOSCHELLA

Mr. Chairman and Members of the Subcommittee:

Thank you for inviting me to testify today. My name is William Moschella and I am the Assistant Attorney General for Legislative Affairs at the Department of Justice. I thank the Subcommittee for holding this hearing on H.R. 2214, the "Reduction in Distribution of Spam Act" or "RID SPAM Act". I commend Chairman Sensenbrenner, Chairman Tauzin, Representative Burr, and all of the other co-sponsors of the legislation for taking steps to address this issue, and I am pleased to be able to discuss the Justice Department's views on that bill with you today.

I. A FRAMEWORK FOR ADDRESSING THE SPAM PROBLEM

Over the last few years, the Department has received an increasing number of letters and calls from citizens complaining about the amount of unsolicited electronic mail appearing in their mailboxes and the potentially fraudulent, dangerous, or obscene content of those electronic mails. We have been in discussions with Internet service providers who tell us that the amount of spam they are handling continues to increase—often doubling or tripling in a matter of months. We are hearing clearly that people simply do not want to wade through unwanted e-mail offering pornography, untested medications, and shady financial deals to hear news from their daughter in college, find out that their order has been shipped from an e-commerce site, or receive offers that they have sought from legitimate marketers.

This is a key element of the problem that we are discussing today—spam deters electronic commerce and communication because it makes consumers less likely and less able to use the Internet for legitimate business. People stop signing up for offers and mailings from legitimate merchants because they fear that their e-mail address will be sold or stolen and instead of getting useful information that they want—like movie times in their community or last-minute airfare deals from an airline—they'll get unwanted pitches from spam marketers. When consumers throw up their hands at their electronic mailbox and when providers are forced to pass increased costs of spam filtering on to their customers because they are taking in more unwanted spam than legitimate mail, the benefits of electronic commerce facilitated by the Internet will diminish. This would be unacceptable.

At the same time, adopting too much regulation in this area or instituting an inflexible regime regulating all commercial electronic mail also threatens the openness and success of the Internet. Our policy toward the Internet from its first significant commercialization in the early 1990s has been to favor solutions that do not restrict progress with overbroad regulation. Thus far, we have encouraged electronic commerce to grow in accord with the Internet's open architecture and have preferred technology-based and market-driven solutions. This policy has served us well to this point and we do not advocate changing that formula. Instead, we support efforts that will target the problem of unsolicited commercial e-mail, particularly e-mail designed to facilitate consumer fraud or unwanted transmission of pornography, while not harming legitimate marketers sending electronic mail that their customers want to read. We encourage the Subcommittee and Congress as a whole to pursue these goals when crafting legislation in this area.

II. THE JUSTICE DEPARTMENT'S COMMITMENT TO HELPING FIGHT THE SPAM PROBLEM

While we believe that the Department of Justice can play a supporting role in addressing the spam problem, we of course do not believe that the problem can be adequately addressed by any single approach or any single agency. Indeed, it is not a problem that government can be expected to solve by itself. We believe strongly that criminal prosecution will be a very small part of a larger cooperative initiative; it is a backstop for the civil, administrative, and market-based remedies that form a larger part of the regime. The role of the criminal justice system in addressing this problem should be appropriately limited to those offenders who are affirmatively hiding their identities or who are sending out unsolicited e-mail with unmarked sexually explicit content. Moreover, our prosecutions should focus on the most egregious violators who are involved in sending thousands of spam messages every day. In keeping with the balanced framework that we recommend for addressing the overall issue, the powerful deterrence of criminal law neither should interfere with the dynamic growth of the Internet and electronic commerce nor should it chill legitimate speech.

Moreover, the Government's efforts to combat unlawful spam will require continued and increased cooperation with users and network providers. It will also require approaching other countries for assistance, because even though we believe that a large percentage of spam begins in the United States and is targeted at the United

States, spammers often route their spam through other countries in order to further hide their tracks. Spam will not be stopped by law alone, but by a combination of solutions: Criminal prosecution for the very worst offenders; civil and administrative remedies against those who cause harm by failing to follow the rules of the road for e-mail marketing; continued technological development to assist network providers and users in filtering their mail; and continued consumer awareness and vigilance about how to protect themselves online.

The Justice Department believes that it can play an important part in a broad response to the problem of unsolicited electronic mail messages. We believe that criminal sanctions are appropriate where a marketer has knowingly lied about his or her identity when sending out commercial electronic mail. As frustrating as all unwanted commercial electronic mail can be, it is even more frustrating for recipients when they cannot find the individual or company responsible for the mail to tell them that it is unwanted, because that spammer has used a screen of deception to hide the true source of the electronic mail. Why do some spammers do this? Why do they hide behind false e-mail addresses, relay their mail traffic through one or more misconfigured Internet hosts [1] to hide the true source of the mail, and place other obstacles in the way of those who wish to contact them? Our discussions with industry indicate that one answer is that a number of these spammers are not proud about what they are doing. At best, they do not want to put true identifying information on this commercial mail because they do not want to have their mail filtered, hear from recipients that they do not wish to receive such mail, or lose their connection to the Internet because they have violated their contract with their provider. At worst, these marketers do not want to be contacted because they are actively engaging in fraud by advertising illegal items or schemes, and want to hide from investigators and victims. In some cases, the lie itself creates additional victims, when unscrupulous spammers misappropriate the e-mail address of an innocent user to send out their spam—resulting in the innocent user receiving thousands of responses and complaints from recipients who have been deceived to believe that the innocent mailbox owner was responsible for this spam, often rendering the account of the innocent victim useless.

We believe that deterring the knowing use of fraudulent identifying information will assist both users and Internet service providers in fighting unsolicited commercial electronic mail. With accurate identifying information, users can contact marketers to tell them that they no longer wish to receive electronic mail, and can tell whether those requests are being honored. Similarly, with accurate identifying information, providers can better identify and, when appropriate, filter traffic from persons who are crippling their network or generating hundreds or thousands of complaints due to unsolicited electronic mail. In fact, in testimony given on May 21st of this year before the Senate Commerce Committee, Ronald Scelson, a self-proclaimed spammer who claimed responsibility for sending approximately 180 million spam e-mail messages per day, indicated that he intentionally forged headers precisely so that he would avoid being shut down by his service provider due to customer complaints. Creating a criminal offense to address the worst behavior will allow law enforcement, in appropriate cases, to work with providers to identify persons responsible for this sort of activity and subject them to prosecution.

Similarly, we believe that we can assist in deterring one of the most common and significant complaints about spam—people receiving unsolicited messages containing sexually oriented content. Requiring marking of that sexually explicit content in unsolicited mail and enforcing that requirement with a criminal deterrent can help individuals and parents to filter out electronic mail that they are likely to find particularly offensive.

III. THE DEPARTMENT'S COMMENTS ON TITLE II OF H.R. 2214

We note that H.R. 2214 attempts to addresses the spam problem with a balanced combination of administrative, civil, and criminal tools. Title I of the bill sets out minimal requirements for commercial electronic mail messages to assist consumers and providers in locating marketers to tell them when their solicitations are un-

[1] We understand from our discussions with industry that spammers seek out mail servers and other Internet hosts running software that permits that host to be an unwitting third-party relay between the spammer and the mail server of the recipient. In some cases, the relay server is running old mail server software with settings permitting such relaying, although most modern mail software does not permit such relaying by default. Spammers trade information about these servers, known as "open mail relays," and exploit them as a mail delivery mechanism. In other cases, the relay is a computer running proxy software. Such proxy software is often installed on home or business computers by a trojan horse program, a computer virus, or a network worm, without the knowledge of that computer's owner.

wanted and to require marketers to respect those requests when they receive them. It also provides for civil enforcement of these "rules of the road" by the Federal Trade Commission, State attorneys general, and Internet service providers. Title II of the bill, which is the focus of my testimony today, creates new criminal penalties for falsifying the sender's identity in commercial electronic mail, for sending unsolicited commercial electronic mail containing sexually-oriented material without identifying it as such, and for using automated processes to collect thousands of electronic mail addresses from web sites, chat rooms, and bulletin boards. Finally, Title III supplements and supports the previous two titles, requiring Federal Trade Commission regulations to implement the administrative provisions and reports to Congress on the effectiveness of various techniques for stopping spam. The Justice Department believes that legislation such as this will help to alleviate the burdens placed on network providers and consumers from the daily onslaught of pitches, fraudulent schemes, and pornography in electronic mail. We believe that this, in turn, will make consumers more likely to use the Internet to purchase goods and services, and help further fulfill the Internet's potential.

In particular, we support the bill's approach to criminalizing the knowing falsification of the identity of the sender. Our conversations with industry have indicated that senders of unsolicited commercial electronic mail are very good at evading filters and rules of all types. Spammers can tell when their electronic mail is being blocked and they react quickly—often finding ways around the filters within hours or minutes. By criminalizing the knowing falsification of the sender's identity and giving non-exhaustive examples of the means by which they currently do this, we believe that the statute would keep better pace with new and inventive ways spammers will undoubtedly develop to knowingly falsify their identities.

The Justice Department also supports making it criminal offense to send unsolicited commercial electronic mail containing sexually explicit content without marking it as such. As I indicated before, this is a frequent complaint that the Department receives—both from individuals who discover that their electronic mail address is now the target of multiple unsolicited pornographic e-mail messages each day and from parents who discover that their child has received unsolicited e-mail that contains explicit content. We believe that requiring appropriate marking for sexually explicit, unsolicited electronic mail will assist parents and individuals in filtering out sexually explicit e-mail that they do not wish to receive and assist parents in protecting their children from receiving such e-mail.

We support H.R. 2214's general approach to criminal penalties. We believe that criminalizing particularly egregious conduct at the felony level is appropriate for several reasons. First, it will help to ensure that these cases will be investigated and prosecuted in the field, as investigators and prosecutors simply lack resources or the incentive to spend weeks tracking down a spammer for a misdemeanor offense. Second, it will provide prosecutors with the necessary tools to investigate these cases, as some Federal investigative tools are reserved solely for felony offenses. Third, it places the United States in a position of being able to seek and receive international assistance in this area in the future, as international treaties, law, and practice often restrict certain types of assistance to cases in which both countries criminalize the conduct at the felony level.

At the same time, however, we are concerned about using a felony threshold that relies on the number of prohibited e-mail messages sent. In order to establish a felony for a first-time offender under the bill, a prosecutor would have to prove beyond a reasonable doubt that the sender knew that he falsified his identity in each of 10,000 commercial electronic mail messages or that each of 10,000 messages containing unmarked sexually explicit conduct were truly unsolicited by all recipients. The prosecutors in the Criminal Division tell me that these thresholds would make these felonies extremely difficult to prosecute because they would have to accumulate a massive documentary case just to meet the felony definition. This, in turn, could require expenditures of resources that simply are not available, given the Department's other key priorities. Even in the cases that the Department envisions prosecuting—people responsible for hundreds of thousands or millions of messages per day with falsified headers or unmarked pornography—the burden of collecting, authenticating, and proving beyond a reasonable doubt that each such message was sent with the necessary intent and falsification could essentially render the crime unprovable.

While the Department understands the desire to set thresholds to guide the exercise of prosecutorial discretion, we strongly suggest that the Subcommittee consider other triggers for felony treatment. We note that S. 1293, recently introduced by Senators Hatch, Leahy, and Schumer, adopts other elements for felony treatment, including that the offense be committed in furtherance of another Federal or State felony, that the offense cause loss aggregating $5,000 or more within one year, or

the individual committing the offense obtained things of value as a result of the offense aggregating $5,000 or more within a year. These and other alternatives would permit felony punishment for appropriately egregious offenders without imposing an effectively insurmountable burden of proof upon the government.

We do have some more specific concerns about particular aspects of title II of the bill. I discuss five of them below and offer additional technical suggestions as well.

First, in proposed section 622 of title 18, which is one of the criminal sections that would be added by section 201 of the bill, we suggest a wording change. Section 622 would establish a crime for intentionally sending a commercial electronic mail message that the sender knows falsifies the identity of the sender. In order to ensure that this section is fully able to withstand a First Amendment challenge that the section is over-broad, in that it could be read to cover messages that are accompanied by header information that is false or misleading in immaterial ways, this section should be clarified to apply to "materially" false or misleading information.

Second, proposed section 622 of title 18 would also prohibit registering for multiple e-mail accounts or domain names using information that falsifies the identity of the registrant, and then sending messages from those accounts without providing the identity and current contact information of the sender. The Department recommends greater specificity in the definition of "current contact information" of the sender. We are concerned that a defendant might contend that a website address contained within the electronic mail or another bogus electronic mail address in the body of the message is sufficient to meet this undefined term. We suggest including a definition that specifies that "contact information" includes, at a minimum, a valid postal address and working telephone number for the sender.

Third, proposed section 623 of title 18 would prohibit sending unsolicited commercial electronic mail containing sexually oriented material without proper marking. We would also suggest a wording change to this section to harmonize the first two subsections and to reduce the risk of a successful constitutional challenge to the section. In subsection (a), the criminal prohibition covers "unsolicited commercial electronic mail that includes sexually oriented material," while in subsection (b), the FTC is required to prescribe marks and notices to be included in or associated with "unsolicited electronic mail that contains a sexually oriented advertisement." The Justice Department believes that harmonizing both subsections by using the formulation in subsection (a) will help avoid confusion and challenges based upon the distinction in wording between the two sections.

Fourth, proposed section 625 of title 18 would prohibit a person from "harvesting" electronic mail addresses from an Internet website operated by another person and using those addresses in another violation of the chapter. It appears to the Department that harvesting alone, without accompanying unlawful spamming activity, is insufficient to justify criminal punishment. Accordingly, because a defendant must be proven to have committed a violation of section 622 or 623 to trigger this section at all, and since both section 622 and 623 are punishable at least as misdemeanors, it is difficult to conceive the circumstances under which this harvesting provision would be utilized by Federal prosecutors. Accordingly, we do not support a separate criminal offense for "harvesting." We believe that the heart of this bill and the narrow role for criminal prosecution should be focused on those who send messages that lack truthful identifying information or appropriate markings denoting sexually explicit content. We believe that harvesting should be an aggravating factor at sentencing and we recommend that this separate harvesting offense be removed from the draft legislation. The Department would be willing to work with Congress to craft an appropriate directive to the United States Sentencing Commission to address this issue.

Finally, title II creates separate civil actions for conduct related to unsolicited commercial electronic mail from those created in title I of this bill. These civil causes of action created by proposed section 626 of title 18 of the United States Code are similar to those created in title I of the bill; accordingly, the civil provisions in the two titles overlap in significant ways. The Department is concerned that the civil actions could be construed to nullify one another, as both titles include a provision stating that it provides the exclusive civil remedies for violations. Accordingly, we recommend to the committee that it re-examine the relationship between title I and title II of the bill and consider centralizing the civil causes of action in title I, while leaving title II to focus exclusively upon criminal offenses and penalties.

IV. ADDITIONAL TECHNICAL SUGGESTIONS

We have some additional technical suggestions related to the definitions section of the bill that we would recommend to the committee.

First, paragraphs (2) ("commercial electronic mail message") and (4) ("consent") duplicate terms already defined in title II of the bill, except that they change the definition slightly from the definition in title II. While it is understandable that the drafters would wish title II to be able to stand on its own, subtle changes in the definitions of identical terms within the same bill promote confusion and could lead to litigation over the meaning of these key terms. We suggest that, if identical terms are used in different sections of the bill, they be defined identically, as is the case with paragraph (9) ("header information") and paragraph (16) ("unsolicited commercial electronic mail message").

Second, paragraph (5) defines "covered computer," used in title II of the bill, but only in the substantive provisions. Title II's definitional section uses the term "protected computer," which then is not used in the substantive section. These uses should be consistent. We recommend using the single term "covered computer."

Third, to the extent that the definitions contained within title II should stand on their own, the definition of "electronic mail message" from section 304 should be similarly included in title II, since it is important in interpreting that title.

On the whole, however, I want to stress that the Department supports the general approach of the criminal provisions in title II of H.R. 2214 and we believe that the issues I have raised can be resolved through the legislative process. We look forward to continuing to work with the Subcommittee on this important issue.

V. CONCLUSION

Mr. Chairman, that concludes my prepared statement. I would like to thank you and the Subcommittee again for soliciting the Justice Department's views on this issue and for allowing me to express them through my testimony here today. I would be pleased to answer any questions you may have.

Mr. COBLE. Mr. Rubin.

STATEMENT OF JOSEPH S. RUBIN, SENIOR DIRECTOR OF PUBLIC AND CONGRESSIONAL AFFAIRS AND EXECUTIVE DIRECTOR OF TECHNOLOGY AND E-COMMERCE, UNITED STATES CHAMBER OF COMMERCE

Mr. RUBIN. Thank you, Mr. Chairman, Mr. Scott, Members of the Subcommittee, for this opportunity to testify this morning.

My name is Joe Rubin. I am the Executive Director of Technology and E-commerce and Senior Director of Congressional and Public Affairs at the U.S. Chamber of Commerce.

The U.S. Chamber of Commerce serves as the principal voice for the American business community here in the U.S. And abroad. Specifically, the Chamber represents the world's largest business federation, representing more than 3 million businesses of every size, sector and region of the country, including ISPs, retailers, employers, marketers and their customers, all who have a keen interest in stopping spam.

The RID Spam Act is balanced, effective legislation that will help play a significant role in reducing the amount of spam that consumers receive in their inboxes. The Chamber is pleased to support your efforts to pass this legislation expeditiously.

The U.S. Has the largest and most dynamic economy in the world, particularly when it comes to consumer choice and control. At no other time in history have consumers been in such control over their economic domain; and e-commerce plays a critical role in that empowerment, giving consumers the power to comparison shop with little or no cost and forcing businesses to respond instantly to changes in consumer demand. No longer is the consumer bound by geographic location, but here he or she can in a nanosecond travel anywhere in the world to purchase products and services that they want with just the click of the mouse.

However, the challenge of spam threatens to destroy many of the benefits of our e-commerce system. The proliferation of bulk, unsolicited, commercial e-mail has become more than a nuisance. Increasingly, consumers are getting inundated with pornographic or false and misleading e-mail that overshadows the online communication efforts of legitimate companies.

It has to be understood, however, that there is a clear distinction between legitimate companies and those who attempt to use fraud and deception to rip off consumers, to force them to open their e-mails, to avoid ISP filters and to rip off consumers. This distinction has to be clearly recognized in any legislative attempts to address spam. Legitimate companies will comply with the rules, even if they are extremely burdensome and unworkable, while spammers will continue to ignore legislative and judicial rules and edicts. Therefore, the rules must be carefully considered and carefully balanced so as not to intentionally restrict the ability of legitimate companies to communicate effectively with their customers or inadvertently provide an unfair advantage to those who ignore the rules of the road.

There is no magic bullet in the quest to stop spam. Any successful effort will require several critical parts, including technology, market-based solutions, cooperation between businesses and between business and Government, increased FTC enforcement, enhanced ability of ISPs to go after bad actors, consumer education and responsibility, increased and enhanced law enforcement and a strong uniform Federal legislative standard.

This legislation represents a critical and effective piece of this puzzle to combat spam, but it does so in a narrowly targeted way that focuses on combating the clear abuses while protecting the continued legitimate use of e-mail. It also eliminates many of the mistakes that have been made in previous efforts to stop spam, such as granting private rights of action for consumers or requiring labels for commercial e-mail. In particular, this legislation provides the FTC with strong enforcement tools, enhances the ability of ISPs to sue spammers, draws an appropriate balance between State and Federal enforcement standards and jurisdiction and institutes a single nationwide standard to facilitate these efforts.

In addition, the RID Spam Act also provides for criminal enforcement and criminal penalties in some cases when the activities of spammers are so egregious and harmful that they rise to the level of a potential criminal offense; and we believe that these criminal provisions are carefully and narrowly drawn to target truly egregious and intentional behavior and will provide an effective backstop and supplement to other remedies provided to stop these criminals.

Mr. Chairman, thank you for the opportunity to testify regarding this important issue. As I said, the RID Spam Act is balanced, effective legislation that will have a serious impact on the amount of spam, without adversely affecting the ability of legitimate companies to communicate with their customers.

I have included more specific recommendations in my written testimony. I look forward to working with you as this legislation moves to the floor, and I am happy to answer any questions.

Mr. COBLE. Thank you, Mr. Rubin.

[The prepared statement of Mr. Rubin follows:]

PREPARED STATEMENT OF JOSEPH S. RUBIN

Mr. Chairman, Ranking Member Scott, and Members of the Subcommittee, my name is Joseph Rubin, and I am the Senior Director of Congressional and Public Affairs and Executive Director of Technology and e-Commerce for the U.S. Chamber of Commerce (Chamber). I appreciate the opportunity to appear before you this morning to discuss H.R. 2214, the Reduction in Distribution (RID) Spam Act of 2003.

The U.S. Chamber serves as the principal voice of the American business community here in the U.S. and around the world. Specifically, the Chamber is the world's largest business federation, representing more than three million businesses of every size, sector and region of the country. On behalf of the business community, therefore, let me thank you for your leadership in dealing with this issue, and in holding this timely and important hearing and moving this legislation.

The RID Spam Act is balanced, effective legislation that will play a significant role in reducing the amount of spam. The Chamber is pleased to support your efforts to pass this legislation expeditiously.

The U.S. has the largest and most dynamic economy in the world, particularly when it comes to consumer choice and control. At no other time in history have consumers been in such control over their economic domain. For example, e-commerce gives consumers the power to comparison shop with little or no cost, forcing business to respond instantly to changes in consumer demand. Businesses understand all too well that if they are not satisfying customer demands, other businesses will. No longer is a customer bound by geographic location to a business, but in a nanosecond can travel anywhere in the world to purchase products and services that they want with just a click of the mouse.

However, the challenge of spam threatens to destroy many of the benefits of our e-commerce system. The proliferation of bulk, unsolicited, commercial email, commonly referred to as "spam," has become more than a nuisance. Increasingly, consumers are getting inundated with pornographic or false and misleading email that diminishes their faith in e-commerce, undermining many of the benefits that consumers derive from e-commerce.

It also has to be understood that there is a clear distinction between legitimate companies, those that do not spoof or mislead their customers, respect and honor opt-outs, seek to gain repeat customers, and who obtain email addresses through legitimate means, versus those who attempt to use fraud and deception to get consumers to open their emails or avoid Internet Service Provider (ISP) filters and obtain customer "leads" by, in effect, stealing addresses from other online service providers. This distinction has to be clearly recognized in any legislative attempts to address spam—legitimate companies will comply with the rules, even if they are extremely burdensome and unworkable, while spammers will continue to ignore legislative and judicial rules and edicts. Therefore, the rules must be carefully considered and balanced, so as not to unintentionally restrict the ability of legitimate companies to communicate effectively with their customers.

The amount of spam is growing exponentially, and imposes real costs on consumers, ISP businesses, and the economy generally. For example, Forrester Research estimates the cost of spam to the business community alone could be as high as $10 billion annually.

Spam imposes significant costs on consumers. Not only do consumers waste valuable time deleting unwanted email, but they are also subject to a bombardment of pornographic as well as false and misleading email. The Federal Trade Commission (FTC) estimates that 66 percent of spam contains at least some form of deception, and confirms that fraudulent operators have been among the first to use email to expand their reach in seeking to exploit the vulnerable and uneducated.

ISPs also suffer real losses as a result of spam. The sheer volume of spam, for example, forces them to divert valuable resources into creating additional bandwidth to carry unwanted messages to their customers. ISPs also invest millions of dollars in technology to stop spam. However, they ironically bear the brunt of customer frustration, as they are often the recipient of consumer complaints about spam. On the other hand, while ISPs have carefully crafted agreements with their users to enable them to block accounts that are used for spam, they are increasingly finding themselves the defendant in suits brought by account holders whose accounts were blocked for allegedly sending spam.

Retailers, marketers, financial services companies, travel providers, and other businesses that communicate with their customers via email also face serious challenges and expenses as a result of spam. For example, companies must ensure that

their communications actually get to their customers, and then need to make sure that their legitimate communications are not deleted along with the spam and pornography that clog their users' email boxes.

Finally, employers are also growing increasingly concerned about the spread of spam. For example, even though it may take less than a second to delete an unwanted email, employers have growing concerns about lost productivity, as more time at the office is spent deleting unwanted spam. They are also concerned about the contents of the spam, including the threat of viruses and trojan horses contained in spam, as well as the potential for sexual harassment and other types of suits that offensive email may create. Also, because the sending of spam often uses spoofing, illegitimately using a well-known company's name and/or email address to avoid blocking and to entice end-users to open their email, companies are increasingly worried about the tremendous harm that a spammer could cause to a well-known brand.

To respond to the challenge of spam, government at all levels; consumers, ISPs, retailers and the experts across the political spectrum have all been working diligently to find a solution to the spam problem. While the success to date is impressive, the amount of spam continues to increase. The range of responses includes:

- ISPs have been on the forefront in their response to spam. First, they have invested millions of dollars in new and better technologies to block spam, and their success rates are significant—blocking billions of unwanted emails a day. ISPs have also filed lawsuits against dozens of companies and individuals who send out billions of spam emails a day, and have recovered millions of dollars in monetary penalties against these spammers. They are also forging alliances with other ISPs to combat spam, seeking to develop open technical standards and industry guidelines that will help fight spam, as well as discussing ways to better cooperate with law enforcement to stop large-scale spammers. Nonetheless, in spite of these efforts, the spam problem keeps increasing;
- The FTC Commission has sued spammers for sending false and misleading email, and has led the effort to educate consumers about the tools that they can use and simple steps that they can take to protect themselves from spammers;
- The states have also been active in attempting to devise ways to stop spammers, such as imposing increased criminal penalties, requiring labels on unsolicited commercial email, and providing ISPs and consumers with the ability to sue spammers;
- Providers of email programs include increasingly sophisticated filtering tools in their software to enable users to filter spam before it gets to their e-mailboxes;
- The U.S. Chamber of Commerce has been a leader and active participant in many of these endeavors, such as educating consumers and small businesses about how to protect themselves from spam through efforts like *www.staysafeonline.info*, and by working with industry and the FTC to help craft cooperative solutions to the common problems created by spam.

Many of these efforts have been relatively successful; while others have been abject failures, but combined they have done little to stem the overwhelming tide of unwanted bulk email. They have, however, helped to point out many of the critical shortcomings of current efforts.

Any successful effort to stop spam will require several critical parts, including a range of tools, ideas, technology, market-based solutions, cooperation between businesses and with government, increased FTC enforcement, enhanced ability of ISPs to go after the bad actors, and increased and enhanced law enforcement, along with a strong, uniform, federal legislative standard. The crafters of this legislation, working with a wide range of experts, businesses, ISPs, consumer groups, law enforcement officials, and others, have identified these shortcomings, and have attempted to address them through this legislation. This legislation therefore, represents a critical and effective piece of the puzzle to combat spam, but does so in a narrowly targeted way that focuses on combating the clear abuses, while protecting the continued legitimate use of email. It also eliminates many of the mistakes in previous efforts, such as granting private rights of action for consumers or requiring labels for commercial email.

One provision that this legislation adds to the current stable of tools to fight spam is an enhanced ability of ISPs, who are in the best position to trace the source of spam, to sue spammers, and institutes a single, nation-wide standard to facilitate their efforts. It does so in a way, however, that protects the needs of legitimate busi-

nesses to communicate with their customers through email. For instance, the legislation requires that ISPs establish a "pattern or practice" of violations with regards to disregarding an opt-out, but has no similar requirements when suing for intentional acts like using false header and routing information or harvesting email addresses—activities that legitimate companies would not undertake, and therefore no additional protection is required.

The legislation will also help to empower the FTC giving the agency the tools it needs to improve its fight against spam and fraudsters who hock their wares through spam. The FTC has the experience and the ability to protect consumers from the dark underside of e-commerce, and it has the national, and in many cases, international, jurisdiction to stop spammers no matter where they reside.

The RID Spam Act also provides state law enforcement with the ability to protect state residents from intentionally harmful acts committed by spammers, such as using false header and routing information and harvesting email addresses. It is entirely appropriate to provide the states with the ability to stop these types of egregious activities, but because of the difficulty of enforcing this type of provision across state lines, to limit their jurisdiction to intentional acts of spammers. We also believe that the ability of State Attorneys General to bring suits against spammers should be further limited by removing their opportunity to recover attorney's fees in cases that they bring against spammers.

This legislation also draws an appropriate balance between state and federal standards and jurisdiction. There are currently 28 states that have enacted some form of spam legislation, from increased civil and criminal enforcement to regulation of the content of email. This legislation provides the states with the continued authority to stop false and misleading messages, but provides for a single, uniform standard regarding other regulation of email. This is the appropriate balance. States traditionally have the authority to protect their consumers, and that authority is retained in this legislation. However, state regulation of email content has created a patchwork system of differing and inconsistent standards and definitions, resulting in an unnecessarily complex compliance system. We need preemptive federal legislation to harmonize these standards and provide powerful tools to enforcement officials.

In addition to civil enforcement tools, the RID Spam Act also provides for criminal enforcement and criminal penalties in some cases, and we believe that these criminal provisions are carefully and narrowly drawn to target truly egregious, intentional behavior, and will provide an effective deterrent against criminals.

There is little stomach in the business community for spam, and we strongly support the civil elements of this legislation to go after those companies and individuals. However, the activities of spammers are sometimes so egregious and harmful, that they rise to the level of a potential criminal offense, and those activities should be treated accordingly. For example, this legislation provides for criminal penalties when a spammer uses false header and routing information or the harvesting of email addresses. These activities, which no legitimate company would use, harm the whole e-commerce system and undermine the faith and trust in e-commerce, taking advantage of the most vulnerable among us. Further, because these are intentional, fraudulent acts perpetrated on unsuspecting consumers, criminal penalties certainly may be appropriate.

Additionally, to further deter and punish this type of egregious behavior, the legislation contains significant civil penalties ISPs can enforce against spammers. Because ISPs are in the best position to find spammers and shut them down, providing them with the tools and incentives to undertake what may be an expensive and time consuming undertaking to thwart criminal activity is appropriate.

In addition to strengthening the enforcement provisions used to stop spammers, this legislation will be effective because it eliminates many of the failed provisions that states have attempted to use to stop spam. For example, the RID Spam Act expressly requires that cases related to spam be heard in federal court, and it prohibits class actions by ISPs or causes of action by individual plaintiffs. These limitations provide necessary protection for legitimate companies while at the same time ensure that spammers will be subject to a wide range of enforcement activity from a host of levels. For instance, while it may be relatively easy to file a frivolous lawsuit against a legitimate company, it is often difficult to find and identify spammers. Therefore, it is vital to protect legitimate companies from exploitive suits for allegedly spamming. Further, granting consumers an individual right of action could ironically impede the ability of ISPs to find and sue spammers, because they would be forced to respond to a flood of discovery requests by consumers seeking to find spammers.

The State of Utah provides a case study of why a consumer private cause of action should be excluded from a spam statute. Utah has enacted a "tough" spam statute

that allows for a consumer private cause of action and class action suits. A single plaintiff's firm in Utah has now filed hundreds of class action lawsuits under this statute. However, the firm is not pursuing spammers. Given the cost and complexity of finding actual spammers, this firm has targeted the low-hanging fruit—deep pocket, leading companies and brands who do not spam their customers, but simply have a presence online and in Utah.

The legislation also explicitly rejects the use of labels, such as "ADV", and expressly forbids the FTC from requiring such labeling. The rationale behind this restriction is simple: legitimate companies will comply with regulations, even if they are burdensome and ineffective, but spammers will continue to ignore any and all regulations that they see as restricting their ability to mislead consumers. The goal of legislation should not be to give spammers and criminals a competitive advantage over legitimate companies, but should seek to reign in the fraudulent and misleading activities of spammers.

Finally, while the Chamber believes that this legislation will be an effective tool in the overall fight against spam, as with any complex legislation in a fast-changing technological environment, a few modifications could help to improve the final product.

For instance, during the first six months the legislation gives companies 20 business days to honor an opt-out, then reduces that time to 10 business days. No company wants to be labeled a spammer, and therefore companies will do their best to comply with all opt-out requests. However, not all companies are completely integrated, and many companies have multiple lists of customers that often do not speak to one another, making it impossible for a company to remove a customer within the requisite 10 business days. Further, given the "pattern and practice" language in Section 101 (b), if a company routinely fails to comply with the 10 business days, even if the company's attempts are clearly good faith efforts, that still makes it vulnerable to suit by an enterprising ISP, and provides little or no defense for a company, subjecting them to a minimum of $75,000 in damages in each suit. Conversely, technology may enable many companies to comply with an opt-out request instantaneously, and therefore the 10 business days may prove to be too long. The goal of this legislation should be to protect legitimate companies. Therefore, we would suggest providing the FTC with the ability, through rulemaking, to determine the appropriate number of days, so that enforcement can reflect the realities of each company's business, rather than an arbitrary period for compliance.

Enforcement could also be enhanced by giving the FTC the ability and authority to go after those businesses that actually benefit from the use of spam. Generally, spammers are not promoting their own products, but are acting on behalf of businesses that hire them to bring in customers. These are the companies that hire spammers to sell their products. These so-called "promoted businesses," whose products are hawked through a deluge of spam, are responsible for most of the spam that permeates the Internet.

The FTC should be given the power and authority to pursue these promoted businesses. The FTC knows how to "follow the money" and such a provision would give the FTC the ability to do just that, but would circumvent its difficultly of finding actual "spammers." The Chamber supported such a provision in the Burns-Wyden bill, and believes that such an addition would enhance the FTC's ability to target spammers.

Finally, we believe that spam should be enforced by functional regulators, rather than by the FTC, in industries where that is feasible. Again, we believe that spam legislation should minimize the burdens on legitimate companies while targeting spammers. Functional regulation would provide strong enforcement in cases where it is required, but would minimize the burden otherwise, because functional regulators are more familiar with the industries that they oversee, and there is less possibility of "getting it wrong" against legitimate companies if a functional regulator is involved.

Mr. Chairman, again thank you for the opportunity to testify regarding this important issue. The RID Spam Act is balanced, effective legislation that will have a serious impact on the amount of spam, without adversely effecting the ability of companies to communicate with their customers and potential customers through whatever means the customer most desires, including through email communications. I look forward to working with you as this legislation moves to the House floor, and I am happy to answer any questions.

Mr. COBLE. Mr. Murray?

STATEMENT OF CHRIS MURRAY, LEGISLATIVE COUNSEL, CONSUMERS UNION

Mr. MURRAY. Chairman Coble, Ranking Member Scott and other distinguished Members of the Committee, I would like to thank you for the opportunity to testify before you today.

As the excellent testimony of the witnesses that have gone before me has indicated, I don't think I need to detail how serious the problem of spam has gotten. Some estimates are that spam is going to cost businesses and ultimately consumers $10 billion this year alone through the costs of the additional bandwidth that spam uses. Some estimate that by the end of this year spam will be half of all e-mail traffic. It is currently somewhere in the 40 percent range of all e-mail traffic. When Internet Service Providers have to ramp up the number of servers that they buy and they have to ramp up the filtering tools that they purchase and they have to ramp up in an arms race against spammers of the tactics that they use, this all costs consumers in the end.

These spammers appear to be a bottomless source of ingenuity. They figured out ways to commandeer our computers to send spam for them. They have figured out ways to evade the filters that Internet Service Providers use. They have even figured out ways to spam us on new devices.

I am hearing increased reports that consumers are getting spam on their mobile phones through text messaging. The incredibly annoying part of that is most spam on your personal computer, you can just hit delete. But the spam that comes over your mobile phone comes with a beep to tell you that it is there and it is there and it is going to be there until you get rid of it. So we know that the problem with spam is a severe one, and I commend the Committee for looking at serious legislation to help consumers deal with this problem.

I commend the drafters of H.R. 2214 for a number of provisions in the bill which I think will go a long way toward helping consumers get rid of spam, especially its prohibition of false headers and its criminalization of fraud in spam and its labeling of pornography. I think I agree with the drafters of the bill that step number one in cleaning up this spam problem for consumers is getting rid of the fraud that is out there.

As Mr. Rubin said, there are sort of two classes of spam out there. There are the rogue spammers who are God-knows-where overseas sending spam that evades filters. It is not legitimate businesses. It is often scams that will cost consumers big time. And then there are legitimate businesses that are using spam, although I would submit that consumers' annoyance with spam does not end with the rogue spammers; and we need to be considering measures that will rid spam in both instances.

I also commend the Committee for labeling pornography. I think this is extremely helpful for consumers, although I would probably prefer an approach such as in the Wilson Green Bill, which ensures that when consumers opt out of that spam, that pornography that was sent to them, they don't have to view that pornography. I don't think that is something we want our children having to see.

Which brings me to where I think where H.R. 2214 falls down, and that is the primary means that the bill uses to rid consumers

of spam is an opt-out provision or a provision that puts the burden on consumers every time they get a piece of spam to tell that individual marketer that they don't want anymore spam from that particular person. The problem is, imagine if you put a "do not solicit" sign on your front door and the way that that do not solicit sign worked was that every solicitor that came to your door got one shot at you, every corporation that came got one shot, every branch of that corporation got one shot. We would spend our entire day just getting rid of those solicitors, as we will spend our entire days just getting rid of that spam.

Our magazine, Consumer Reports, recommends opt-in as the way to truly rid consumers of spam. The reason that we think opt-in is absolutely critical because consumers find themselves in a paradox right now, which is, the recommendation we give consumers to get rid of spam is to do absolutely nothing. Don't view spam. Don't opt out. Don't do anything. Because as soon as you opt out or even view it, I have recently found out, that tells the spammer that your e-mail address is a live address and so they then say, great, I am going to sell it to 50 other companies and make money on it, and I am going to continue to spam you.

The problem is, once we have an opt-out regime with some stiffer penalties, which I think will go a long way, those penalties will not reach overseas; and that is a huge source of concern of spam right now because overseas companies are responsible for a huge volume of that spam. So if the burden is then on consumers to say, well, is this from the Netherlands or is this from within the United States, I think you can see it is extremely difficult to tell where that spam is coming from. So it seems unlikely to me that Consumer Reports' recommendation would change even were this bill passed, that consumers exercise that opt-out. So we will still be telling consumers to do nothing, and there will be nothing that they can do to avail themselves.

I will fast forward and just say I agree with the remarks of Mr. Moschella which say that, in order to stem the rising tide of spam, we need the help of everyone. We need the help of law enforcement, the Federal Trade Commission, and we need the help of consumers through a private right of action, and I believe we need the enforcement that comes with class action lawsuits.

As Senator Hatch indicated in the Senate Judiciary Committee 2 weeks ago when they enacted their bill, the Federal Trade Commission recently held a workshop on spam and it seemed to be the consensus of many participants in that workshop that opt-in combined with the private right of action and class action enforcement was perhaps the best way to rid consumers of spam. As Senator Hatch noted, the best model that we have for this is the Telephone Consumer Protection Act, or the TCPA, also known as the junk fax law.

What that law did—Mr. Chairman, I will wrap up in 10 seconds—that law did provide as its two key elements private right of action, class action enforcement with an opt-in approach.

I thank the Committee for the opportunity to testify today.

[The prepared statement of Mr. Murray follows:]

PREPARED STATEMENT OF CHRIS MURRAY

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

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

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

Spam costs consumers and businesses money.

Some estimate that roughly 40% of all email is spam[3] and experts say that by the end of this year more than half of all email traffic will be spam. Consumers pay for all that spam, because when ISPs' costs go up—because ISPs have to buy more servers and pay personnel to figure out how to filter that spam—consumers' monthly ISP subscription fees go up.

One company estimates that spam will cost business $10 billion dollars this year alone (due to lost productivity, bandwidth costs, and money spent on filtering tools).[4] A study released last week estimates that spam costs businesses $874 per employee every year, because employees spend an average of 6.5 minutes every day dealing with it.[5]

America Online, the largest ISP, is currently blocking up to *2.4 billion* spam messages every day.[6] The costs of the bandwidth and servers required to move that volume of spam are astronomical—when we add the costs of sophisticated filtering systems and personnel to battle the continually escalating spam arms race, the costs of spam to ISPs (and ultimately to consumers) is truly staggering.

Recently the Washington Post reported that mainstream e-commerce companies are selling consumers email addresses to spammers.[7] For example, when consumers purchased popular "Hooked On Phonics" products, their addresses were being sold in complete violation of their privacy policy. That is, the company told consumers that they would not sell their personal information and then turned around and did precisely the opposite. "Hooked on Phonics" corporate parent subsequently updated their privacy policy and said that they meant to update it earlier; they claimed they had done nothing wrong, they were simply slow to update their privacy policy.

Even worse, one company who was contracting with a 3rd party "shopping cart" provider (the mechanism used by consumers to complete an electronic commerce transaction) had a privacy policy which would have prevented consumers' email ad-

---

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

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

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

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

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

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

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

dresses from being shared with anyone. However, consumers might not have noticed that the shopping cart company behind the scenes of the electronic transaction—"art Manager"—had a completely different privacy policy and that by purchasing a product online, they were unwittingly making themselves vulnerable (there was no link to the shopping cart company's privacy policy in the process of check out).[8]

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

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

> Send an Excel spreadsheet of your customers' names, addresses and phone numbers to an e-mail appending company, and the appending company will send back e-mail addresses that belong to those customers.
>
> What the appending company doesn't mention is that often it is missing a good deal of the information that you possess, and it may decide to append your data to its files just as it appends its e-mail addresses to yours. That means you are paying the company to incorporate your information into its e-mail database.
>
> For example, the automotive department at Sears provides its customers' names, addresses, phone numbers, and car models, makes and repair histories to e-mail appending firms when it requests customers' e-mail addresses. Sure, the company gets the e-mail addresses, but at the same time it contributes to privacy erosion—all so it can send an e-mail about its lube, oil and filter change special.[9]

A large percentage of spam is also fraudulent and/or misleading, making it a serious consumer problem as well as difficult to prosecute. The Federal Trade Commission (FTC) recently issued a report[10] regarding false claims in spam, which found that 96% of spam had false information in either the message text or in the "From" and "Subject" lines.

Clearly, spam is ripe for legislative action. We agree with the ISPs and others that strong criminal enforcement and an ISP right of action are essential ingredients to successfully reducing spam. But thus far the bills proposed, including H.R. 2214, have an "opt-out" of spam as part of their core solution. In other words, an ISP must first pass on the spam to consumers, consumers must then read the spam, and then they can exercise their right to stop receiving messages from that particular sender (perhaps at their peril as described below). We believe H.R. 2214 needs to be improved because it lacks an "opt-in" provision and private right of action for consumers at the same time that it excludes class action suits. This puts too much burden on consumers to block spam and makes it too difficult to hold spammers legally accountable for their inappropriate interference with consumers' email.

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

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

When the Federal Trade Commission recently took a close look at spam and what could be done to reduce it, many, if not most of the participants in that workshop

---

[8] Id.

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

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

agreed that opt-in was the best way to eliminate spam. It would be unwise for Congress to proceed down the opt-out path, which was clearly disfavored by experts.

Senate Judiciary Committee Chairman Hatch suggested several weeks ago that he would be willing to consider drafting legislation that entails an opt-in approach. He noted that one of the primary weaknesses of opt-out is that it leaves the burden on the consumer to eliminate spam. "People who receive dozens, even hundreds, of unwanted emails each day would have little time or energy for anything other than opting-out from unwanted spam." [11]

Senator Hatch continued on to say that,

> "[a] third way of attacking spam—and one that was favored by many panelists and audience members at the FTC forum—is to establish an opt-in system, whereby bulk commercial email may only be sent to individuals and businesses who have invited or consented to it. This approach has strong precedent in the Telephone Consumer Protection Act of 1991 (TCPA), which Congress passed to eliminate similar cost-shifting, interference, and privacy problems associated with unsolicited commercial faxes. The TCPA's ban on faxes containing unsolicited advertisements has withstood First Amendment challenges in the courts, and was adopted by the European Union in July 2002." [12]

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

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

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

> One [California] state senator, who represents several Los Angeles suburbs, accused Microsoft of eleventh-hour arm-twisting to exempt Internet service providers from responsibility for being the conduits of spam. Firms such as Microsoft, America Online and Yahoo Inc. market to their own members, and large portions of overall e-mail traffic traverse their systems.
>
> "Microsoft is talking out of both sides of its mouth," said state Sen. Debra Bowen (D), who points to statements by Microsoft Chairman Bill Gates about how much the company is fighting to eliminate junk e-mail. But "their focus has been on getting immunity for themselves and preserving their ability to strike deals to send spam," she said.[13]

Ronald Scelson, also known as the "Cajun Spammer," testified before the Senate Commerce Committee [14] that some ISPs are signing "pink contracts" which allow spammers to send emails to ISPs' subscribers, charging the spammers more than they charge other commercial clients.

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

---

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

[12] Id.

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

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

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

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

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

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

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

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

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

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

In addition, by including preemption of state laws and class actions, I believe HR 2214 will fail to stem the rising tide of spam. Congress should enact federal legislation that offers basic protection for consumers, and states should have a right to

increase such protections based on unique local needs, just as the FTC did with the Federal "Do Not Call" list.

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

Mr. COBLE. We thank all of you for being here; and we have been joined by the gentleman from Virginia, Mr. Goodlatte.

Mr. Attorney General Kilgore, the bill if enacted would not only allow you to continue to enforce your own law but also provide a role for States' attorneys general to enforce the Federal statute. Do you believe that you would use those provisions or would you for the most part continue to focus on enforcing your own law?

Mr. KILGORE. We have great cooperative efforts with both United States attorneys in Virginia. We would work with the United States attorneys as we do on most computer crimes currently. We have our Computer Crimes Unit that have prosecutors who are cross-designated and has special assistant United States attorneys, and we would use the same calculus looking at the Federal statute versus the State statute and see which would provide the best deterrent to the particular criminal act.

Mr. COBLE. Mr. Moschella, we have heard testimony and gathered evidence that spam is, in fact, a real problem. But in the grand scheme of vile conduct with which your Department must deal, it probably ranks on the lower end of the scale, I am thinking. If this legislation is enacted, how will it affect the Justice Department's resources, A; B, are you going to have to divert attention from the terrorism, emphasis on homeland security and other priorities or will you be concentrating your prosecutorial resources on the very worst spam offenders?

Mr. MOSCHELLA. Thank you, Mr. Chairman.

The short answer is we will focus our attention on the most egregious spammers who are falsifying their identities and sending these pornographic e-mails without the proper labeling.

It is true we will not be able to go after every spammer. As you know, and this Committee has a great interest in the work of the Computer Crimes and Intellectual Property Section of the Criminal Division, there are 40 attorneys there working on a range of issues—hacking, denial of service attacks and the like. We think that the most egregious types of spam can be dealt with by the Justice Department in a criminal setting, understanding that this is a piece of the larger solution. As I said in my statement, international cooperation is needed, as is cooperation with ISPs and the constant vigilance of consumers.

Mr. COBLE. I am going to suspend for the moment in view of your departure, Mr. Kilgore, to permit other Members to question you before you leave; and then we can resume a second round.

Mr. SCOTT. Thank you, Mr. Chairman.

Mr. Kilgore, one of the problems that we have been dealing with here is the problem of jurisdiction, because the Internet is kind of hard to nail down. Criminal laws require you to commit the crime within your jurisdiction. How does Virginia expect to figure out which of the spammers are within the jurisdiction of Virginia or are you going to use the fact that it landed on a Virginia computer to get jurisdiction?

Mr. KILGORE. We will use every way we can to get jurisdiction. We will use the fact that it landed on a Virginia computer to get jurisdiction. We have on the civil side successfully defended the constitutionality of Virginia's long-arm statute in reaching those who have been sending spam through Virginia illegally and using civil enforcement mechanisms. We have defended that on two different occasions. So our law does allow us to base jurisdiction on the fact that it came into a Virginia computer.

Mr. SCOTT. Now, in the Virginia law, you have a private right of action?

Mr. KILGORE. Yes, we do.

Mr. SCOTT. What can an individual sue for?

Mr. KILGORE. Under our Virginia law to that point, mostly it has been used by ISPs, Congressman Scott to sue these spammers. But the consumers as well can seek the—any person is allowed to sue and any person is allowed to sue for the actual damages they have suffered from the spam.

Mr. SCOTT. Do they get attorneys fees?

Mr. KILGORE. They do as well get attorneys fees.

Mr. SCOTT. Does the Virginia law prohibit—require the identifiers in the e-mail? You do not.

Mr. KILGORE. We do not. We looked at that Congressman Scott and determined that the law-abiding ones would be the only ones that would comply.

Mr. SCOTT. And there are also some constitutional limitations on that that may complicate prosecution.

Mr. KILGORE. Right.

Mr. COBLE. We are pleased to recognize the primary sponsor of the bill, the distinguished gentleman from North Carolina, Mr. Burr; and in order of appearance the gentleman from Wisconsin is recognized to question the Attorney General.

Mr. GREEN. Thank you.

I guess my questions are to basically everyone on the panel: What is wrong with an opt-in provision? I guess I will start with you, Mr. Moschella. What is wrong with an opt-in provision?

Mr. MOSCHELLA. Mr. Green, the Department of Justice hasn't——

Mr. COBLE. Mr. Green, if you will suspend. Mr. Green, the Attorney General is going to have to leave at 11.

Mr. GREEN. I will reserve my time.

Mr. COBLE. The gentleman from California.

Mr. SCHIFF. I thank the Chairman; and I apologize, Mr. Attorney General, if—I was out of the room—if you may have responded to this already.

The main question, I had offered an amendment in the last session that would have required ADV to appear in the subject line that would allow people to use either private software or merely

delete it on their own. There are a couple of bills that are more along that model than the one we have been focusing on, and I wonder if you could comment on the various strengths and weaknesses.

The present bill has some provisions about the veracity of some of the claims that are made which may be more difficult to tackle legally. Would we be better off with a bill that requires ADV language in it, allows you to basically—or requires spammers to check a spam list and remove you, much as we did with the phones? Would that be a cleaner approach?

Mr. KILGORE. Using ADV, certainly that those who are law abiding would comply. They would be glad to place ADV. For those who are law abiding and send out adult material, I am sure they would be glad to put ADT on their e-mails. However, in studying the labeling laws of other States, those States that had strong labeling laws and thought that would be the solution to this problem, we found that it wasn't a solution, that the spammers were still sending these unsolicited bulk e-mails. The topic that bothers us, the obscene material, Virginia's law now covers obscene as opposed to pornographic material. We covered the obscene material to make sure that we can go after those individuals. We just did not believe that having ADV as part of Virginia law was the solution, that we needed tougher criminal penalties, we needed forfeiture penalties to move beyond just the cost of doing business to make it hurt these spammers.

Mr. SCHIFF. Is that the issue, though, about what the penalty ought to be for the failure to include ADV or do you need other liability for the truth or veracity of the labeling?

Mr. KILGORE. Certainly, Congressman, you could make tough penalties for failing to include ADV or ADT; and that would be a good step, I would think, if you want to go down that road.

Mr. SCHIFF. I thank the gentleman. I yield back the balance of my time.

Mr. COBLE. The gentleman from Florida, Mr. Feeney.

Mr. FEENEY. Thank you, Mr. Chairman; and thank you, Mr. Kilgore. I have a number of short questions.

Does the Virginia statute preempt local governments from getting involved in regulating spam activity?

Mr. KILGORE. Generally, in Virginia, the laws are passed at the State level for criminal acts, and the Commonwealth attorneys are elected locally, and they enforce the Virginia code. Local ordinances rarely cover criminal natures of this. They tend to be limited to traffic and other offenses.

Mr. FEENEY. Well, elsewhere in the country, they tend to wander into other areas, everything from interest rates to fair credit reporting. So there is no specific preemption as a presumption.

Mr. KILGORE. In Virginia, we have what we call the Dillon rule, which prevents local governments from getting into any area that the State does not give them permission to get into. They haven't asked for permission to get into regulating spammers, and I am not sure that the General Assembly would give them that permission.

Mr. FEENEY. The application of the long-arm statute and with the constitutional minimum contacts test, presumably you don't try to interfere with spammers who are just using your lines from—

going from a Maryland-based spammer to a customer in Pennsylvania because you need some minimum contacts. Presumably, your statutes already prohibit fraud. Have you been able to apply successfully to a constitutional challenge about minimum contacts a situation where an unsolicited spam was sent to an individual who wasn't victimized by fraud but just bothered and harassed? Has this been tested under your statute?

Mr. KILGORE. Yes, it has. We have defended the constitutionality on two different occasions, one with an ISP and the other with a consumer action.

Mr. FEENEY. What was the highest level of appellate court that ratified the constitutionality?

Mr. KILGORE. I think it went to the Fourth Circuit Court of Appeals—the Federal.

Mr. FEENEY. Presumably, civil penalties, including attorneys fees and civil damages, would be a deterrent to individuals or businesses with assets. The big problem out there is that a lot of spammers have literally no assets or at least none that are attachable. So the question is, heretofore we haven't made it a criminal penalty, for example, to invade my mailbox with unsolicited junk mail; and one of the problems we have is people like me who have very old-fashioned principles trying to apply those old-fashioned principles to new technological applications. If we are not going to criminalize someone who wants to routinely drop junk mail in my mailbox, what is the principal distinction between criminalizing unwanted but not fraudulent spam in my inbox?

Mr. KILGORE. You know, the Virginia statute talks about the fraudulent—using fraudulent means. We make the fraudulent means the felony in Virginia, where you are changing the addresses so that you can't trace it back to a legitimate business so that you can't ask to be removed from their list. So we certainly base our law on fraudulent acts occurring.

Mr. FEENEY. I will ask one last question because I appreciate what you have done. The fraud is already proscribed in most States and in Federal law. I guess here is my bottom line. Supposing I am one of those old-fashioned guys that almost believes in buyer beware. I would never buy anything over the telephone or Internet, no matter how reputable the seller was. I want to go kick tires. Just supposing hypothetically for a second——

What bothers me about spam is the same thing that bothered me coming home from the 4th of July weekend in western Pennsylvania, the traffic jam that is created. And I know that that is what bothers the Chamber of Commerce. I know that is what bothers legitimate businesses trying to use the Internet. It is the harassment feature that in many respects for me is the bigger trouble than the outright fraud, which is already proscribed. Can you give me a principle to lay down my support for this bill?

Mr. COBLE. If you can do that quickly. I want to give everybody a chance to examine you.

Mr. KILGORE. I can stand at my mailbox, and I know junk mail when I see it, and I can dump it in the trash can in the house. Unfortunately, with the computer, you so often have to open it up to see if it is serious business, if someone is trying to contact you, in my case, if a constituent is trying to ask an important question.

Then all of a sudden you get obscene material coming across your computer or you have to deal with the annoyance of opening it and then deleting it and so often businesses have to employ and purchase so much new technology just to deal with this. In Virginia, AOL—I mean, the millions they stop each and every day from just getting to consumers all around the world——

Mr. COBLE. The gentleman from Ohio.

Mr. CHABOT. Thank you, Mr. Chairman; and, Attorney General Kilgore, I want to join my colleague from Virginia, Mr. Scott, in welcoming you to the Committee. He noted that you are a graduate of William and Mary's Law School, and I am a graduate of the undergraduate program. I spent 4 wonderful years at the College of William and Mary.

Mr. COBLE. Keep it objective.

Mr. CHABOT. But I will be very objective, although it is somewhat difficult. I was just down there last weekend over the break and took my family to Busch Gardens, and I kept trying to convince my 5-year-old that a 50-year-old guy shouldn't be on Apollo's chariot. So he dragged me on and—were you going to comment?

Mr. KILGORE. I wouldn't get on it either.

Mr. CHABOT. I did, unfortunately.

In any event, the questions I have are just a couple, and I will be real brief. How would this legislation or how does your legislation deal with one of the issues that Mr. Murray brought up and that is the difficulty of overseas spammers? I know yours was only enacted, you said, 7 days ago.

Mr. KILGORE. Seven days ago.

Mr. CHABOT. It is difficult to say what your experience is.

Mr. KILGORE. We are forming task forces with the ISPs, with those in the Federal Government to come up with a plan to deal with these overseas individuals. You know certainly they will have contact with Virginia computers, they will have contact coming through Virginia ISPs, and we want to work to bring them to justice in Virginia.

Mr. CHABOT. Secondly, along the lines of what Mr. Green was going to say and with some of the other panel members, what was Virginia's rationale or thought process relative to not going to an opt-in type statute?

Mr. KILGORE. Well, we didn't—we have not addressed opt in or opt out as far as our consumers go. We provide civil remedies for consumers. As far as I am concerned, I personally prefer to opt into something as opposed to opt out. But we have seen the opt-out program work well with the telemarketers bill that Congress passed. You have millions of people opting out—registering on the Federal do-not-call list.

Mr. CHABOT. My understanding is—how would this work as far as—I mean, it wouldn't be the same type of thing, would it, where you could just call some number and opt out of all of it in the proposed legislation. That is not what we have in mind here, but I guess that is something for us to consider. But, finally, did Virginia—are there other States that have already passed or—I wouldn't say passed legislation about this. Do we know the experience of any other States or is Virginia on the cutting edge?

Mr. KILGORE. We believe we are on the cutting edge on this one. We have looked at other States' laws in crafting this legislation. We believe we needed to move much further and bring criminal actions and make it felonies for these type of activities as well as continue our tough civil penalties.

Mr. CHABOT. Okay. Thank you very much. I yield back my time, Mr. Chairman.

Mr. COBLE. Mr. Attorney General, one more questioner. And he is, appropriately enough from your State. Mr. Goodlatte.

Mr. GOODLATTE. Thank you, Mr. Chairman. I hope I am in under the wire here with our great Attorney General. I want to thank you first for holding this hearing. And I was pleased to introduce this legislation, along with my friend, Mr. Burr from North Carolina, and most pleased that we have been able to work together with the Commerce Committee.

I appreciate your show of support by coming today. In the last Congress, this Committee passed out a variation of a bill that I introduced in the last Congress, and we confronted the Commerce Committee with a different bill.

And this time, I think because the chairmen of both the Committees have worked together and have cosponsored the legislation, this bill has great prospects for success. I thank the gentleman from North Carolina for his leadership on that.

I want to welcome my good friends, Joe Rubin and Will Moschella. I especially want to welcome our Attorney General. I thank you for coming to testify today. But I most especially thank you for the leadership that you have shown on this issue. You do have, as a result of your personal efforts and the efforts of the Attorney General's Office, and the Virginia General Assembly, the toughest anti-spam bill in the country.

And I think it is important that Virginia show that leadership, because the State is the hub of so much Internet activity for not just the country but the world. I also appreciate very much the focus that you have taken on the criminal nature of this.

In response to the gentleman representing Consumer's Union and to my good friend from Florida, I would just say that when I go to that mailbox, and I pull out all of that junk mail, 90 percent of it goes straight into the trash.

But maybe 10 percent of it is something that I may have some interest in. And for that reason alone, I think an opt-out approach is the most suitable here. If you take the ability of legitimate businesses to share information with consumers out of the process by requiring the consumer find them first, and opt-in to the process, then you are taking the information out of the most important vehicle for sharing information of the information age, the Internet, and therefore, I think that is a bad approach.

Can I ask you, Attorney General Kilgore, why Virginia has determined that criminal penalties are necessary to combat spam?

Mr. KILGORE. Well, we just found that the civil penalties, while ISPs were using them, individuals were beginning to use the civil penalties, they just weren't working. Spammers were chalking it up to the cost of doing business. They were adding it into their costs and continuing to operate and continuing to spam individuals.

We believe criminal sanctions will make a big difference in Virginia. We are already working with the ISPs to target some of these individuals who are violating Virginia Statute.

Mr. GOODLATTE. Thank you very much. I appreciate your shortness of time and wish you could stay longer.

Mr. COBLE. Mr. Goodlatte, you did not include Mr. Murray as you were welcoming others. I am sure you are glad to have him here.

Mr. GOODLATTE. Well, in doing so, I disagreed with him.

Thank you.

Mr. COBLE. Mr. Attorney General, delight to have you with us. We will excuse you. We will revert to the regular order now in our second round.

Mr. Moschella and/or Mr. Rubin, there is broad recognition, it seems to me, that some balanced Federal legislation may be of benefit. But I also detect equally broad recognition that perhaps no legislation alone can resolve the spam problem, and that any bill which attempted to do so might pose a substantial risk of unintended harm to the Internet.

Now, Mr. Moschella do you think criminal penalties alone, or for that matter any legislation alone can solve the problem? And I would like to hear from you as well, Mr. Rubin.

Mr. MOSCHELLA. Thank you, Mr. Chairman. Spam isn't going to be stopped by the passage of legislation alone. And it will be a combination of solutions that will address it. As I testified, and as the Justice Department is particularly concerned about in this bill, criminal prosecution for the very worst offenders, civil and administrative remedies against those who cause harm by failing to follow the rules of the road the Congress will lay out; continued technological development that will assist network providers and users to filter their e-mail or set their preferences on their computer inbox and continued consumer awareness and vigilance about how to protect themselves on line.

Mr. Chairman, if I may. I would just like to address one issue. Maybe I misunderstood something that Mr. Feeney said. He said that fraud was already illegal. That is true when we are thinking about the scams. I am not an expert in section 5 of the FTC Act. But, he is correct in that front.

But the kind of fraud that we are talking about there, using fraudulent identity to get around the ISPs, to route the e-mail, the commercial e-mail to avoid detection, to avoid the victims, that is not illegal and that is what this bill will do.

Mr. COBLE. Mr. Rubin, do you want to be heard?

Mr. RUBIN. Thank you, Mr. Coble. The legislation is not going to solve the problem on its own. And criminal penalties certainly will not solve the problem on their own, but criminal penalties can be an effective backstop. They can help with the worst of the worst, those who clearly and intentionally violate the law to try and either defraud consumers or defraud ISPs.

But, it is going to take more. ISPs have filed hundreds of lawsuits against spammers and recovered millions of dollars in damages. That effort will continue and will be facilitated, I think, by this legislation. Technology is going to play a key role. ISPs are experimenting with new filters and with new technology every day.

Consumer education is certainly going to play a major role, and enforcement by the FTC and by others is a necessary component to this.

Mr. COBLE. Thank you. Mr. Murray, you testified about an individual private right of action, but you also noted the difficulties of enforcement against the true problem, spammers, some of whom are offshore. Even the most sophisticated enforcement units of the ISPs and the Department of Justice encountered difficulty in tracking the identity of some of those people. How would the average consumer track down such spammers, and is there not a real possibility that consumer suits would instead be concentrated against the easy-to-locate legitimate businesses who occasionally make a mistake, rather than the real problem spammers, the herbal Viagras, the porn spammers, et cetera, of the world.

Mr. MURRAY. Well, Chairman Coble, the first part of that question is the difficulty of the average consumer in tracking down the spammer. And that is why I think class action suits are absolutely critical to enforcement, because it allows what is a relatively minor cost to an individual consumer to be aggregated over a large body of consumers, and that gives the right incentives to actually get spam taken care of.

As far as the second part of the question, I can't—I think you are right that they would first go after deep pockets. And that is why if we set up a system whereby good actors have a mechanism that they can still reach consumers, I think that that works.

To respond to something that was said about opt-in sort of taking the Internet out of the advertising world, I think it is clear that what we are talking about here is not removing the Internet as advertising vehicles. Consumers will still get pop-up ads, they will still be able to go, when they are on any Internet site, they will get banner ads, there are lots of possibilities for advertising.

The difference here is that e-mail is a means that—of one-on-one communication, and it is the same difference that allowed the Federal Trade Commission recently to enact the Federal do-not-call list, where, you know, we said you can put a do-not-solicit sign on your front door, and now the Federal Trade Commission and the President have said, you can put a do-not-solicit sign at your dinner table.

And I think it is incumbent on Congress to say the same thing for consumers with respect to e-mail. If I can say one more——

Mr. COBLE. My time has expired. So wrap up.

Mr. MURRAY. Certainly. To respond to Representative Goodlatte's point about opt-in versus opt-out, I think the big difference between direct mail and e-mail is this: There is a cost with direct mail which is borne by the sender of that mail, and that is not the case with spam.

If each spammer had to spend 37 cents to send every individual spam, I don't suspect Mr. Scelson, the Cajun Spammer, would be able to send 180 million e-mails every day.

Mr. COBLE. Well, that would clearly be a disincentive. The gentleman from Virginia, Mr. Scott.

Mr. SCOTT. Thank you, Mr. Chairman. Mr. Moschella, on the identifiers, there have been a number of Supreme Court cases protecting the right to anonymous speech, some of these have been ac-

tually been applied to e-mail. How would this bill fare under those cases?

Mr. MOSCHELLA. Thank you, Mr. Scott. We have taken a look at that issue. You are right. Commercial speech enjoys First Amendment protection. That is why, in our written testimony, we asked the Committee to narrow the false identifier provision to make sure it is material.

With that change, that is, that the falsification, that it is a material falsification, we believe that change will ensure that this provision survives any Constitutional scrutiny.

Mr. SCOTT. How does that deal with the right to anonymous speech?

Mr. MOSCHELLA. Well, Mr. Scott, in these cases, we don't know any legitimate reason, I can think of no legitimate reason for commercial speech to be anonymous to hide one's identify from the ultimate end user. I don't think this is the case of Thomas Payne and political speech.

Mr. SCOTT. That is fine. What does the Supreme Court say about that, or what have the Courts said about the right to anonymous speech? Mr. Murray, do you want to give any comment on that?

Mr. MURRAY. I am not the world's foremost First Amendment expert, Representative Scott, but my understanding is that there has always been a very clear distinction in the law between commercial speech on one hand and political speech on the other.

And I think that measures, such as the Telephone Consumer Protection Act, have survived first amendment scrutiny.

Mr. SCOTT. Now, Mr. Moschella, this bill is not limited to bulk e-mail. It would include individual e-mail. Is that my understanding?

Mr. MOSCHELLA. My understanding is that the statute sets out some thresholds that would be part of the trigger for prosecution.

Mr. SCOTT. Now, Mr. Rubin, you indicated a term, "bulk unsolicited commercial e-mail." do you want all of those to apply before any legislation affects the communication, that it would have to be bulk, it would have to be unsolicited, and it would have to be commercial?

Mr. RUBIN. Well, there has to be a clear distinction drawn between e-mail that is fraudulent, that has indicia of fraud. As the FTC pointed out, more than 60 percent of the e-mail that they have investigated has indicia of fraud versus e-mail sent out by legitimate companies.

So we think that the threshold, the first threshold needs to be indicia of fraud or misleading, and clearly there needs to be some——

Mr. SCOTT. Well, if it is not fraudulent, if it is not misleading, it is just a bunch of advertisements, true advertisements, not hiding anything, is that—should that not be covered?

Mr. RUBIN. It clearly is covered under this legislation.

Mr. SCOTT. Is that a good thing or a bad thing?

Mr. RUBIN. It is not a bad thing that e-mail—that e-mail senders should not hide their identities, should not use fraudulent header or routing information——

Mr. SCOTT. But there should be unlimited right to fill up your mailbox with—your e-mail mailbox with unsolicited bulk commercial e-mail?

Mr. RUBIN. Again, we have to look at the distinction between legitimate senders and illegitimate senders.

Mr. SCOTT. Well, legitimate senders.

Mr. RUBIN. Legitimate senders—we think before you try and tackle the—as you point out the Constitutional problems and other problems with legitimate senders, you need to look at——

Mr. SCOTT. Some people are offended by legitimate advertisements loading up your mailbox on your computer.

Mr. RUBIN. Well, Mr. Scott, as I pointed out in my testimony and as—companies want to keep consumers as their customers. Legitimate companies intentionally try and keep customers, they try and make sure that they are happy customers. They respect opt-outs. They respect the rights of their customers and their potential customers. If they don't, as a business, I am going to lose that potential customer.

Mr. SCOTT. Okay. Mr. Moschella, is there a private right of action in the bill?

Mr. MOSCHELLA. I understand that there is.

Mr. SCOTT. Individual right of action, or the right of

AOL or the ISP to take a private action?

Mr. MOSCHELLA. In title 2 of the bill, there is a private right for the ISPs and the FTC and the Attorney General can act, also pursuant to that provision.

Mr. SCOTT. What about an individual?

Mr. MOSCHELLA. I don't believe so. No, sir.

Mr. SCOTT. Technologically, does the ISP provider have the ability to stop bulk unsolicited commercial e-mail?

Mr. MOSCHELLA. That is a question better posed to the ISPs. My understanding is that, yes, they can filter e-mail as long as, you know, however they set their filtering systems to capture the mail. The problem here is, and the reason why, at least on the—with regard to the criminal provision we feel it so important, is that these spammers, like this individual who testified before the Senate, are sending hundreds and thousands and millions of e-mails a day by avoiding those filters, flaunting the rules of the ISPs, the contractual obligations that they have, and in many cases, using weaknesses in third party computers, misconfigured computers, if you will, to send their spam.

We believe that this is the most egregious type of mail, and if you can address the fraudulently sent mail, you will be addressing a large part of the problem.

Mr. SCOTT. Thank you.

Mr. RUBIN. If I can answer. The ISPs are private networks. They have agreements with their customers and with folks who—who use their networks. You know, they spend millions of dollars every year to maintain their systems, to upgrade their systems, to make sure that their customers have the highest speed possible and other provisions.

They also try and filter out spam. You know, they have agreements with their customers that if you send out fraudulent spam, for example, from your e-mail account, we can shut you down. So

they do have the authority. And this bill does not impact that authority one way or the other.

Mr. COBLE. The gentleman from Wisconsin, Mr. Green.

Mr. GREEN. Thank you, Mr. Chairman. I just want to, one more time, briefly go through the opt-in versus opt-out question, because I think it is the most interesting debate in this legislation. So I will begin with our new assistant Attorney General.

Mr. MOSCHELLA. Thank you, Mr. Green. As I started saying earlier, the Department has not taken a position on opt-in versus opt-out. As you consider what to do here, I would urge the Committee to consider, you know, the various balances. On the one hand, you have the interests of legitimate businesses to communicate with potential customers.

On the other hand, you have the interest that was talked about earlier, the consumers' interest in not being bothered. Someone once said, well, this is merely a nuisance, why are we even getting involved? At least with regard to the criminal provisions here, we at the Department believe that this legislation addresses the most difficult types of e-mail to address, and that is the fraudulent and the pornographic.

And for that reason, we are very supportive.

Mr. RUBIN. Mr. Green, if I can also address that. Again, you have to try a distinction between legitimate and illegitimate e-mailers. Legitimate companies are going to follow whatever rules Congress sets down, even if they are burdensome, even if they make it more difficult for them to communicate with their customers.

Spammers aren't. They are going to ignore whatever rules Congress puts in place, if they feel that it diminishes their ability to communicate with consumers. So they—so clearly if you put an opt-in regime in place, you are going to discriminate against legitimate companies who are going to have to bear higher costs, or may not have their e-mail—may not be able to use e-mail to market at all.

You may force a lot of the spammers overseas, in which case, as was pointed out numerous times, there is even less ability to enforce U.S. Laws overseas than we have to enforce U.S. Law.

And then again, most of the spam that we are dealing with here is fraudulent. Sixty-seven percent plus has some indicia of fraud or misleading—either in the subject line or the "from" line or even in the body of the e-mail.

That, it seems to us, needs to be where the activity, law enforcement activity and others is focused.

Mr. GREEN. I understand what you have said. Respond, though, to the argument that someone who goes to his or her laptop in the morning doesn't want to have to, each time they see an item of spam, take it up, take a look at it, decide whether or not they want to receive future solicitations from this source, and then take action to block them. Why should someone be forced to do that in response to the problem?

Mr. RUBIN. Well, you are not forcing a consumer to do that. I think what you see here—first of all, if you get rid of two-thirds of the spam that is fraudulent, already you have cut down significantly on the amount of e-mail that a consumer is going to receive.

Once you get rid of all of that, there are presumably interests that consumers have in receiving good deals. For example, if I am looking for airfare, I probably, if I am looking to go away for the weekend, I wouldn't be upset to see a cheap air fare e-mailed to me, or as Mr. Murray pointed out in his testimony, if Sears sends me an e-mail regarding a discount for a lube job at Sears, that is something that most consumers would not be upset about.

So again, once you get rid of all of the bad stuff, you get rid of the porn, you get rid of the fraudulent stuff, then you know at that point, I think Congress can come back and reconsider. There are studies under the legislation which provide for the FTC and others to look at this issue and say, are consumers now content with their e-mail, or are they still begun inundated with fraud, or are they upset with continued legitimate offers?

Mr. GREEN. Thank you. Mr. Murray, respond, if you would, to the argument made by Mr. Rubin, that if we are not careful, our approach will simply force spammers beyond the reach of our law, beyond the reach of our territorial jurisdiction.

Mr. MURRAY. I think we run that risk with any law we enact in this space. I don't have a good answer for that question, but I think that question doesn't differ whether or not we are talking opt-in, opt-out, criminal penalties. We are still, in a sense, going to send people abroad.

If I can clarify one thing, which is, opt-in does not prohibit marketers from sending you materials if you request it from those marketers. It just means that we start with the presumption that you can't send me something if I have made the decision to—rather, if I have not made the decision to opt in.

What it says is, if I go to an airline site, even if I am still protected by the opt-in, if I go to an airline site and say, I would like weekly e-mail alerts about what your fares might be this week, they can still send those fares to you.

Anybody that you request information from, they can still send it. Well, I will end there.

Mr. GREEN. Thank you, Mr. Chairman.

Mr. COBLE. Thank you. The gentleman from California, Mr. Schiff.

Mr. SCHIFF. Mr. Chairman, I will waive my time.

Mr. COBLE. The gentleman from Florida, Mr. Feeney.

Mr. FEENEY. Thank you, Mr. Chairman. I want to leave aside, if I can for the panelists, the questions about fraud and pornography, because I think they are fairly easy cases, at least in my mind. I am more concerned about the junk, and criminalizing, in effect, unrequested or unsolicited junk.

You know, I am a freedom lover, but I am also part of the leave-us-alone coalition, and the most bothersome about junk spam is that it is terribly annoying; it tends to shut down your ability to navigate your computer.

Having said that, it is not—you know, I do believe that we have the right to regulate these things. I mean, a merchant is free to hawk his wares historically in any free market, but they are not free to harass you while you walk up and down the open market place. We have rules with respect to fax machine use, and telephone use.

And so now we are trying to apply the old principles to a new technology, to continue to open markets of commerce and advertising, but to do it in a legitimate way. And Mr. Rubin from the Chamber wants to draw a distinction between legitimate and illegitimate, but everyone starting in a business, presumably, unless they are an outright con artist, things they intend to get legitimate 1 day.

And the way that they are going to do it is to start selling discount watches on the street, or in this case, use spam to pierce into the marketplace.

I want to know what the current status of technology is with respect to what the ISPs are capable of doing. I guess I want to ask this question: Why should the Government get involved in regulating this at all? If my ISP has the ability to insist on all of the information that this bill does, identification—you know, one of the things that we require for a fictitious entity to do business, corporations in our States is that they have to register their corporation, establish a resident agent so we know a physical place where we can serve them papers, haul them into court and subject them to either civil or criminal penalties, if necessary.

Does an ISP have the technical ability to do that today, or something equivalent to that, and if so, why would I want the Federal Government to regulate this at all?

For example, we have a choice of where we go to malls to shop. I don't want to go to a mall that has dozens of solicitors and panhandlers and people harassing me with their wares; I want to be able to get in and out of the stores that I want, pursue the mall on a casual basis. Some people like to shop at Tiffany; some people like to shop at flea markets.

So if my ISP wants to be open to spam, so be it. If I have an ISP that is going to be very jealous of my time and ability to navigate exactly where I want to go, why can't they do that?

So for any of the panelists, I will open that up. What is the technological capability? Are we there yet? Is an ISP going to be able to have this technology pretty quick? If so, then the question would be, why the Federal Government would want to get involved at all.

Mr. RUBIN. Well, Mr. Feeney, I will take a first crack at that. First, ISPs currently block literally billions of e-mails a day. AOL, in and of itself blocks somewhere over a billion e-mails a day.

The ISPs I think need help, because, they can't identify fraudulent e-mail. You can identify some bulk e-mailers, but if someone is using an open relay to hide their identity, to hide the source where the e-mail came from, an ISP doesn't know if that is a legitimate or illegitimate e-mail. They don't want to block something that you are getting from your mother, but they do want to block something that you are getting from, you know, some spammer.

I think that they do need additional tools. Additionally, we are seeing more and more competition among ISPs. ISPs are now running ads: We block all spam. We block most spam. So I think the consumers are getting more and more choices as the technology advances. There is now a challenge-response technology that some ISPs are starting to use, which will challenge any bulk e-mail. And if they don't get a certain password back, they won't allow the e-mail in.

So there are technological solutions, but the ISPs still don't have all of technology they need. Plus technology, I don't think, can solve all of the problems. You still have the fraudsters who, even if they don't hide their identify, if they send a fraudulent offer, a pyramid scheme or something, you still need law enforcement to have the ability to come in and protect the consumers.

Mr. FEENEY. Well, I would like to hear from the Attorney General for a second. Now Mr. Rubin did great there until the last second, when he got right back into fraud. I want to go back, because that is an easy question. I want to go back to junk. If you can answer this, Mr. Attorney General, of what technological capabilities are out there, because I am interested in this.

And then, finally, if we allow ISPs to determine exactly what is legitimate, and what is not legitimate advertising, are we walking toward a monopoly threshold on Internet advertising? Is that something that we have to be careful of?

Mr. MOSCHELLA. Well, Mr. Feeney I want tell the Attorney General that you promoted me. I am going to have to just jump back to fraud just for a moment, because our understanding, from talking to the ISPs, is that they can block e-mail if they want to. They just can't block that which is fraudulently routed, purposefully concealing the identity.

This bill, at least with regard to the criminal provisions, does not address the issue that you are getting at. That is a decision for the ISP. They are not common carriers. ISPs are private networks. They can carry your e-mail or not carry your e-mail, particularly if you are violating the terms of your contact with the ISP. They will probably have an incentive to terminate that contract.

But, if they are getting around the terms by using technology, the false routers, false headers and the like, that is something that can't be addressed. That is a gap that the criminal provisions in title 2 attempt to fill.

Mr. MURRAY. If I can briefly respond. Filtering technologies do offer some promise. The problem is that filtering technologies are both overbroad and underbroad at the same time. For instance, I try to set up filters on my e-mail system at work. And the problem was that it was filtering some spam, but it was also filtering my colleagues messages I found out a month later, when they were very angry at me for not showing up at meetings and the like.

And so I think Representative Schiff has his finger on something, which is an ADB label or something like that, which makes it easier for ISPs to filter, may go a long ways to making those filters more effective.

The problem is if consumers want something like cable modem service, which is the Cadillac of high speed Internet, gives you video and other things that other forms of service can't do, you have really only got one choice. There is no market, very few communities in the country where you can get multiple ISPs to develop a market for tools. Maybe an ADB label could work for consumers.

Mr. COBLE. The gentleman's time has expired. Mr. Burr, even though you are not a Member of the Subcommittee, you are a primary sponsor. After the Members of the Subcommittee exhaust our line of questioning, we will be glad to hear briefly from you on your bill.

Mr. BURR. I thank the Chair.

Mr. COBLE. The gentleman from Ohio, Mr. Chabot.

Mr. CHABOT. Thank you, Mr. Chairman. Mr. Rubin, or Joe, let me ask you if I can, first of all, you had mentioned in your testimony that some ISPs are now advertising that they block all spam or some spam or whatever. How effective are some of these, especially the ones that say that they can block all spam? Is there any indication that some are pretty successful in that?

Mr. RUBIN. I don't know how successful, specifically how successful they are now. I know that AOL has been cited numerous times as being a very effective blocker. But my AOL account still gets a lot of spam. So, you know, I think every day they are spending more money. They are really—they are expending more resources, they are expending their technology, they are trying to get to the point where they can block everything.

But, again, because they don't always know where things come from, or if someone wants a particular e-mail or doesn't, it is very difficult for them to necessarily block everything.

Mr. CHABOT. Mr. Murray, would your organization have anything they want to add to that? Are you aware of any companies that are particularly successful at blocking, or are they all having difficulties in that area.

Mr. MURRAY. I can only speak anecdotally. I have heard that Earthlink does quite a good job. They do quite a good job of blocking spam. And AOL needs to be commended for the fact that they get 2.4 billion spam messages every day, some days. That is an enormous volume of spam. To try to figure out what spam you pass through and what spam you block, that is a mystery to me.

We go through, in the article that I left, in the Consumer Reports article—we actually review some filtering tools that consumers can use, and some filtering tools that ISPs use, but I can't speak with great expertise.

Mr. CHABOT. You mentioned AOL is to be commended, because they receive 2.4 billion spam—could you complete that. How successful are they?

Mr. MURRAY. I can't speak to what percentage of spam actually gets through. Again, anecdotally, I know that quite a lot of spam still goes through, because of the techniques that spammers are using to evade the filters. If they know that Viagra is going to block them, they do V space, I space, A, et cetera. That is how they evade the filtering tools. But, what percentage is getting through, I don't know.

Mr. CHABOT. Okay. Thank you. Let me ask you again, Mr. Rubin, on this one. I know that your organization represents companies that are very large and others that are mid size and very small companies—some are emerging businesses. Do you have any concerns about, you know, the newer companies that are coming out, especially those that are emerging that we should take their point of view into consideration when we are deciding on any changes in this legislation or whether it ought to be passed as is or whatever?

Mr. RUBIN. Absolutely. That is one of the reasons that we focused on the distinction between legitimate and illegitimate companies and e-mail. There are, you know, new companies, new products that companies want to be able to sell, perhaps on-line, that,

you know, we are concerned that overbroad legislation will limit their ability to communicate with potential customers. That actually raises one interesting question from Senator McCain's amendment on the Senate side. He actually proposed an amendment which would give the FTC authority to go after not the bulk spammers themselves, but the companies that actually sell the products.

What usually happens is companies will hire—a Viagra company will hire a spammer to sell their stuff. Even if they are a semi-legitimate company, they are selling the Iraqi cards, for example, they will hire a spammer to sell the stuff.

The one thing that is common about all spam, is there has to be a way to get the money out of the consumer. So the McCain amendment empowers the FTC, who has a long history of being able to trace the money—empowers them to be able to go back and find—trace the money, and find the actual company that hired the spammer. We think solutions like that will really help this legislation become much more effective.

Mr. CHABOT. Thank you. One of the particulars of this legislation is the labeling and whether it is, you know, on the pornographic site is what I wanted to ask you about.

Would these particular folks that are trying to spam relative to pornography, would they have to self-label? Is that the way that it would work? It would have to have ADT, or they wouldn't be allowed to do it at all?

Mr. MOSCHELLA. Under the current draft of the bill, the FTC is directed to promulgate rules about where the label would be placed in this unsolicited commercial e-mail that has, you know, the pornographic material in it.

Mr. CHABOT. Okay. Thank you very much.

Mr. COBLE. I thank the gentleman. The gentleman from Virginia, Mr. Goodlatte.

Mr. GOODLATTE. Mr. Chairman, thank you very much. I have an opening statement that I would ask to be made part of the record.

Mr. COBLE. Without objection.

Mr. GOODLATTE. I want to also acknowledge your note that I had neglected Mr. Murray in my earlier comments. I don't intend to do that now.

First of all, Mr. Murray, I want to say that certainly it was not to snub you. I am a subscriber to Consumer Reports, and have read your—in fact, prior to today's hearing I had read your very helpful presentation on ways that you can fight spam. I think it is a very useful benefit to consumers and discusses the issue very well.

But, I have to take very, very strong issue with one of the conclusions that you and your organization have taken. That is that a scheme of opt-in, coupled with a private right of action and class action lawsuits is a way to solve this problem. I think that would be a nightmare for legitimate American businesses. It would be a great hinderance to the legitimate uses of the Internet. It would be particularly a problem for small and growing businesses that are out looking for new customers and want to make them aware of the products that they have.

I use e-mail extensively. I rarely am exposed to the pop-up ads and other things, because I pretty much utilize it. I will tell you

that the spam that I receive is overwhelmingly from illegitimate businesses. The things that I find offensive. Occasionally I will get something from a legitimate business. I will delete it or tell them not to send me any more if they persist. That seems to work very well with a legitimate business.

But with an illegitimate business, you are right. That action of opting-out does let them know that they are—they have a live one on the hook. And I think the only solution to that is very strong criminal provisions that are provided in this legislation, coupled with a great deal of international work that is going to have to be done to get other countries cooperating with us in that area.

Now, I think there is a big difference between this and the fax law that you cited. And you are correct, it costs the advertiser money to send that junk mail to my mailbox. But with the fax, it costs the consumer money to receive even that very first fax. They have got to pay for the paper and the toner that goes over their line in order to get rid of that. And so to criminalize the very use of fax machines for commercial purposes was for a very different reason than we are addressing the issue of this form of communications.

With regard to the issue of class action lawsuits, I think that would be an abomination. We would have a situation where the legitimate businesses that we want to encourage to share valuable, useful information with consumers, and who may go wrong some of the time, in terms of whatever scheme might be devised, to face the fact that they would then face a lawsuit, not just for the one angry consumer, but for the 999,000 or 2 million or 10 million other consumers who just did what I did, that is, just deleted that ad or sent a request for an opt-out, suddenly we are all made a part of a class action lawsuit as plaintiffs, and what happens is, we will all get some nominal benefit from it, because we only suffered a very nominal loss by receiving it, and some attorney will, as we have seen in the class action lawsuit litigation which this Committee passed out, which the House of Representatives passed recently, some attorney will get 5 or 10 million, $15 million in attorney fees for having successfully extorted this particular legitimate business for doing that.

And the end result will be that legitimate businesses, which are very careful, as Mr. Rubin has already pointed out, to not offend consumers because they want them as customers, these legitimate businesses will suffer, consumers will receive less information, and the people that we are really having a problem with, the pornographers, the overseas spammers, the people sending all of the kind of information that the Chairman cited, they are going to continue on their merry way. Because, the only way to get at them is not from a class action lawsuit, they don't have the deep pockets that will be hurt by this, and they are going to go to another country, another location, another identity as soon as they see the slightest hint of smell.

I have worked with the Federal Communication Commission on the fax law. We actually got a massive fine imposed upon a New York fax operation. They moved to Canada just as soon as that happened. We have got to work on the criminal aspects of this law and go after those folks, get them extradited to this country and

put them in prison. And I don't—I think, Mr. Chairman, I would like to give them a brief opportunity to respond to my diatribe, but my objection to your approach in terms of civil litigation by private individuals, particularly in the form of a class action, is, I think, very misguided.

Mr. MURRAY. Representative Goodlatte, I appreciate your subscribership and helping to pay my salary.

With respect—I think we actually agree a hundred percent that, as I said in my opening statement, number one, we need to deal with the criminal and fraudulent aspects to spam. I think that is absolutely, as Mr. Rubin said, we are talking about two-thirds of spam.

That would be step one in dealing with this spam problem. But, as I also said, I don't think consumers' annoyance ends with spam. And, you know the difference between the legitimate business and illegitimate business is a very fine line. And a legitimate business or businesses is legitimate until it decides it is illegitimate.

Recently I found out that Hooked on Phonics, a company, I used their products when I was 3 and 4 and 5 years old, they were selling—after posting a privacy policy which said that they would not pass consumers e-mail addresses on to people, they turned around and sold those e-mails address out the back door.

That is a reputable business. They have an interest in an ongoing business. As for the fact that the junk fax law is different, you are saying that people pay for toner, they pay for paper. The fact is that consumers pay for ISPs' bandwidth; they don't have those businesses out of the goodness of their hearts. Consumers pay for ISPs when they put in filtering tools. So we are paying for those things in the end.

Just to wrap up on the class action point. Like you, we are completely opposed to coupon settlements as you alluded to—these attorneys that are collecting $5 million while consumers get a coupon or $5 off of their next ice cream cone.

Maybe what we need to do to protect legitimate businesses, because I do believe that class action enforcement is really the only way we are going to clean this up, maybe what we need is to do "three strikes—you are out" sort of thing, where you give people one chance, you give them two chances, if they continue to do it, then the third time around you are going to allow for that enforcement.

Mr. GOODLATTE. Mr. Chairman, I will just close by saying I disagree with that final conclusion about class actions and yield back.

Mr. RUBIN. Can I respond to that real quickly? The legislation does require ISPs to establish a pattern and practice to bring suit. So in effect, a lot of Mr. Murray's concern is addressed.

Mr. COBLE. I have one more question. If others have questions, we will have another round. And then Mr. Burr, we will hear from you.

Mr. Murray, since Mr. Goodlatte has placed you in the bullseye on the target, and since you are there, I will put this question to you.

The bill deals only with commercial e-mail but would not prevent what some consumers consider unwanted e-mail including, for example, political e-mail or fund-raising e-mail—you likely are aware

that some political activist groups on both sides of the political spectrum have expressed some concern that overbroad spam laws may possibly infringe, or may probably infringe on their ability to use e-mail to communicate and to do fund-raising. What say you to that?

Mr. MURRAY. I share those concerns, Chairman Coble. As I alluded to earlier, the law has also made a distinction between political speech on the one hand and commercial speech on the other. While I think it is acceptable for a spam bill to cover commercial speech, I don't think it can bring political speech within its purview without violating the Constitution.

Mr. COBLE. Anybody want to—Mr. Rubin or Mr. Moschella, want to add to that?

Mr. MOSCHELLA. Mr. Chairman, I would just say that we share the concern that regulation of political speech would venture into an area that would be subject to—that would be constitutionally infirm.

Mr. COBLE. Thank you, gentlemen. The gentleman from Virginia, Mr. Scott.

Mr. SCOTT. Thank you, Mr. Chairman. Would this legislation, Mr. Moschella, have any effect on the so-called banner ads or ads placed by the ISP?

Mr. MOSCHELLA. It would not.

Mr. SCOTT. What about placing cookies on your computer?

Mr. MOSCHELLA. No.

Mr. SCOTT. Is there any way we can stop that, Mr. Murray? Is placing cookies on your computer, just because you opened an e-mail, they have a marker on your computer. Is there any effort to get at that?

Mr. MURRAY. Not that I know of.

Mr. SCOTT. Mr. Rubin, some of us don't think fraud is the only problem going on, just the volume in itself, whether it is legitimate or so-called illegitimate. Is it your position that businesses ought to have an unlimited right to spam, so long as it is an honest advertisement?

Mr. RUBIN. Well, I don't know that we—that any business wants to send unlimited e-mail. But we are simply trying to draw a distinction, again, between the legitimate and illegitimate. If there continues to be a problem with legitimate companies, if they don't honor the opt-out, for example, or if they—if they try and use fraudulent or misleading header information or try to get around ISPs——

Mr. SCOTT. I am talking about someone who advertises that they have a product and they want to sell it, and they honestly represent themselves as the vender, is it your position that an honest vendor and honest vendors out there have an unlimited right to spam?

Mr. RUBIN. They have—if they obtain your e-mail legitimately, they have the—we don't think that they should be limited in terms of how they communicate with their customers.

Mr. SCOTT. Mr. Moschella, we talked about the right to anonymous speech. Has the Department of Justice done an analysis on the constitutionality of the identifiers that are listed in the bill?

Mr. MOSCHELLA. With regard to the pornographic e-mails?

Mr. SCOTT. No. The fact that you have to identify yourself.

Mr. MOSCHELLA. We believe that this statute is, on its face, a constitutional statute.

Mr. SCOTT. Is there, within the Department of Justice, an analysis?

Mr. MOSCHELLA. I don't have the specific analysis to share with you.

Mr. SCOTT. Can you get one? Because there are many people that have gone back and forth on this, and have concluded that it is clearly unconstitutional. Some cases have specifically applied to e-mails. I understand there is an injunction in at least one jurisdiction. And so we need to work on that.

Mr. MOSCHELLA. Mr. Scott, I would point out that I believe in the record of the full Committee in testimony that was heard on this issue last Congress, that there is a CRS report that at least addresses the pornographic e-mail criminal provision.

And in that opinion the Congressional Research Service concluded that it was Constitutional.

Mr. SCOTT. Mr. Chairman, my time has expired. I want to point out, as Mr. Murray has indicated, that the prohibition in the bill on class actions makes any private right of action virtually meaningless, because as it has been pointed out, the person who finally gets to court, you can give him a $200 or $300 check, it is just a cost of doing business.

Without a meaningful class action provision, any individual right of action, I believe, is meaningless.

Mr. COBLE. I thank the gentleman. The gentlelady from California, Ms. Waters.

Ms. WATERS. Well, thank you very much, Mr. Chairman. I almost did not make this hearing. And I guess I am a little bit sorry about being late. However, my being here may not be as productive as it should be, because I don't believe in any of this. I do not believe there should be any limits on the use of e-mail, fax, telephone calls or anything.

You know, I am constantly irritated by the fact that we all want as much as we can get in new technology and conveniences, and the minute that we have access to it, then we start wanting to censor, to limit, to give new definitions. I don't know what spam is.

And I am not going to spend a lot of time trying to figure out what it is. I believe that we should not try and create a definition of spam and decide what is valuable, what is not valuable, what is meaningful, what is not meaningful.

If there are questions of fraud, and pornography, we have laws that deal with that in certain ways. And if we need to model laws consistent with what we do about mail fraud, pornography in the mail, that is okay.

But, beyond that, because you don't like junk or spam, or jokes or too much advertising, I am just not in the business of that kind of censorship. And I just have no use for this at all.

Mr. COBLE. I thank the lady. Mr. Burr, you have been patiently standing by. And without objection, we will be glad to hear from you briefly.

Mr. BURR. I thank the Chairman for that. I thank the gentlelady. Her comments are very appropriate. I think it is the reason that

we need to have hearings on this. It is the reason that it needs to be brought up, is because there are differing opinions.

Mr. Chairman, I am not going to ask questions of your witnesses, but I can tell from just sitting and listening, that this has been invaluable to your Members, as it has been to me to hear from them.

I think it also explains the difficult balance that we try to reached with this legislation. We are not here to interpret what should go through or shouldn't go through. We are here to be a little more specific on legal and illegal. We are here to design some rules that everybody understands. But to protect the rights of those businesses who use this as a valuable business tool.

And to the customers to evaluate the value of it based upon whether they purchase or not, and not to infringe or limit that in any way. But, by the same standpoint, to set down a marker to those that illegally spam, to say that we are after them.

There is one thing that I have learned, Mr. Chairman. That is, that as technology gets better, our challenges get more abundant. This is another example of that. By the same standpoint, I have learned that those who want to be illegal will continue to strive to find ways around anything, anything, that we build to filter.

So though I applaud the efforts of AOL and many of the ISPs to filter out, we can't walk away and believe that by their efforts alone, we have filtered out 100 percent of that unsolicited e-mail that we would classify or that might be classified by the American people as information they didn't want to receive.

That is why I believe that we have struck the right balance. It is not perfect. Little legislation that I have worked on since I have been here has been perfect. But it is a step in the right direction. I think we do little damage.

And I would also make the last point. My hope is that my colleagues on the Judiciary Committee will not increase the ability for individuals to sue under class action. I think that that submarines the legislation. I can see us if that were to pass at some point in the future having to defend as legal the solicitation by lawyers through e-mail as they solicit the members of their class action suits.

That is not a world that I necessarily want to develop out of this legislation. I thank the Chairman.

Mr. COBLE. I thank the gentleman. I want to thank the witnesses, including the Attorney General, who had to leave us early for your testimony. I think it has been a good hearing. We appreciate your contribution.

This concludes the legislative hearing on H.R. 2214, the "Reduction in Distribution of Spam Act of 2003." The record will remain open for 1 week.

Thank you for your cooperation, and the Subcommittee stands adjourned.

[Whereupon, at 12 p.m., the Subcommittee was adjourned.]

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

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

Mr. Chairman, thank you for holding today's hearing on this important legislation to combat spam. I joined Mr. Burr, Chairman Sensenbrenner, and Chairman Tauzin to introduce the RID Spam Act in order to combat the growing problems that spam poses to businesses and consumers.

It is estimated that about half of all email currently sent is spam. AOL filters about 1.6 million junk email messages per minute. Last year, 261 billion pieces of spam were sent. By the end of this year, it is estimated that 1 trillion pieces of spam will be sent.

In addition to the exponential increase in the volume of spam, most spam is fraudulent. An FTC report published on April 30, 2003, found that 66% of all spam contained false information in the "from" line, the "subject" line, or in the message text. Furthermore, 96% of all spam analyzed that related to investment and business opportunities contained false information in the "from" line, the "subject" line, or in the message text.

Even more disturbing is the fact that much spam contains sexually explicit material. This graphic material flows into the in-boxes of innocent Americans daily and attacks users when they open their email accounts and view their messages. Unknowing consumers who do not wish to look at such graphic pictures are often tricked into opening the messages because the true nature of the email is disguised by false information in the "subject" and "from" lines.

It is clear that spam is not just a nuisance anymore. It is a real problem that affects real people and real businesses. Business groups estimate that $9 billion will be lost in productivity due to spam this year alone. Consumers bear the costs in the form of the time it takes to delete unwanted messages and in the slowdown of Internet traffic; telecommunications companies must provide additional bandwidth to compensate for the bandwidth used up by the increased volume of spam messages; ISPs must devote employees, time, and technological research and development to combat spam.

H.R. 2214, the RID Spam Act, is a common sense approach to the spam problem. It requires that all commercial email include (1) identification that the message is a solicitation, (2) a valid email address to which consumers can opt-out of future commercial email messages, (3) clear notice of the opportunity of consumers to opt out of future commercial email messages, and (4) a valid street address for service of process.

The bill also prohibits spammers from sending email after the consumer has opted out and prohibits spammers from harvesting email addresses from online databases and then sending spam messages to those email addresses.

The RID Spam act makes it a crime to falsify the identity of the sender and to send unsolicted, sexually explicit email without the required warning labels. In addition, the bill provides state attorneys general, ISPs, the FTC and the DOJ with the necessary criminal and civil tools to enforce the bill and maintains the ability of states to enact and enforce state fraud laws against spammers.

One essential characteristic of H.R. 2214 is the technology-friendly nature of the bill. It is clear that any successful attempt to combat spam must protect the ability of ISPs and small businesses to continue to develop technological solutions to the problem. Small businesses and ISPs have increasingly developed new and innovative methods and technologies to combat spam, including filtering technologies and techniques to determine whether a real person or a computer program is on the other side of the line. H.R. 2214 protects these technological efforts by specifically stating that the bill does not affect the legality of ISPs' policies of blocking email

messages. Protecting the ability of businesses to create innovative technological solutions to combat unsolicited email is crucial to winning the fight against spam.

I believe that the RID Spam act is a significant step in the fight against spam. I look forward to hearing the testimony of the witnesses today regarding this legislation. Thank you again, Mr. Chairman, for holding this important hearing.

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

Mr. Chairman and Mr. Ranking Member, I thank you for convening this legislative hearing today to hear testimony on the "Reduction in Distribution of Spam Act of 2003," also known as the "RID Spam Act."

Once again we are considering legislation that requires us to strike a balance between personal liberties and adequate regulation.

Unsolicited Commercial E-mails, commonly known as "spam," have become a nuisance to Internet users and a source of great concern for parents, schools, public libraries, and other entities trying to control the internet content reaching minors.

Spam is saturating the Internet with multiple copies of the same electronic message in an effort to force the message on people who would not otherwise have chosen to receive it. Most spam is commercial advertising that is often promoting untrustworthy products, get-rich-quick schemes, or quasi-legal services.

There many reasons why proponents of this legislation seek to regulate spam. One reason is that spam cost the recipient more than it cost the sender. For example, America On-Line was spending 5,000 per day of connect time to erase spam messages at a substantial cost to their subscribers. The spam senders, on the other hand, were spending approximately $100 per day to send their messages. Another reason is that a substantial portion of the spam content may be illegal. For example, some spam advertisements offer access to child pornography which is undoubtedly illegal in the United States.

The impact that spam may have on America's children is of particular concern to myself and many others. Most internet service providers offer a filtering system to prevent inappropriate material from reaching minors. However, no filtering system provides a 100% guarantee of protection. I strongly believe that spam advertisements, and the internet as a whole, should be regulated to prevent pornographic advertisements or other unwanted materials from being accessed by children.

It is at this point of regulation that a balance must be struck. Spam e-mails may be a nuisance and the products they promote my be objectionable to some of us, but that does not give the Members of the Subcommittee carte-blanche to impose upon the personal liberties of Americans who purchase spam e-mail products. As the Senate considered similar legislation to control spam, several regulatory schemes were proposed. The ideas included an email tax, an international treaty, and a "no bulk e-mail" option in email applications that would bounce the spam advertisement back to the sender. Bill Gates submitted written testimony in the Senate recommending new and improved legislation and enforcement paired with increased efforts at industry self-regulation. In the Federal Trade Commission's Orson Swindle complained that self-regulation has not been effective among email marketers and that improved technological solutions may be the only answer.

Mr. Chairman and Mr. Ranking Member, I am a proponent of controlling spam and protecting America's children from inappropriate content on the web. I am also a proponent of personal liberties and protecting all American's right to read and view legal websites of their choosing. I look forward to hearing the testimony of our witnesses today and learning how we can legislate spam without infringing on personal liberties.

LETTER FROM WILLIAM MOSCHELLA, ASSISTANT ATTORNEY GENERAL, OFFICE OF LEGISLATIVE AFFAIRS, UNITED STATES DEPARTMENT OF JUSTICE

U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

September 4, 2003

The Honorable Howard Coble
Chairman
Subcommittee on Crime, Terrorism,
and Homeland Security
Committee on the Judiciary
U.S. House of Representatives
Washington, DC 20515

Dear Mr. Chairman:

Enclosed is the corrected transcript of my testimony for the hearing held before your Subcommittee on July 8, 2003, regarding H.R. 2214, the "Reduction in Distribution of Spam Act of 2003."

Also attached is the version of my testimony that I submitted on the day of the hearing. Please note that this is different in technical respects from the testimony that was submitted to you in advance. Thank you for ensuring that the correct testimony is made part of the final hearing record.

If we may be of further assistance, please feel free to contact this office.

Sincerely,

William E. Moschella
Assistant Attorney General

Enclosures

Note: The attachment referred to in this letter can be found on page 15 of this hearing.

Department of Justice

STATEMENT

OF

WILLIAM E. MOSCHELLA
ASSISTANT ATTORNEY GENERAL
OFFICE OF LEGISLATIVE AFFAIRS

BEFORE THE

SUBCOMMITTEE ON CRIME, TERRORISM AND HOMELAND SECURITY
COMMITTEE ON THE JUDICIARY
UNITED STATES HOUSE OF REPRESENTATIVES

CONCERNING

H.R. 2214, REDUCTION IN THE DISTRIBUTION OF SPAM

PRESENTED ON

JULY 8, 2003

Testimony of William E. Moschella
Assistant Attorney General for Legislative Affairs
United States Department of Justice

before the
Subcommittee on Crime, Terrorism and Homeland Security of the
House Committee on the Judiciary
July 8, 2003

Mr. Chairman and Members of the Subcommittee:

Thank you for inviting me to testify today. My name is William Moschella and I am the Assistant Attorney General for Legislative Affairs at the Department of Justice. I thank the Subcommittee for holding this hearing on H.R. 2214, the "Reduction in Distribution of Spam Act" or "RID SPAM Act". I commend Chairman Sensenbrenner, Chairman Tauzin, Representative Burr, and all of the other co-sponsors of the legislation for taking steps to address this issue, and I am pleased to be able to discuss the Justice Department's views on that bill with you today.

I. A Framework for Addressing the Spam Problem

Over the last few years, the Department has received an increasing number of letters and calls from citizens complaining about the amount of unsolicited electronic mail appearing in their mailboxes and the potentially fraudulent, dangerous, or obscene content of those electronic mails. We have been in discussions with Internet service providers who tell us that the amount of spam they are handling continues to increase – often doubling or tripling in a matter of months. We are hearing clearly that people simply do not want to wade through unwanted e-mail offering pornography, untested medications, and shady financial deals to hear news from their daughter in college, find out that their order has been shipped from an e-commerce site, or receive offers that they have sought from legitimate marketers.

This is a key element of the problem that we are discussing today – spam deters electronic commerce and communication because it makes consumers less likely and less able to use the Internet for legitimate business. People stop signing up for offers and mailings from legitimate merchants because they fear that their e-mail address will be sold or stolen and instead of getting useful information that they want – like movie times in their community or last-minute airfare deals from an airline – they'll get unwanted pitches from spam marketers. When consumers throw up their hands at their electronic mailbox and when providers are forced to pass increased costs of spam filtering on to their customers because they are taking in more unwanted spam than legitimate mail, the benefits of electronic commerce facilitated by the Internet will diminish. This would be unacceptable.

At the same time, adopting too much regulation in this area or instituting an inflexible regime regulating all commercial electronic mail also threatens the openness and success of the Internet. Our policy toward the Internet from its first significant commercialization in the early

1990s has been to favor solutions that do not restrict progress with overbroad regulation. Thus far, we have encouraged electronic commerce to grow in accord with the Internet's open architecture and have preferred technology-based and market-driven solutions. This policy has served us well to this point and we do not advocate changing that formula. Instead, we support efforts that will target the problem of unsolicited commercial e-mail, particularly e-mail designed to facilitate consumer fraud or unwanted transmission of pornography, while not harming legitimate marketers sending electronic mail that their customers want to read. We encourage the Subcommittee and Congress as a whole to pursue these goals when crafting legislation in this area.

II. The Justice Department's Commitment to Helping Fight the Spam Problem

While we believe that the Department of Justice can play a supporting role in addressing the spam problem, we of course do not believe that the problem can be adequately addressed by any single approach or any single agency. Indeed, it is not a problem that government can be expected to solve by itself. We believe strongly that criminal prosecution will be a very small part of a larger cooperative initiative; it is a backstop for the civil, administrative, and market-based remedies that form a larger part of the regime. The role of the criminal justice system in addressing this problem should be appropriately limited to those offenders who are affirmatively hiding their identities or who are sending out unsolicited e-mail with unmarked sexually explicit content. Moreover, our prosecutions should focus on the most egregious violators who are involved in sending thousands of spam messages every day. In keeping with the balanced framework that we recommend for addressing the overall issue, the powerful deterrence of criminal law neither should interfere with the dynamic growth of the Internet and electronic commerce nor should it chill legitimate speech.

Moreover, the Government's efforts to combat unlawful spam will require continued and increased cooperation with users and network providers. It will also require approaching other countries for assistance, because even though we believe that a large percentage of spam begins in the United States and is targeted at the United States, spammers often route their spam through other countries in order to further hide their tracks. Spam will not be stopped by law alone, but by a combination of solutions: Criminal prosecution for the very worst offenders; civil and administrative remedies against those who cause harm by failing to follow the rules of the road for e-mail marketing; continued technological development to assist network providers and users in filtering their mail; and continued consumer awareness and vigilance about how to protect themselves online.

The Justice Department believes that it can play an important part in a broad response to the problem of unsolicited electronic mail messages. We believe that criminal sanctions are appropriate where a marketer has knowingly lied about his or her identity when sending out commercial electronic mail. As frustrating as all unwanted commercial electronic mail can be, it is even more frustrating for recipients when they cannot find the individual or company responsible

for the mail to tell them that it is unwanted, because that spammer has used a screen of deception to hide the true source of the electronic mail. Why do some spammers do this? Why do they hide behind false e-mail addresses, relay their mail traffic through one or more misconfigured Internet hosts[1] to hide the true source of the mail, and place other obstacles in the way of those who wish to contact them? Our discussions with industry indicate that one answer is that a number of these spammers are not proud about what they are doing. At best, they do not want to put true identifying information on this commercial mail because they do not want to have their mail filtered, hear from recipients that they do not wish to receive such mail, or lose their connection to the Internet because they have violated their contract with their provider. At worst, these marketers do not want to be contacted because they are actively engaging in fraud by advertising illegal items or schemes, and want to hide from investigators and victims. In some cases, the lie itself creates additional victims, when unscrupulous spammers misappropriate the e-mail address of an innocent user to send out their spam – resulting in the innocent user receiving thousands of responses and complaints from recipients who have been deceived to believe that the innocent mailbox owner was responsible for this spam, often rendering the account of the innocent victim useless.

We believe that deterring the knowing use of fraudulent identifying information will assist both users and Internet service providers in fighting unsolicited commercial electronic mail. With accurate identifying information, users can contact marketers to tell them that they no longer wish to receive electronic mail, and can tell whether those requests are being honored. Similarly, with accurate identifying information, providers can better identify and, when appropriate, filter traffic from persons who are crippling their network or generating hundreds or thousands of complaints due to unsolicited electronic mail. In fact, in testimony given on May 21st of this year before the Senate Commerce Committee, Ronald Scelson, a self-proclaimed spammer who claimed responsibility for sending approximately 180 million spam e-mail messages per day, indicated that he intentionally forged headers precisely so that he would avoid being shut down by his service provider due to customer complaints. Creating a criminal offense to address the worst behavior will allow law enforcement, in appropriate cases, to work with providers to identify persons responsible for this sort of activity and subject them to prosecution.

Similarly, we believe that we can assist in deterring one of the most common and significant complaints about spam – people receiving unsolicited messages containing sexually

---

[1] We understand from our discussions with industry that spammers seek out mail servers and other Internet hosts running software that permits that host to be an unwitting third-party relay between the spammer and the mail server of the recipient. In some cases, the relay server is running old mail server software with settings permitting such relaying, although most modern mail software does not permit such relaying by default. Spammers trade information about these servers, known as "open mail relays," and exploit them as a mail delivery mechanism. In other cases, the relay is a computer running proxy software. Such proxy software is often installed on home or business computers by a trojan horse program, a computer virus, or a network worm, without the knowledge of that computer's owner.

oriented content. Requiring marking of that sexually explicit content in unsolicited mail and enforcing that requirement with a criminal deterrent can help individuals and parents to filter out electronic mail that they are likely to find particularly offensive.

III. The Department's Comments on Title II of H.R. 2214

We note that H.R. 2214 attempts to addresses the spam problem with a balanced combination of administrative, civil, and criminal tools. Title I of the bill sets out minimal requirements for commercial electronic mail messages to assist consumers and providers in locating marketers to tell them when their solicitations are unwanted and to require marketers to respect those requests when they receive them. It also provides for civil enforcement of these "rules of the road" by the Federal Trade Commission, State attorneys general, and Internet service providers. Title II of the bill, which is the focus of my testimony today, creates new criminal penalties for falsifying the sender's identity in commercial electronic mail, for sending unsolicited commercial electronic mail containing sexually-oriented material without identifying it as such, and for using automated processes to collect thousands of electronic mail addresses from web sites, chat rooms, and bulletin boards. Finally, Title III supplements and supports the previous two titles, requiring Federal Trade Commission regulations to implement the administrative provisions and reports to Congress on the effectiveness of various techniques for stopping spam. The Justice Department believes that legislation such as this will help to alleviate the burdens placed on network providers and consumers from the daily onslaught of pitches, fraudulent schemes, and pornography in electronic mail. We believe that this, in turn, will make consumers more likely to use the Internet to purchase goods and services, and help further fulfill the Internet's potential.

In particular, we support the bill's approach to criminalizing the knowing falsification of the identity of the sender. Our conversations with industry have indicated that senders of unsolicited commercial electronic mail are very good at evading filters and rules of all types. Spammers can tell when their electronic mail is being blocked and they react quickly – often finding ways around the filters within hours or minutes. By criminalizing the knowing falsification of the sender's identity and giving non-exhaustive examples of the means by which they currently do this, we believe that the statute would keep better pace with new and inventive ways spammers will undoubtedly develop to knowingly falsify their identities.

The Justice Department also supports making it criminal offense to send unsolicited commercial electronic mail containing sexually explicit content without marking it as such. As I indicated before, this is a frequent complaint that the Department receives – both from individuals who discover that their electronic mail address is now the target of multiple unsolicited pornographic e-mail messages each day and from parents who discover that their child has received unsolicited e-mail that contains explicit content. We believe that requiring appropriate marking for sexually explicit, unsolicited electronic mail will assist parents and individuals in

filtering out sexually explicit e-mail that they do not wish to receive and assist parents in protecting their children from receiving such e-mail.

We support H.R. 2214's general approach to criminal penalties. We believe that criminalizing particularly egregious conduct at the felony level is appropriate for several reasons. First, it will help to ensure that these cases will be investigated and prosecuted in the field, as investigators and prosecutors simply lack resources or the incentive to spend weeks tracking down a spammer for a misdemeanor offense. Second, it will provide prosecutors with the necessary tools to investigate these cases, as some Federal investigative tools are reserved solely for felony offenses. Third, it places the United States in a position of being able to seek and receive international assistance in this area in the future, as international treaties, law, and practice often restrict certain types of assistance to cases in which both countries criminalize the conduct at the felony level.

At the same time, however, we are concerned about using a felony threshold that relies on the number of prohibited e-mail messages sent. In order to establish a felony for a first-time offender under the bill, a prosecutor would have to prove beyond a reasonable doubt that the sender knew that he falsified his identity in each of 10,000 commercial electronic mail messages or that each of 10,000 messages containing unmarked sexually explicit conduct were truly unsolicited by all recipients. The prosecutors in the Criminal Division tell me that these thresholds would make these felonies extremely difficult to prosecute because they would have to accumulate a massive documentary case just to meet the felony definition. This, in turn, could require expenditures of resources that simply are not available, given the Department's other key priorities. Even in the cases that the Department envisions prosecuting – people responsible for hundreds of thousands or millions of messages per day with falsified headers or unmarked pornography – the burden of collecting, authenticating, and proving beyond a reasonable doubt that each such message was sent with the necessary intent and falsification could essentially render the crime unprovable.

While the Department understands the desire to set thresholds to guide the exercise of prosecutorial discretion, we strongly suggest that the Subcommittee consider other triggers for felony treatment. We note that S. 1293, recently introduced by Senators Hatch, Leahy, and Schumer, adopts other elements for felony treatment, including that the offense be committed in furtherance of another Federal or State felony, that the offense cause loss aggregating $5,000 or more within one year, or the individual committing the offense obtained things of value as a result of the offense aggregating $5,000 or more within a year. These and other alternatives would permit felony punishment for appropriately egregious offenders without imposing an effectively insurmountable burden of proof upon the government.

We do have some more specific concerns about particular aspects of title II of the bill. I discuss five of them below and offer additional technical suggestions as well.

First, in proposed section 622 of title 18, which is one of the criminal sections that would be added by section 201 of the bill, we suggest a wording change. Section 622 would establish a crime for intentionally sending a commercial electronic mail message that the sender knows falsifies the identity of the sender. In order to ensure that this section is fully able to withstand a First Amendment challenge that the section is over-broad, in that it could be read to cover messages that are accompanied by header information that is false or misleading in immaterial ways, this section should be clarified to apply to "materially" false or misleading information.

Second, proposed section 622 of title 18 would also prohibit registering for multiple e-mail accounts or domain names using information that falsifies the identity of the registrant, and then sending messages from those accounts without providing the identity and current contact information of the sender. The Department recommends greater specificity in the definition of "current contact information" of the sender. We are concerned that a defendant might contend that a website address contained within the electronic mail or another bogus electronic mail address in the body of the message is sufficient to meet this undefined term. We suggest including a definition that specifies that "contact information" includes, at a minimum, a valid postal address and working telephone number for the sender.

Third, proposed section 623 of title 18 would prohibit sending unsolicited commercial electronic mail containing sexually oriented material without proper marking. We would also suggest a wording change to this section to harmonize the first two subsections and to reduce the risk of a successful constitutional challenge to the section. In subsection (a), the criminal prohibition covers "unsolicited commercial electronic mail that includes sexually oriented material," while in subsection (b), the FTC is required to prescribe marks and notices to be included in or associated with "unsolicited electronic mail that contains a sexually oriented advertisement." The Justice Department believes that harmonizing both subsections by using the formulation in subsection (a) will help avoid confusion and challenges based upon the distinction in wording between the two sections.

Fourth, proposed section 625 of title 18 would prohibit a person from "harvesting" electronic mail addresses from an Internet website operated by another person and using those addresses in another violation of the chapter. It appears to the Department that harvesting alone, without accompanying unlawful spamming activity, is insufficient to justify criminal punishment. Accordingly, because a defendant must be proven to have committed a violation of section 622 or 623 to trigger this section at all, and since both section 622 and 623 are punishable at least as misdemeanors, it is difficult to conceive the circumstances under which this harvesting provision would be utilized by Federal prosecutors. Accordingly, we do not support a separate criminal offense for "harvesting." We believe that the heart of this bill and the narrow role for criminal prosecution should be focused on those who send messages that lack truthful identifying information or appropriate markings denoting sexually explicit content. We believe that harvesting should be an aggravating factor at sentencing and we recommend that this separate harvesting offense be removed from the draft legislation. The Department would be willing to

work with Congress to craft an appropriate directive to the United States Sentencing Commission to address this issue.

Finally, title II creates separate civil actions for conduct related to unsolicited commercial electronic mail from those created in title I of this bill. These civil causes of action created by proposed section 626 of title 18 of the United States Code are similar to those created in title I of the bill; accordingly, the civil provisions in the two titles overlap in significant ways. The Department is concerned that the civil actions could be construed to nullify one another, as both titles include a provision stating that it provides the exclusive civil remedies for violations. Accordingly, we recommend to the committee that it re-examine the relationship between title I and title II of the bill and consider centralizing the civil causes of action in title I, while leaving title II to focus exclusively upon criminal offenses and penalties.

IV. Additional Technical Suggestions

We have some additional technical suggestions related to the definitions section of the bill that we would recommend to the committee.

First, paragraphs (2) ("commercial electronic mail message") and (4) ("consent") duplicate terms already defined in title II of the bill, except that they change the definition slightly from the definition in title II. While it is understandable that the drafters would wish title II to be able to stand on its own, subtle changes in the definitions of identical terms within the same bill promote confusion and could lead to litigation over the meaning of these key terms. We suggest that, if identical terms are used in different sections of the bill, they be defined identically, as is the case with paragraph (9) ("header information") and paragraph (16) ("unsolicited commercial electronic mail message").

Second, paragraph (5) defines "covered computer," used in title II of the bill, but only in the substantive provisions. Title II's definitional section uses the term "protected computer," which then is not used in the substantive section. These uses should be consistent. We recommend dropping the use of the phrase "covered computer" and in all instances using the phrase "protected computer" as that term is defined in 18 USC 1030(e)(2), or if the term is to be defined differently than in 18 USC 1030(e)(2), then consistently using the single term "covered computer" as defined in the bill, and not using the phrase "protected computer".

Third, to the extent that the definitions contained within title II should stand on their own, the definition of "electronic mail message" from section 304 should be similarly included in title II, since it is important in interpreting that title.

On the whole, however, I want to stress that the Department supports the general approach of the criminal provisions in title II of H.R. 2214 and we believe that the issues I have

raised can be resolved through the legislative process. We look forward to continuing to work with the Subcommittee on this important issue.

V. Conclusion

Mr. Chairman, that concludes my prepared statement. I would like to thank you and the Subcommittee again for soliciting the Justice Department's views on this issue and for allowing me to express them through my testimony here today. I would be pleased to answer any questions you may have.

LETTER FROM THE AMERICAN CIVIL LIBERTIES UNION (ACLU)

WASHINGTON NATIONAL OFFICE
Laura W. Murphy
Director

1333 H Street, NW Washington, D.C. 20005
(202) 544-1681 Fax (202) 546-0738

July 8, 2003

The Honorable Howard Coble
Chairman, House Subcommittee on Crime,
Terrorism and Homeland Security
2468 Rayburn House Office Building
Washington, DC 20515-3306

The Honorable Robert C. Scott
Ranking Member, Subcommittee on Crime,
Terrorism and Homeland Security
2464 Rayburn House Office Building
Washington, DC 20515-4603

Re: **H.R. 2214, the "Reduction in Distribution of Spam Act of 2003"**

Dear Chairman Coble and Ranking Member Scott:

H.R. 2214, the Reduction in Distribution of Spam Act of 2003, attempts to address spam through imposition of civil and criminal penalties. While the bill addresses "commercial" electronic mail, the definition of "commercial" is elusive, particularly where a commercial purpose is inextricably intertwined with speech that is also political or educational in nature and therefore clearly the highest form of protected speech. As a result of this confusion, speakers will likely err on the side of compliance with the provisions of the bill, thereby chilling protected speech, or penalizing speech that should be considered noncommercial. Additionally, certain provisions of H.R. 2214 are not narrowly tailored in that they apply to *any* unsolicited commercial electronic mail message rather than messages sent in bulk. Finally, the provision regarding "identifiers" constitutes a form of prior restraint and compelled speech, endangering constitutionally protected anonymous speech. For all of these reasons, we urge you to oppose H.R. 2214.

The definition of "commercial electronic mail message" may chill speech in cyberspace.

H.R. 2214 defines commercial electronic mail message as "an electronic mail message the primary purpose of which is the commercial advertisement or promotion of a product or service." While the phrase "primary purpose" provides some delineation, it may be insufficient in practice to avoid problems. Because "commercial speech" is often broadly defined, H.R. 2214 may also sweep broadly, encompassing noncommercial, political, and even educational speech that is highly protected under First Amendment jurisprudence, simply because it is intertwined with some form of "commercial" speech.

The United States Supreme Court has held that commercial speech is "speech proposing a commercial transaction." *Central Hudson Gas & Elec. v. Public Serv. Comm'n*, 447 U.S. 557, 562 (1980), *Bolger v. Youngs Drug Products Corp.* 463 U.S. 60, 66 (1983). Within those narrow confines, the definition may be sufficient. The question of what constitutes commercial speech however is far more nuanced, and bright lines are hard to find. For example, in *Rubin v. Coors Brewing Co.*, 514 U.S. 476 (1995), the Court found that a statement of alcohol content on the label of a beer bottle constituted commercial speech. Likewise, the Court found commercial speech in statements on an attorney's letterhead and business cards identifying him as a Certified Public Accountant and Certified Financial Planner. *Ibanez v. Florida Dept. of Business & Professional Regulation, Bd. Of Accountancy*, 512 U.S. 136 (1994).

In *Bolger*, the United States Supreme Court was faced with a question of whether a federal law prohibiting the mailing of unsolicited advertisement for contraceptives violated the federal Constitution's free speech provision as applied to certain mailings by a corporation that manufactured, sold, and distributed contraceptives. One category of the mailings in question consisted of informational pamphlets discussing the desirability and availability of prophylactics in general or the corporation's products in particular. The Court noted that these pamphlets did not merely propose commercial transactions. *Bolger, supra.* at 62. While the parties conceded the pamphlets were advertisements, the Court did not find that fact alone sufficient to make them commercial speech, because paid advertisements are sometimes used to convey political or other messages unconnected to a product or service or commercial transaction. *Id.* The Court concluded that a combination of three factors, all present in this case, provided strong support for characterizing the pamphlets as commercial speech. The three factors examined by the court were: (1) advertising format; (2) product references; and (3) commercial motivation.

Part of the difficulty in applying *Bolger* is that the Court rejected the notion that any one of the factors was *sufficient* by itself, but also declined to hold all of these factors in combination, or any one of them individually, was *necessary* to support characterizing certain speech as commercial. *Id.* at 67, fn. 14, and 66, fn. 13. It is no wonder the Supreme Court in later decisions acknowledged that "ambiguities may exist at the margins of the category of commercial speech." *Edenfield v. Fane*, 507 U.S. 761, 765 (1993). *See also, Cincinnati v. Discovery Network, Inc.*, 507 U.S. 410, 419 (1993) [recognizing "the difficulty of drawing bright lines that will clearly cabin commercial speech in a distinct category"] *and Zauderer v. Office of Disciplinary Counsel*, 471 U.S. 626, 637 (1985) [stating that "the precise bounds of the category of . . .commercial

speech" are "subject to doubt perhaps."].

Illustrative of this problem is *Nike v. Kasky*, a case the Supreme Court recently dismissed as having improvidently granted *certiorari*. Several members of the Court specifically noted the difficulty of the questions presented. In *Kasky v. Nike*, 27 Cal. 4th 939 (2002), Nike responded to allegations that in the overseas factories where Nike products were made workers were paid less than the applicable local minimum wage; required to work overtime; allowed and encouraged to work more overtime hours than applicable local law allowed; subjected to physical, verbal, and sexual abuse; and exposed to toxic chemicals, noise, and heat, without adequate safety equipment, in violation of applicable local occupational health and safety regulations. In responding to these allegations, Nike made statements and press releases, wrote letters to newspapers, wrote a letter to university presidents and athletic directors, and distributed other documents for public relations purposes. Nike also bought full-page advertisements in leading newspapers to publicize a report that found no evidence of illegal or unsafe working conditions at Nike factories in China, Vietnam, and Indonesia. Based on these statements, Kasky filed a private attorney general action against Nike based upon California's unfair competition law and false advertising law.

There was no question that the allegations *against* Nike were fully protected under the First Amendment to the United States Constitution. The issue for the California Supreme Court was whether Nike's *responses* to the allegations were commercial or noncommercial speech for purposes of constitutional free speech analysis. Despite the fact that none of Nike's responses proposed a commercial transaction, the California Supreme Court deemed the speech "commercial," providing it less protection than the initial allegations. In a dissent, Justice Chin noted that "[w]hile Nike's critics have taken full advantage of their right to ' uninhibited, robust, and wide-open' debates, the same cannot be said of Nike, the object of their ire. When Nike tries to defend itself from these attacks, the majority denies it the same First Amendment protection Nike's critics enjoy. Why is this, according to the majority? Because Nike competes not only in the marketplace of ideas, but also the marketplace of manufactured goods. And because Nike sells shoes--and its defense against critics may help sell those shoes--the majority asserts that Nike may not freely engage in the debate, but must run the risk of lawsuits under California's unfair competition law and false advertising law should it ever make a factual claim that turns out to be inaccurate." Quoting from *First National Bank of Boston v. Bellotti*, 435 U.S. 765, 785-86 (1978), Justice Chin stated, "[W]here. . .suppression of speech suggests an attempt to give one side of a debatable public question an advantage in expressing its views to the people, the First Amendment is plainly offended."

Because the Supreme Court has dismissed the case, Nike must now defend the allegations in California. It remains to be seen whether the case will wend its way back to the Supreme Court, and whether the Court will attempt to more adequately define "commercial" speech.

To use the language of H.R. 2214, what was the "primary purpose" of Nike's responses? Nike was clearly responding in a public debate concerning the use of low-cost foreign labor to manufacture goods sold in America. Nike's statements regarding its labor

practices in China, Thailand, and Indonesia provided vital information on this very public controversy. None of Nike's responses included product labels, inserts, packaging, or commercial advertising intended to reach only Nike's actual or potential customers. Yet, the majority concluded that Nike's speech was "commercial," entitled to less protection than the initial allegations. Thus, instead of a level playing field, Nike is disadvantaged simply because it may have an economic motivation in engaging in public debate.

This uncertainty as to what is and is not "commercial speech" may have the very real effect of chilling not only commercial speech, but speech that should be fully protected under the First Amendment. This bill does little to settle the controversy, and now transfers the problem from the real world to cyberspace.

Because the bill does not appear to define "commercial electronic mail" in the civil provisions, a company could face civil penalties for any number of scenarios in which their behavior is deemed "commercial." While there is the rather vague definition in the criminal provisions (Title II), discussed above, a company could now face criminal penalties as well if it believes the message to be non-commercial and a court or jury disagrees. Such uncertainty does little to foster business, and chills both commercial and non-commercial speech.

H.R. 2214 fails to recognize the extremely fluid nature of human relationships, particularly in the business context. A conversation at a cocktail party or a conference can move into and out of commercial speech without any clear demarcation. Subsequent e-mail communication seeking to solidify those connections may be ambiguous enough so that whether they warrant the label "advertisement" is unclear. The warmth, informality and frequency of such correspondence may well be checked by rules requiring "prior consent" or the placement of a word or phrase to denote that the e-mail is an "advertisement." Many individuals may inadvertently violate the law, and others may choose to avoid even legitimate correspondence out of fear of criminal or civil sanctions. This bill may also chill commercial outreach in a context unlikely to aggrieve e-mail recipients. For example, suppose a vendor attends a specialized industry conference, where she hears complaints about the lack of a useful product on the market. Upon returning to her company, she secures assurances that the company can develop that product. Under H.R. 2214, she may be prohibited from sending that information out to the list of conference attendees who would be delighted to receive it.

The bill should only apply to bulk mail, 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. 2214 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 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. 2214 declares a substantial government interest, it fails to narrowly tailor the regulation to achieve that asserted interest.

Section 2(a)(3) focuses on the effect of the increasing abundance of UCE on network bandwidth, network storage costs, and so forth. Internet Service Providers testifying on similar bills, have argued that 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 often 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. 2214 only peripherally discusses bulk electronic mail. For example, Section 622 provides an affirmative defense to the crime of "falsifying identity" if the defendant sent fewer than 100 prohibited messages during any 30-day period. A sentencing enhancement is authorized where the defendant sent 10,000 or more electronic mail messages within a 30-day period. Otherwise, the bill prohibits *any* unsolicited commercial electronic mail failing to meet the bill's requirements. 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. The e-mail is truthful and accurate, but fails to abide by all the restrictions contained in the bill. According to H.R. 2214, you

may now have sent an unsolicited commercial electronic mail message, subjecting you to the possibility of sanctions.

The net cast by H.R. 2214 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, yet this bill treats them both the same.

Other provisions of the bill are similarly not narrowly tailored, subjecting them to possible constitutional problems.

The section immediately above discusses the necessity for regulations on commercial speech to be narrowly tailored. H.R. 2214 fails in several respects to either address the problems noted, or to narrowly tailor the proposed remedy.

Section 2(a)(4) notes the "network security risk to businesses and governments because of the introduction of viruses and malicious code delivered via UCE messages." While this is apparently offered as a reason for governmental intervention in commercial electronic mail, the bill does not provide a remedy for this situation. Additionally, the alleged threat is not contingent upon a message being "commercial," as *any* message could contain such code. Fortunately, the law already provides a remedy: 18 U.S.C. §1030(5)(A) prohibits such conduct, whether or not the code is contained in a commercial electronic mail message. Thus, this provision appears to be superfluous.

Section 2(a)(5) discusses a "decreased level of consumer trust for legitimate email marketers and decreased willingness of end users to test new advertising formats." To the extent there is a decreased level of consumer trust, it is likely based upon false, deceptive, or other illegal activities. Such messages can be adequately prosecuted under Section 5 of the Federal Trade Commission Act. Increased enforcement action by the FTC is more likely to restore consumer confidence, and less likely to infringe upon First Amendment activity.

Section 2(a)(10) alleges that "intentionally misleading information" contained in some messages frustrate spam filters. These programs block spam based on the content of the e-mail messages and headers. Despite attempts to subvert filters, the technology for filtering is getting better. The newest algorithms, known as Bayesean filters, claim to perform with 99% accuracy. Thus, the need for government intervention in requiring accuracy in header information or a label on commercial e-mail is questionable.

A more narrowly tailored approach would be to establish a national "do not spam" list, similar to the "do not call" list. Consumers who wish to receive spam could continue to do so, while those who wish not to receive it could enter their e-mail address on the "do not spam" list. An "opt-out" approach for junk mail was upheld by the Supreme Court in *Rowan v. United States Post Office*, 397 U.S. 728 (1970). There, the Court found that the mailer has a right to communicate, but the recipient has the option to remove herself from

the list and thereby refuse any further mailings. Under such a program, the mailers' right to communicate is preserved, while the recipients' right to choose which messages to receive is likewise protected.

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

H.R. 2214 additionally requires a clear and conspicuous identifier be placed on unsolicited commercial electronic mail. 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 bill prohibits constitutionally protected anonymous speech.

H.R. 2214 requires that unsolicited commercial email include a "valid physical street address of the sender." It is unclear what the "significant" government interest is that is being addressed by this provision. However, it *is* clear that this provision undermines the right to anonymous speech on the Internet.

Additionally, requiring header information that is not "false or misleading" further devalues this right, as the provision essentially requires accurate headers, regardless of the intent of the sender.

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). By requiring accurate header information and inclusion of a valid physical street address, the bill in one fell swoop destroys anonymous commercial communication on the Internet.

A similar provision 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 avoid social ostracism, to prevent discrimination and harassment, and to protect privacy. . ."

H.R. 2214 suffers from the same infirmities. With no compelling justification, it prohibits anonymous speech by requiring a valid physical postal address, and would seem to punish anonymous speech even where there is no intent to deceive regarding the offer or information transmitted.

The bill states in Section 2(a)(9) that "there is no legitimate reason to falsify the header information accompanying commercial email," which ignores reality. Businesses may have a variety of legitimate reasons to prefer remaining anonymous in the emails they distribute. In *NLRB v. Midland Daily News, supra.*, the court upheld the right of the business to advertise anonymously for a job position to avoid being inundated with phone calls and walk-ins. A business may also wish to test the waters for interest in a particular product, but not dilute its own name or set up a subsidiary in case the product proves unsuccessful. Similarly, a business or individual that provides goods or services that are

either controversial or socially awkward might prefer those not to be linked to their name. For example, a business expanding into products associated with aging, such as ways to treat or adapt to incontinence, hair replacement, or varicose veins, may wish to avoid the brand stigma that has attached to the producer of "Depends." A for-profit medical clinic might try to launch a campaign to promote organ donation in the community, but fear that religious and other groups opposed to transplant procedures would embark on a smear campaign - or themselves "slam" the clinic's server with multiple hostile e-mails - if it attaches its name and return address. An independent book publisher or distributor in a conservative region might wish to promote books about Islam in order to dispel myths about the religion, but fear a backlash if its name is associated with that effort. Likewise, many self-published books are offered anonymously. This bill would limit one major avenue of advertisement for such books.

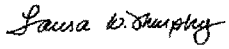
In requiring reports, the bill ignores the effects on privacy and civil liberties.

In Title III of H.R. 2214, a report is required from the Federal Trade Commission and the Federal Communications Commission "regarding the need to protect the rights of users of electronic mail to avoid receiving unwanted commercial electronic mail." After the bill goes into effect, the FTC and the FCC are to submit a study of the effects of the act. Nowhere in the list of "required analysis" is mention made of the effect on privacy and civil liberties. Where a bill so clearly has implications for privacy and First Amendment protections, this is an egregious oversight.

Conclusion

H.R. 2214 will chill constitutionally protected speech, as well as prohibit anonymous speech protected under the Constitution. The bill is not narrowly tailored to achieve the asserted governmental interests. For all of these reasons, we urge you to vote against H.R. 2214.

Sincerely,



Laura W. Murphy
Director

Marvin J. Johnson
Legislative Counsel

○