AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

THE CONSUMER PRIVACY PROTECTION ACT OF 2002

HEARING

BEFORE THE

SUBCOMMITTEE ON
COMMERCE, TRADE, AND CONSUMER PROTECTION

OF THE

COMMITTEE ON ENERGY AND
COMMERCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTH CONGRESS

SECOND SESSION

ON

H.R. 4678

SEPTEMBER 24, 2002

Serial No. 107–131

Printed for the use of the Committee on Energy and Commerce

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

U.S. GOVERNMENT PRINTING OFFICE

81–960PS WASHINGTON : 2002

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

COMMITTEE ON ENERGY AND COMMERCE

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

MICHAEL BILIRAKIS, Florida
JOE BARTON, Texas
FRED UPTON, Michigan
CLIFF STEARNS, Florida
PAUL E. GILLMOR, Ohio
JAMES C. GREENWOOD, Pennsylvania
CHRISTOPHER COX, California
NATHAN DEAL, Georgia
RICHARD BURR, North Carolina
ED WHITFIELD, Kentucky
GREG GANSKE, Iowa
CHARLIE NORWOOD, Georgia
BARBARA CUBIN, Wyoming
JOHN SHIMKUS, Illinois
HEATHER WILSON, New Mexico
JOHN B. SHADEGG, Arizona
CHARLES "CHIP" PICKERING, Mississippi
VITO FOSSELLA, New York
ROY BLUNT, Missouri
TOM DAVIS, Virginia
ED BRYANT, Tennessee
ROBERT L. EHRLICH, Jr., Maryland
STEVE BUYER, Indiana
GEORGE RADANOVICH, California
CHARLES F. BASS, New Hampshire
JOSEPH R. PITTS, Pennsylvania
MARY BONO, California
GREG WALDEN, Oregon
LEE TERRY, Nebraska
ERNIE FLETCHER, Kentucky

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

DAVID V. MARVENTANO, *Staff Director*
JAMES D. BARNETTE, *General Counsel*
REID P.F. STUNTZ, *Minority Staff Director and Chief Counsel*

SUBCOMMITTEE ON COMMERCE, TRADE, AND CONSUMER PROTECTION

CLIFF STEARNS, Florida, *Chairman*

FRED UPTON, Michigan
NATHAN DEAL, Georgia
Vice Chairman
ED WHITFIELD, Kentucky
BARBARA CUBIN, Wyoming
JOHN SHIMKUS, Illinois
JOHN B. SHADEGG, Arizona
ED BRYANT, Tennessee
GEORGE RADANOVICH, California
CHARLES F. BASS, New Hampshire
JOSEPH R. PITTS, Pennsylvania
MARY BONO, California
GREG WALDEN, Oregon
LEE TERRY, Nebraska
ERNIE FLETCHER, Kentucky
W.J. "BILLY" TAUZIN, Louisiana
(Ex Officio)

EDOLPHUS TOWNS, New York
DIANA DeGETTE, Colorado
LOIS CAPPS, California
MICHAEL F. DOYLE, Pennsylvania
CHRISTOPHER JOHN, Louisiana
JANE HARMAN, California
HENRY A. WAXMAN, California
EDWARD J. MARKEY, Massachusetts
BART GORDON, Tennessee
PETER DEUTSCH, Florida
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
JOHN D. DINGELL, Michigan,
(Ex Officio)

CONTENTS

	Page
Testimony of:	
Barrett, Jennifer, Chief Privacy Officer, Acxiom Corporation	23
Misener, Paul, Vice President, Global Public Policy, Amazon.com	31
Palafoutas, John P., Senior Vice President, Domestic Policy and Congressional Affairs, AeA	7
Rotenberg, Marc, Executive Director, Electronic Privacy Information Center	35
Schall, John A., Executive Director, National Business Coalition on E-commerce and Privacy	15
Servidea, Philip D., Vice President, Government Affairs, NCR Corporation	12
Whitener, Rebecca, Director of Privacy Services, EDS	19

THE CONSUMER PRIVACY PROTECTION ACT OF 2002

TUESDAY, SEPTEMBER 24, 2002

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

The subcommittee met, pursuant to notice, at 9 a.m., in room 2322, Rayburn House Office Building, Hon. Cliff Stearns (chairman) presiding.

Members present: Representatives Stearns, Bass, Walden, and Harman.

Also present: Representative Boucher.

Staff present: Ramsen Betfarhad, majority counsel; Yong Choe, legislative clerk; and Jonathan J. Cordone, minority counsel.

Mr. STEARNS. The subcommittee will come to order.

And good morning. I apologize; I was a little late, and I thank my colleague for her patience. Thank you, Mr. Boucher.

Let me just say I welcome our distinguished witnesses to this legislative hearing on our bill, H.R. 4678, the Consumer Privacy Protection Act of 2002.

I guess about a year and a half ago our committee began creating, I think one of the most exhaustive set of hearings dealing with this type of legislation. We had six hearings on privacy, and it was a workout to get these hearings, particularly because there was no need, it appeared, when we requested these hearings, because the chairman and others said, Well, I'm not sure we need it.

But I think, as many in the audience would say today, that there is going to be a need. So I decided to go ahead, and after careful examination, we had these six hearings; and we were very pleasantly surprised.

We took the basic premise that we wanted to do no harm to the Internet. The Federal information privacy legislation should ensure that no harm comes to the consumer from unwanted breaches of their information privacy, and at the same time, it should not harm—most importantly today—economic growth by hurting the sharing of consumer information. So our bill, H.R. 4678, I think goes a long way to establishing that balance. Now, perhaps—a lot of you will probably agree.

I think today we are going to feather out some of the nuances of my privacy bill and also that Senator Fritz Hollings has. I like to use this quote—I am not necessarily an avid fan of Ayn Rand, but she did say at one time that "Civilization is the progress to-

ward a society of privacy. The savage's whole existence is public, ruled by the laws of his tribe. Civilization is the process of setting man free from men."

So here in America, where we enjoy an open society, we cherish our privacy too. With the advent of on-line data collection, the American consumer's information privacy concerns have rightfully been heightened. As individuals and businesses turn to computers and computer networks for commercial and personal reasons, massive volumes of personal information are generated, collected and stored for personal, governmental and commercial activities.

All of these activities generate a footprint of sorts: personal data. And that footprint, in turn, has heightened consumers' concern over their personal information privacy. The fact is that personal data is collected both online and offline. The collection of consumer data on line is just a new dimension of a very old practice, although an increasingly significant one.

Moreover, consumer information, whether collected online or offline, is aggregated into the same data bases and processed by the same computers without regard to the source of that data. The consumers' legitimate concerns over their information privacy must, in turn, be weighed against the fact that our economy is highly consumer information dependent as it is a consumer-based economy where over two-thirds of our gross domestic product is comprised of consumer spending, and that is nearly $7 trillion.

Historically, consumer information has played an important role in our economic growth. The free flow of consumer information has served all of us as American consumers well throughout our modern economic history. Any Federal law or regulation that unduly burdens information sharing may bring about a substantial and negative impact, of course, on our economy. Therefore, any Federal legislation intended to be responsive to the public's information privacy concerns must include within its scope protection from both unwanted on-line and off-line data collection and use activities, and balance those protections against the legitimate consumer information gleaning and sharing activities of a consumer-based economy; and I think our bill does just that.

Shortly after the conclusion of our hearings I offered some basic principles. We have outlined these seven principles that we have and believe that the Consumer Privacy Protection Act of 2002 is a very meaningful effort for all of us. The bill mandates a privacy policy and statement. The bill requires that any organization collecting, selling or using consumer's personally identifiable information for a purpose unrelated to the consumer transaction must establish a privacy policy, and the principal elements of that privacy policy must be accessible to the consumer at the time the organization first collects this personally identifiable information and subsequently.

In addition, a data collector must provide the consumer with the opportunity to preclude the sale or disclosure of his or her PII to any other data collector and user. As noted in our bill, it applies to both online and offline, and that has been our policy from the very beginning.

It preempts States' action, forecloses private right of action, and vests in the FTC the exclusive authority to enforce its provisions.

The bill entails a novel cyber security provision designed to improve the integrity of consumer data and a provision addressing the interplay between the U.S. privacy protection and those of other countries.

And finally, my colleagues, the bill fosters self-regulatory programs by defining the outer parameters of what would constitute an acceptable privacy program.

I think all of us in the aftermath of the September 11 terrorist attack, the American people and the government, have understandably focused on enhancing security. Although protecting our citizens is the top priority of Congress, I do not want to see the issue of consumer information privacy overwhelmed by the events of 9/11. Even as a Nation wages war on global terrorism, it is appropriate that Congress still considers the matter of information privacy.

I will conclude by stating that I think we have a balanced and bipartisan bill, and the American consumer is empowered with information about what is done with his or her personally identifiable information so that he or she can make an informed choice. Commerce, in turn—and this is very important—is spared the undue burden of regulation that could follow.

So I look forward to our witnesses, and I want to thank them.

And the gentlelady from California.

Ms. HARMAN. Thank you, Mr. Chairman. I have obviously advanced in seniority on this committee at a rapid rate, and I appreciate it. I want to apologize, first, to you and Mr. Boucher and our witnesses for the fact that I must leave at 9:45. I am a member of what's called the Joint Inquiry—it sounds very British to me—which is looking into the plot of 9/11 and what reforms we might be able to make; and while I agree with you that 9/11 should not shape our views on every issue, it certainly does seem to me that we must still focus on it and the threats that may come after it.

But when I leave, I will hand over this ranking position to Mr. Boucher, a senior member, a real senior member of the full committee and a cosponsor of this bill; and I trust that you will agree that he will ably carry out these duties.

I want to commend you for the efforts you made before you introduced the bill to reach for all the members of the subcommittee. I was one of the people reached for. You asked me my views, you urged me to cosponsor the bill; and at that time I said that I thought it was a good bill, but I would prefer to hold off in order to reflect very carefully on whether you had achieved a balance that I thought would work between the need to foster technology and the need to protect privacy.

Having thought about it for a couple of months, I thought I would come to your hearing to tell you that I have now decided to cosponsor the bill.

Mr. STEARNS. Appreciate your support.

Ms. HARMAN. Well, you are welcome.

And I appreciate the way you worked on this and I appreciate the fact that you have put together a very able panel, which I am sure will make suggestions to us that could improve this product further.

I don't think you are claiming perfection here, Mr. Chairman. As a mother of four, I often say that perfection is not an option. But I think you have a very good working document, and if better ideas are suggested, I am sure you will be open to better ideas.

So I just want to say that I am proud to cosponsor your legislation. I think this is an excellent panel, and I look forward to getting smarter as we hear from these witnesses.

And finally, I would like to ask unanimous consent that any other members' opening statements be inserted into the record.

Mr. STEARNS. By unanimous consent, so ordered.

And I thank the gentlelady from California, Ms. Harman, for your support; and I think you know, you are not a senior member in the one sense, but you are senior in another since you have been here twice, and that creates a lot of wisdom which a lot of us don't have.

So—having run for Governor, you bring to the table a lot of perspective, and so your support will be very helpful, I think, for a lot of our colleagues.

Ms. HARMAN. I thank you for that. I would just observe, however, that I call myself the repeater in Congress; and it may make me smarter or it may make me dumber for going through this again.

Mr. STEARNS. It is my pleasure to welcome an opening statement from Mr. Boucher from Virginia, who is an original cosponsor with me and has been very helpful in the whole development of this bill. So a lot of the credit for this bill also comes from his participation, and I welcome his opening statement.

Mr. BOUCHER. Well, thank you very much, Mr. Chairman. I appreciate your inviting me to take part in the hearing today. While not a member of this subcommittee, I have a deep and abiding interest in this subject matter. And I am pleased to take part in the hearing.

I want to commend you, Mr. Chairman, for your leadership in the development of the privacy measure we have before us, and I am pleased to be an original coauthor of the measure. The bill would establish a baseline set of guarantees for personal privacy with respect to personally identifiable information collected by Web site operators and by off-line entities that use information for commercial purposes.

The requirements of the bill are straightforward and would be in the nature of a minimum set of guarantees. These guarantees protect consumers while promoting effective and unhindered electronic commerce. First, each Web site and off-line entity would be required to provide a clear locus of what information about consumers is collected and then how that information is used by the party that collects it.

As a second right, after reviewing the privacy statement, the consumer would be able to decline to have information about him collected. We commonly refer to this as an opt-out provision.

As a third matter, the Federal Trade Commission would be empowered to assure compliance with the basic privacy guarantees afforded.

And as a fourth matter, the legislation declares that these guarantees are the true national policy, and the bill preempts any inconsistent or more onerous requirements that would be imposed by

a State or local government. Were each of the 50 States to impose its own privacy laws, it would be exceedingly difficult, if not impossible, for companies doing business nationwide to comply with these varying requirements.

The bill also makes it clear that the baseline Federal guarantees set forth in this legislation do not affect other, more specific Federal privacy requirements. So if a particular industrial sector is subject to some other more precise Federal privacy regime, then that set of privacy laws would apply and the provisions of this bill would not.

A number of benefits will flow from passage of the measure. It would assure that all Web sites and commercial users of personally identifiable information respect privacy. While well-known commercial sites tend to be members of self-regulatory programs and generally respect the privacy rights of their users, many smaller Web sites do not belong to the SROs, and currently collect information about users without any privacy guarantees.

All Web site operators and off-line entities which collect information for commercial purposes other than some very small businesses and certain nonprofit entities would be covered by the bill that we are putting forward. By establishing only a minimum set of guarantees, the bill fully preserves the ability of conditions to offer higher levels of privacy and then market these increased protections as a competitive advantage.

In my experience, consumers use privacy along with convenience, quality, selection, price and other factors in order to distinguish among competing electronic commerce services. Enhanced privacy protection can become a true competitive asset to businesses that want to step up above the minimum guarantees required in the law.

Through the legislation that we are putting forth, Congress would also send the powerful message that both the privacy of our citizens as well the free flow of information for unencumbered global electronic commerce are of paramount concern. With the strong enforcement mechanisms in place in the U.S. and the specific enforcement mechanisms added by this bill the measure would assure a corset of enforceable privacy rights for American consumers.

Mr. Chairman, I think this a valuable effort, and I want to commend you for the work that you have done. It has been my privilege to partner with you in this, and I hope that we can succeed in passing the bill. Thank you.

Mr. STEARNS. I thank my colleague.

[Additional statements submitted for the record follow:]

PREPARED STATEMENT OF HON. CHARLES F. BASS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEW HAMPSHIRE

Thank you, Mr. Chairman, for holding this hearing and building on this subcommittee's impressive record of examining the issues relevant to privacy and the protection of consumers.

Mr. Chairman, as I look forward to today's testimony, I am anxious to hear from the many assembled witnesses, and will thus be brief.

I am a cosponsor of this H.R. 4678 because I believe it is the best effort any committee in either chamber has put forward to address the legitimate problems that exist for consumers. I am particularly pleased with the bill's:

- rejection of distinction between data collected offline and online;

- with its federal jurisdictional protection of what may well be inherently Interstate commerce; and
- significant further progress on identity theft.

The combined weight of these strengths plus the clarity the bill brings to the international trade arena make it an effort worth supporting. I look forward to the testimony and a later opportunity to use these comments to improve on this draft

---

PREPARED STATEMENT OF HON. W.J. "BILLY" TAUZIN, CHAIRMAN, COMMITTEE ON ENERGY AND COMMERCE

Thank you, Mr. Chairman, and let me commend you, first of all, for the extraordinary effort you and the Subcommittee members have put into this complex and intricate issue of consumer privacy. I believe this good work shows in the thoughtful, comprehensive new bill that is the subject of today's hearing.

One reason I am a cosponsor of H.R. 4678 is because of your careful consideration of the issue as you crafted this legislation: you have listened to all sides, all interested parties, and worked off an extensive record of some six privacy hearings held by this Subcommittee this Congress. The result, I believe, promises to be a significant enhancement of the privacy protections for American consumers when conducting commercial transactions.

The hearing process behind this bill brought out a fact that we must remember as we move forward: There are legitimate consumer concerns about how companies collect and use information. There are also actual abuses of consumer privacy occurring in the marketplace today. Whether or not such abuses cause direct harm, they can still harm consumer trust and confidence, which can produce a chilling effect on the expansion of goods and services available to consumers overall.

Of course, leading companies, often those with the biggest brand names, understand the value of protecting consumer privacy. They realize that making consumers comfortable about their privacy practices is good for business. They also understand that betraying consumer trust is business suicide. If all companies were like those leading the pack, then this legislation might not be needed.

But this is not the case. We know there are some bad actors, a small minority of companies and individuals causing the greatest grief for consumers. There is also a host of companies that haven't made privacy a priority for their business. And so I think there is need for targeted legislation to provide additional privacy protections for consumers.

This will provide a standard level of federal law to govern privacy of consumers in those areas not already covered by law. It brings everyone up to the level where the good guys already are. We are going to raise the tide.

H.R. 4678 embodies a principal that I think is essential for any new commercial privacy legislation: promote consumers' privacy without unfairly hampering current commercial activity and the vast consumer benefits generated by information sharing.

The many components of this bill align well with my position on privacy legislation. For example, I will not support a bill that takes a medium-specific approach to privacy, such as applying only to Internet transactions. Today's information collection activities are not bound by any one medium. Companies generally don't build separate databases or have differing privacy regimes based on the medium used to collect consumer data. And we should not legislate as if they do.

We also cannot have 50 different laws for information sharing, which will only stifle interstate commerce—a scenario that gets even worse if localities start to jump on the bandwagon. I'm pleased, Mr. Chairman, to see the bill takes a firm stance towards state preemption.

We must also ensure that consumers have the information they need to make educated decisions about the information collected and used about them. So I'm also pleased to see that H.R. 4678 includes a detailed process to empower and educate consumers about company privacy practices through notices and statements.

And given that the sale of information has been one of the strongest concerns raised during the hearings, the bill appropriately includes an important obligation to permit the consumer to preclude the sale of information from one company to another. But it doesn't mandate that this be either opt-in or opt-out—as broadly locking in this decision is not in the best interest of consumers.

Because privacy intersects so many difficult issues, the list of essential measures needed to navigate this terrain is too long to go into here. Suffice to say, I'm also pleased to see the bill takes solid, defendable stances on other necessary fronts.

It emphatically makes clear that self-regulation is a necessary part of the process. It includes a lengthy and extensive self-regulatory mechanism to allow privacy orga-

nizations to police the actions of its members with an FTC backstop, if necessary. This should increase compliance and ease the process consumers have to deal with to get a problem resolved.

On the legal front: The bill bans private rights of action, which will prevent harmful lawsuits and limit legal shenanigans. It is proper to do this because the bill includes strong authority for the FTC to take enforcement action against violators—and we expect vigilance by the FTC in this matter.

Lastly, the bill would deploy new information security obligations and has specific, targeted fixes for identity theft and an extensive provision dealing with the international aspect of this law. All are needed and worthy provisions.

I will encourage all Members to join this effort, and be part of this **bipartisan, balanced approach.** No one should assume that every word and comma of the bill is locked in stone. On the contrary, we will be open to discussions on how best to improve the bill—without gutting essential principles. If we work together perhaps we can work through any perceived shortfalls.

Let me add that we also have no set agenda for moving the bill. We will decide where to go after the hearing. As I stated during the privacy hearings last year, we are set on our own, determined course here. We certainly haven't designed this bill as a response to the Senate's work. This measure builds on our own thoughtful process.

Thank you again Mr. Chairman, and I look forward to the witness testimony.

Mr. STEARNS. We welcome our panel. John Palafoutas, Senior Vice President, Domestic Policy, AeA; Mr. Phillip Servidea, Vice President, Government Operations, NCR; John Schall, Executive Director, National Business Coalition on E-Commerce and Privacy; Ms. Rebecca Whitener, Director of Privacy Services, EDS Security & Privacy Services; Ms. Jennifer Barrett, Chief Privacy Officer, Acxiom; Paul Misener, Vice President, Global Public Policy, Amazon.com; and Mark Rotenberg, the Executive Director of Electronic Privacy Information Center.

Let me thank all of you for coming, and I welcome your opening statements. We will just start from my left to my right.

STATEMENTS OF JOHN P. PALAFOUTAS, SENIOR VICE PRESIDENT, DOMESTIC POLICY AND CONGRESSIONAL AFFAIRS, AeA; PHILIP D. SERVIDEA, VICE PRESIDENT, GOVERNMENT AFFAIRS, NCR CORPORATION; JOHN A. SCHALL, EXECUTIVE DIRECTOR, NATIONAL BUSINESS COALITION ON E-COMMERCE AND PRIVACY; REBECCA WHITENER, DIRECTOR OF PRIVACY SERVICES, EDS; JENNIFER BARRETT, CHIEF PRIVACY OFFICER, ACXIOM CORPORATION; PAUL MISENER, VICE PRESIDENT, GLOBAL PUBLIC POLICY, AMAZON.COM; AND MARC ROTENBERG, EXECUTIVE DIRECTOR, ELECTRONIC PRIVACY INFORMATION CENTER

Mr. PALAFOUTAS. Thank you, Mr. Chairman. The first thing I want to do is comment on the process that you employed on this bill, which I think was extremely important. People forget in the swirl of Internet privacy and the Internet that the Internet is a new—it is a new medium. It is a new industry. It is 8 years old.

And there has been a lot of hyperbole, both on our side and on other sides, of the Internet and its use. And the process that you and the Democratic members employ on this bill was extremely important because you brought consumer groups in, privacy act advocates and the high tech industry. And I can't tell you how important that was as a model for this body, and I hope for the other body, to use in coming up with good privacy legislation.

We face this problem all the time at AeA. As you know—and you spoke to our board, Mr. Chairman, on this bill a few months ago—

AeA is one of the largest high tech trade associations in the country. And the reason we got involved in this early is because we have operations in 18 cities around the country and we lobby in a dozen States. And our board became concerned because we saw the proliferation, the possible proliferation, of privacy rules at the State level and this concerned us because the big question of interstate commerce and the proliferation of 50 State regimes on privacy is extremely—of great concern to us.

And it is amplified by the fact that some of the State legislatures are only meeting part-time, and while they are good decent people, they are not spending the time that this body can in coming up with the kind of legislation, getting the kind of background that we need on this.

We saw this most clearly this past summer in Minnesota. Minnesota and California have been the first two States to pass Internet privacy laws. The Minnesota model is the one that scares industry the most. It was done in a politically overheated atmosphere. It was not a bipartisan bill. It was being pushed through as part of the election year, and we got what we consider as pretty bad legislation. In fact we are going to spend a lot of resources, both time and money, in taking this bill to court because of the issues that it brings up.

And we are glad that this bill, with its strong preemption, is going to provide the kind of context that the industry needs, because now that we have a bill in California and a bill in Minnesota, what we are concerned about at AeA is that we are going to see more and more States using these as a template, and they are going to go out—and now that this is the floor, they are going to start to implement other legislation that really causes a great concern to our industry. And because of, again, our large lobbying activity at the State level, we have seen that legislatures are not focused on this as they should.

The other thing that this bill highlights—and it is important for the members to see—is, nobody is more concerned about consumer confidence than our member companies. I need to say that again. Nobody is more concerned about consumer confidence than our member companies. If consumers don't have confidence in a Web site, they are going to go somewhere else. If they think that their information is being misused, they are going to go somewhere else. And I think what your bill has done is strike a proper balance in saying, Here's the rules; but, consumers, you have responsibilities too.

So in both the preemption and in the choice provisions we see very strong and important provisions because we believe that consumers should have a choice. But it is a choice that is dictated between them and the provider of the service that they are getting over the Internet, whether it is—in this case, you provide for an opt-out, which I think is very important.

Certain companies in our industry have an opt-in model for their business model. We think that is perfectly appropriate. But it should be part of that implicit and probably sometimes explicit contract that the companies have with the consumer.

Your bill comports with our privacy principles that we have outlined in our written testimony and we have conveyed to your staff.

And I have to comment a little bit on your staff. I state in my written comments the persistence and professionalism of Ramsen. He has indeed been a junkyard dog on many of those issues in making sure that the committee is getting all the information that it should have. So I couldn't go by without making that comment.

As I said, generally speaking, this bill hits our principles. One—two issues that we are concerned about are the—what we consider excessive penalties in the enforcement provision, the fact that in—actually three—the fact that this does not cover government Web sites which—and also nonprofits. I remind you that AeA is a nonprofit organization and we do use information at times. And we do have, as I mention in my comments and I am sure you will hear from the other panelists, concerns about the Safe Harbor and the EU privacy directive.

But we applaud you for this bill. It is a very strong bill, and we look forward to working with you in the next Congress to make it even stronger.

[The prepared statement of John Palafoutas follows:]

PREPARED STATEMENT OF JOHN PALAFOUTAS, SENIOR VICE PRESIDENT, DOMESTIC POLICY & CONGRESSIONAL AFFAIRS, AEA

INTRODUCTION

Mr. Chairman, Members of the Committee, I thank you for the invitation to appear today to discuss the need for stronger federal protections for consumer privacy, and comment specifically on H.R. 4678, the "Consumer Privacy Protection Act of 2002."

My name is John Palafoutas, and as AeA's Senior Vice President of Domestic Policy and Congressional Affairs, I have responsibility for policy implementation of AeA's Internet privacy initiative, as directed by our Board of Directors.

By way of background, AeA is the nation's largest high-tech trade association. AeA represents more than 3,000 companies with 1.8 million employees. These 3000+ companies span the high-technology spectrum, from software, semiconductors, medical devices and computers to Internet technology, advanced electronics and telecommunications systems and services. With 17 regional U.S. councils and offices in Brussels and Beijing, AeA offers a unique global policy grassroots capability and a wide portfolio of valuable business services and products for the high-tech industry. AeA has been the accepted voice of the U.S. technology community since 1943. If you'd like more information about us and our mission, you can visit our website at www.aeanet.org.

Mr. Chairman and Mr. Towns, I especially want to thank you both for your leadership on the issue of Internet privacy. By seeking out information from all corners—consumer groups, privacy advocates, and the high tech industry—you have shown your commitment to creating bipartisan legislation that is well rounded and responsive to the concerns of all. I also wish to commend your committee's Majority Counsel, Ramsen Betfarhad. In his persistence and professionalism, he has served this Committee well.

Privacy is an especially important topic for our member companies, as you may recall Mr. Chairman when you spoke at our Board of Directors meeting in May of this year. Every one of our member companies' businesses revolves around the Internet in one way or another. Protecting online consumers is of paramount importance to our companies. It is for this reason that AeA has been championing the cause of strong, non-discriminatory pre-emptive federal privacy legislation for almost two years now—something that no other trade association can lay claim to.

As use of the Internet continues to grow, online vendors are gathering more information about the purchasing habits of their customers. The increase in the collection and use of this data has raised public concern over precisely what information is being collected about consumers, how that information is being used, and whether it is being transferred to third parties. As a result, addressing concerns related to the collection and use of consumer information is becoming of increasing importance to legislators at the state and federal levels.

E-commerce continues to be one of the driving forces behind the growth of the U.S. and world economy. Online companies collect a tremendous amount of informa-

tion about customers in order to provide discounted goods and services, efficiently target niche markets, and notify customers of new products and services. Furthermore, these personal information databases are a valuable business asset for online companies. These companies use the databases not only to promote their own products, but oftentimes transfer this information to third party marketers. This allows companies to obtain and attract additional revenue and funding for their operations. However, surveys show that consumers are concerned over how their information is collected, used, and distributed.

Policy makers face a dilemma in addressing two very legitimate needs. On one side of the balance is the very real need for consumer privacy, and on the other, the constructive actions business has undertaken in numerous self-regulatory solutions. The role of government is to be the balance point in the middle—assuring that effective and enforceable solutions are implemented fairly, without jeopardizing the beneficial uses of this information by online companies. Caution must also be taken to assure against the adoption of burdensome regulations that could impede the continued growth of online commerce or patchwork state level solutions that are neither consonant nor enforceable across a borderless medium.

The imposition of stringent privacy regulations on the Internet could severely slow down the projected e-commerce growth. The Department of Commerce predicts e-commerce to pass $300 billion by the end of this year while some in private industry are predicting numbers much higher. It is for this reason that we have put considerable thought and effort into our privacy principles.

AEA'S PRIVACY PRINCIPLES

We first released our Privacy Principles in January of 2001 in order to guide federal policy makers in considering balanced, pre-emptive privacy legislation that is sensitive to the needs of consumers and to the Internet's economic and technical realities. These principles have been crafted from input and advice garnered from AeA's member companies, our Grassroots Network, and responses from town hall meetings across the country. Overwhelmingly, the responses all identified the grim possibility of multiple and conflicting state privacy regulations as their top legislative concern.

Federal preemption legislation plays a crucial role in ensuring consistency and certainty into the marketplace. The passage of Internet privacy legislation this past year in California and Minnesota highlights the growing need for preemption legislation. The inherent danger is both imminent and profound. Other states are now looking to make a template of these new laws—laws that are provincial in nature and unconcerned with their deleterious impact on interstate commerce.

Further, only the federal government is in a position to create uniform U.S. privacy standards that not only protect American consumers, but that will harmonize with international privacy directives. Federal legislation should not, however, attempt to replace or impede constructive private sector efforts, but rather build upon the baseline that they have laid down.

What good federal preemption language will do is protect consumers without imposing burdensome, impractical new requirements. Poorly crafted legislation will translate into higher consumer costs, fewer online services, and less free content—thus hurting the same consumers such legislation intends to benefit.

Mr. Chairman, because this legislation largely comports with AeA's Privacy Principles, AeA believes that H.R. 4678 is generally good legislation, and with some technical adjustments, it is something I believe AeA member companies may support.

Legislation Should Ensure National Standards. H.R. 4678 Does This. The Internet is a new and powerful tool of interstate commerce. Public policies related to Internet privacy should be national in scope, thus avoiding a patchwork of state and local mandates. This uniform framework will promote the growth of interstate e-commerce, minimize compliance burdens, sustain a national marketplace and make it easier for consumers to protect their privacy.

H.R. 4678 successfully preempts state and local statutory law, common law, and rules and regulations dealing with the use of personally identifiable information (PII) in interstate commerce.

Legislation Should Not Discriminate Against the Internet. H.R. 4678 Doesn't. Consumers should have confidence that their privacy will be respected regardless of the medium used. Similar privacy principles should apply online and offline. Public policy should not discriminate against electronic commerce by placing unique regulatory burdens on Internet-based activities.

H.R. 4678 makes no distinction between the online and offline worlds.

Legislation Should Provide Individuals with Notice. H.R. 4678 Does This. Web sites that collect personally identifiable information should provide individuals with clear and conspicuous notice of their information practices at the time of information collection. Individuals should be notified as to what type of information is collected about them, how the information will be used, and whether the information will be transferred to unrelated third parties.

Because H.R. 4678 requires data collectors who sell customer PII to post notice at the time of data collection, consumers will know that the collector's practices may raise an issue of consumer privacy, and allows them to find out exactly what those practices are. Further, H.R. 4678 sets out the requirements for what the notice must contain, as well as allowing the FTC to issue guidelines and advisory opinions.

Legislation Should Ensures Consumer Choice. H.R. 4678 Does This. Consumers should have the opportunity to opt out of the use or disclosure of their personally identifiable information for purposes that are unrelated to the purpose for which it was originally collected. Consumers should be allowed to receive benefits and services from vendors in exchange for the use of information. It is important that the consumer understands this use and is able to make an informed choice to provide information in return for the benefit received.

H.R. 4678 mandates that all data collectors *shall* allow consumers to opt-out of the sale of their PII to non-affiliated third parties, and the withholding of consent will last five years.

Legislation Should Leverage Market Solutions. H.R. 4678 Does This. Private sector privacy codes and seal programs are an effective means of protecting individuals' privacy. Lawmakers should recognize and build upon the self-regulatory mechanisms the private sector has put in place and continues to build. These mechanisms are backed by the enforcement authority of the Federal Trade Commission and state attorneys general. Public policies also should allow organizations to implement fair information practices flexibly across different mediums and encourage innovation and privacy enhancing technologies.

H.R. 4678 rewards participation in recognized seal programs by placing the burden of proving non-compliance on the FTC, as well as allowing for the use of binding private arbitration.

Legislation Should Utilize Existing Enforcement Authority. H.R. 4678 Does This. With the imposition of notice requirements, the Federal Trade Commission should use its existing authority to enforce the mandates of federal legislation. Legislation should not create any new private rights of action.

H.R. 4678 provides that any violation will be an unfair or deceptive act under § 5 of the Federal Trade Commission Act, thus not adding new sanctions into the already expanding pantheon of penalties. However, H.R. 4678 imposes strict monetary penalties that we believe are excessive, especially the doubling of civil penalties.

Legislation Should Avoid Conflicting or Duplicative Standards. H.R. 4678 Does This. In cases where more than one government agency seeks to regulate the privacy practices of a particular organization or industry, those agencies should offer a single coordinated set of standards.

H.R. 4678 ensures that organizations complying with other federal privacy laws dealing with the protection of a consumer's PII are deemed to be in compliance with this act.

AEA DOES HAVE SOME CONCERNS WITH H.R. 4678:

H.R. 4678 Does Not YET Protects Consumers in the Public and Private Arena. Government and non-profit organizations collect a tremendous amount of personally identifiable information about citizens. The need to foster consumer confidence applies to private and public sector activities. Government agencies and non-profit organizations that collect personally identifiable information should be required to follow fair information practices imposed on the private sector by law or regulation. It is well known that consumer information gleaned from government websites is often traded to third-parties without notice or consent. We believe this to be an unacceptable practice. H.R. 4678 should hold all government websites—federal, state, and local—to the same high standards imposed upon private industry.

H.R. 4678 May Have a Negative Impact on the EU Data Protection Safe Harbor. Back in 2000, a safe harbor was negotiated that would provide U.S. companies with protection from the EU Data Protection if they agreed to abide by the privacy principles included in the Safe Harbor. The EU only agreed to the U.S.'s self-regulatory approach if the FTC provided the enforcement mechanism for those companies that signed up for the safe harbor. As it stands today, 242 American corporations have signed up for the Safe Harbor, and many of those companies are AeA Members. Further investigation needs to be undertaken to determine if H.R. 4678

will harmonize with the EU Data Directive, and if it doesn't then if it will not jeopardize the negotiated Safe Harbor now in place. It is one thing to say that we are in compliance with the European Data Directive, and it is quite another to convince the Europeans of that fact.

We believe that while these concerns are not fatal to the bill at hand, they do present very important questions that do need to be addressed before our unqualified support can be given to H.R. 4678. My staff and I will be happy to work with you and the Subcommittee in taking up these issues.

Mr. Chairman, thank you for the opportunity to testify on H.R. 4678. AeA looks forward to working with the Committee in developing—and passing—practicable consumer privacy protection, if not in this Congress then in the next. I would be pleased to answer any questions that you may have.

Mr. STEARNS. I thank you.

Mr. Servidea.

STATEMENT OF PHILIP D. SERVIDEA

Mr. SERVIDEA. Mr. Chairman, Representative Harman, members of the subcommittee, I am Phil Servidea, Vice President of Government Affairs for NCR Corporation. Thank you for the invitation to testify before your subcommittee today.

NCR's heritage for providing solutions for retail and financial industries goes back almost 120 years to its founding as the National Cash Register Company. Today, NCR is one of the world's largest suppliers of solutions that enable transactions between consumers and businesses, be it in stores, through self-service terminals or over the Internet.

Mr. Chairman, NCR's corporate slogan, "Transforming Transactions Into Relationships," speaks to the importance we place on consumer protection in our solutions. So the subject of today's hearing is important to NCR as it is to all of us, since we are all consumers.

I am also the working chair of the Privacy Task Force of the Computer Systems Policy Project, or CSPP. CSPP is the Nation's leading advocacy organization, comprised exclusively of CEOs of the information technology industry. We have worked closely with the chairman and the committee staff in the formation of H.R. 4678.

We commend the chairman on the deliberative process used to craft the legislation. Businesses collecting information about their customers is not new. Your grandmother's butcher probably knew not only her name and her favorite cuts of meat, but also how the children were doing in school. We used to call it friendly, personal service at a time when businessmen and their customers were also neighbors.

Today, technology makes it possible for companies thousands of miles away to also serve their customers better. The growth of data collecting is fueling the global debate over privacy, creating a tension between consumers sharing personal information and businesses' attempts to serve them more effectively and personally.

The benefits to consumers of personalized service and the protection of their personal data are not incompatible. Consumers should and must have control over the use of their personal data. The protection and appropriate use of personal information is a growing concern for consumers and businesses alike. To ensure continued success and growth, it is important for companies to address privacy as an important consumer expectation.

One fundamental necessity of commerce, both traditional as well as e-commerce, is trust. Without trust, businesses cannot survive. Businesses that do not heed the expectations of their customers will quickly lose trust, and ultimately their viability. Quite simply, the business of privacy is good business.

Consumers in control of their data may freely choose the release of their personal information in return for better choices or services. I suspect that each of us as airline passengers would not mind being offered an upgrade at the gate because the airline agent knows that we experienced a flight cancellation days earlier.

Most companies are doing the right thing in providing privacy options. But as long as there is potential short-term gain in abusing personal information, can we count exclusively on company volunteerism to prevent abuse. While many company executives shudder at the thought of more regulation, their companies and their customers alike will be better served if industry and government work together toward rational and uniform rulings that are fair to all.

NCR believes that the right legislation built on top of market-driven solutions can assure that all consumers are afforded this protection.

Presently Federal privacy laws exist which govern specific industry sectors, protect sensitive information and target specific harmful or fraudulent behaviors. But in the U.S. there is no single, broad-based law that affects the use of personal data, which is why we are here today.

But what type of legislation can work? The CSPP has advanced a set of four principles for such legislation. I would like to comment on two of those. First, legislation must be comprehensive and apply with appropriate flexibility to personal data, whether collected on-line, over the telephone or in face-to-face commercial transactions. To enact legislation that applies only to on-line activities would mislead the American consumer.

As a supplier of business intelligence solutions, NCR knows, as the chairman said, that click-and-mortar firms do not distinguish between personal data obtained through different channels. Further, on-line transactions account for only a small fraction of consumer transactions, last year less than 1 percent. Also, as technologies merge, such as the Internet and wireless technologies, the distinction between online and offline is blurring.

Simply put, when it comes to customer's rights, data is data.

Second, the legislation must recognize that markets, particularly on the Internet, are national in scope. One only need recall the endless mailings from banks implementing Gramm-Leach-Bliley to imagine the morass of legal uncertainty that would ensue if both State and Federal legislation purported to govern consumers' rights for personal data protection. Federal legislation in this area should preempt State and local law.

Mr. Chairman, and Ranking Member Towns, while I have commented on only two principles, I am proud to say that your bill, overall, effectively balances consumer and business interests. H.R. 4678 requires clear and conspicuous disclosure of businesses' privacy practices and enables individuals to make informed choices about sharing their personal information.

During NCR's long history, a lot of things have changed, but its philosophy has not. If you want your customers' trust, you have to respect your customers' privacy. In summary, NCR is pro-privacy. H.R. 4678 is a step in the right direction, and we look forward to working with the subcommittee toward the bill's enactment.

Thank you, Mr. Chairman, for holding this hearing today. Thank you for your hard work on drafting H.R. 4678.

[The prepared statement of Philip D. Servidea follows:]

PREPARED STATEMENT OF PHILIP D. SERVIDEA, VICE PRESIDENT OF GOVERNMENT AFFAIRS, NCR CORPORATION; CHAIR, NETWORKED WORLD COMMITTEE, COMPUTER SYSTEMS POLICY PROJECT

Mister Chairman, Representative Towns, and members of the Subcommittee, I am Phil Servidea, Vice President of Government Affairs for NCR Corporation. Thank you for the invitation to testify before your Subcommittee today.

NCR's heritage in providing solutions for retail and financial industries goes back almost 120 years to its founding as the National Cash Register Company. Today, NCR is one of the world's largest suppliers of solutions that enable transactions between consumers and businesses, whether in stores, through self-service terminals, or over the Internet.

Mister Chairman, NCR's corporate slogan, "Transforming Transactions Into Relationships", speaks to the importance we place on consumer protections in our solutions. So, the subject of today's hearing is important to NCR, as it is to all of us since we are all consumers.

I am also the Working Chair of the privacy task force of the Computer Systems Policy Project, or CSPP. CSPP is the nation's leading advocacy organization comprised exclusively of CEOs of the information technology industry. We have worked closely with the Chairman and Committee staff in the formation of HR 4678. We commend the Chairman on the deliberative process used to craft this legislation.

Businesses collecting information about their customers is not new. Your grandmother's butcher probably knew not only her name and her favorite cuts of meat, but how the children were doing in school, as well. We used to call it "friendly, personal service" at a time when businessmen and their customers were also neighbors.

Today, technology makes it possible for companies thousands of miles away to also serve their customers better. The growth in data collecting is fueling the global debate over privacy; creating a tension between consumers' sharing personal information and business' attempt to serve them more effectively and personally.

The benefits to consumers of personalized service and the protection of their personal data are not incompatible; consumers should and must have control over the use of their personal data.

The protection and appropriate use of personal information, is a growing concern for consumers and businesses alike. To ensure continued success and growth, it's important for companies to address privacy as an important consumer expectation. One fundamental necessity of commerce, both traditional as well as e-commerce, is trust. Without trust, businesses cannot survive. Businesses that do not heed the expectations of their customers will quickly lose trust, and ultimately their viability. Quite simply, the business of privacy is "good business".

Consumers in control of their data may freely choose the release of their personal information in return for better choices or services. I suspect that you as an airline passenger would not mind being offered an upgrade at the gate because the airline agent knows you experienced a flight cancellation days earlier.

Most companies are doing the right thing in providing privacy options. But as long as there is potential short-term gain in abusing personal information, can we count exclusively on company voluntarism to prevent abuse? While many company executives shudder at the thought of more regulation, their companies and their customers alike will be better served if industry and government work together toward rational and uniform rules that are fair to all. NCR believes that the right legislation built on top of market-driven solutions can assure that all consumers are afforded this protection.

Presently, federal privacy laws exist which govern specific industry sectors, protect sensitive information, and target specific harmful or fraudulent behaviors. But in the U.S. there is currently no single, broad-based law that affects the use of personal data, which is why we are here today.

But what type of legislation can work? CSPP advanced a set of core principles for such legislation. I would like to comment on two of those principles.

First, legislation must be comprehensive and apply, with appropriate flexibility, to personal data, whether collected online, over the telephone or in face-to-face commercial transactions. To enact legislation that applies only to online activities would mislead the American consumer. As a supplier of business intelligence solutions, NCR knows that click-and-mortar firms do not distinguish between personal data obtained through different channels. Further, online transactions account for only a small fraction of consumer transactions, last year less than one percent. Also, as technologies merge, such as the Internet and wireless technologies, the distinction between online and offline is blurring.

Simply put, when it comes to consumers' rights, data is data.

Secondly, legislation must recognize that markets, particularly on the Internet, are national in scope. One only need recall the endless mailings from banks implementing Gramm-Leach-Bliley to imagine the morass and legal uncertainty that would ensue if both State and federal legislation purported to govern consumers' right for personal data protection. Federal legislation in this area should preempt State and local law.

Mister Chairman and Ranking Member Towns, while I have commented on only two principles, I am proud to say that your bill overall effectively balances consumer and business interests. HR 4678 requires clear and conspicuous disclosure of business' privacy practices and enables individuals to make informed choices about sharing their personal information.

During NCR's long history, a lot of things have changed, but its philosophy has not—if you want your customers' trust, you have to respect your customers' privacy. In summary, NCR is pro-privacy. HR 4678 is a step in the right direction and we look forward to working with the Subcommittee toward the bill's enactment.

Thank you, Mister Chairman, for holding this hearing today and thank you for your hard work on drafting HR 4678.

Mr. STEARNS. And I thank you for your compliments.

Mr. Schall.

STATEMENT OF JOHN A. SCHALL

Mr. SCHALL. Mr. Chairman, thank you for the opportunity to discuss the Consumer Privacy Protection Act. I am John Schall, the Executive Director of the National Business Coalition on E-Commerce and Privacy. We are 15 widely recognized companies dedicated to the pursuit of a balanced and uniform national privacy policy.

We are engaged in virtually every sector in the economy and in every geographic location in the country, with over 40 million customers. We are both online and offline, and we are both financial and nonfinancial companies, companies like General Motors, John Deere, Home Depot, General Electric, Charles Schwab.

We believe that H.R. 4678 moves the privacy debate in a positive direction; and we would like to thank you, Mr. Chairman, for the enormous amount of work that you and your staff have put into crafting this legislation.

The straightforward step of letting consumers know how information is going to be used is the single most important thing we can do in the area of privacy. A well-informed customer is the heart of the matter because knowledge empowers the consumer.

I will focus my remarks today on three areas. One, creation of a uniform national privacy standard; two, the equal treatment of on-line and off-line information; and three, private rights of action.

A patchwork of State laws would pose a significant disincentive for companies that would be forced to navigate a sea of conflicting local laws. Mr. Chairman, over 548 bills were introduced in the 50 State legislatures this year dealing with privacy; that is 548 different approaches to what 50 different State jurisdictions ought to do with the single issue we are discussing here today. And if that

weren't enough, numerous local jurisdictions are now also jumping in to tackle the privacy question.

In Ms. Harman's home State of California, for example, San Mateo County and Daly City have both just passed their own privacy laws. And six more counties and cities in just the San Francisco area are expected to do so in the coming months, coming weeks. And surely there will be more after that.

Remember, there are almost 100,000 local government jurisdictions in the United States. I am not sure I even want to contemplate how a company could comply in 50 different States and 100,000 different localities.

I would also add that those who argue that they seek a Federal privacy law to create, quote, "a floor but not a ceiling" are begging the question of fundamental fairness. A world of floors and ceilings will result in conflicting standards that benefit some consumers and punish others merely because of geographic location. We wish to strongly impress upon the Congress, then, the urgent need to pass legislation that preempts both State and local laws and provides a uniform privacy standard across the Nation.

Second, all our companies operate both online and offline, and we are pleased that this bill treats both types of information in the same way. Making a distinction between online and offline would present real difficulty. As a general rule, all information collected by companies, either online or offline, is stored in the same system. No distinction is made based on where the information is collected.

And such a distinction becomes an exercise in hair-splitting. If information is collected in person and then stored online, is that online or offline? What if the information is transmitted from a telephone to a computer? I mean, these are the sorts of Solomonic judgments that could keep the courts busy for years.

Third, we are pleased that H.R. 4678 does not permit private rights of action at a time when everyone agrees that our society is already far too litigious. The Federal Trade Commission has recognized that existing enforcement authority deals with most violations of privacy law.

Opening the door to private rights of action would result in unnecessary lawsuits and a clogged legal system. Instead, H.R. 4678 more appropriately creates a Self-Regulatory Organization process with binding arbitration.

I would also point out that under this bill the States would still have private rights of action and the litigation authority vested in them through the many FTC acts.

Mr. Chairman, H.R. 4678 is the most promising alternative currently pending in the Congress. We would like to suggest, however, some potential sand traps to avoid and a few drafting improvements in the bill. For example, the opt-out provisions of the bill should apply to the use of information and not to the collection of information. Likewise, our companies who all deal in both on-line and off-line transactions and both the business-to-business and the business-to-consumer environments would like it to be more explicit that this bill applies to business-to-consumer relationships only. We believe it would also be helpful to prohibit class action lawsuits.

Finally, unnecessary access provisions are best avoided because they could, ironically, create perverse incentives for companies to centrally maintain exactly the sort of customer profiles that we all seek to avoid.

So, Mr. Chairman, on behalf of the National Business Coalition on E-Commerce and Privacy, I would like to congratulate you on striking a sensible balance between the privacy of the consumer and the needs of the business community. And thank you.

[The prepared statement of John A. Schall follows:]

PREPARED STATEMENT OF JOHN A. SCHALL, EXECUTIVE DIRECTOR, NATIONAL BUSINESS COALITION ON E-COMMERCE AND PRIVACY

Mr. Chairman and Members of the Subcommittee, on behalf of the members of the National Business Coalition on E-Commerce and Privacy, I want to thank you for permitting me the opportunity to discuss our views on HR 4678, the Consumer Privacy Protection Act of 2002. We believe that this is an important piece of legislation with profound consequences not only for e-commerce specifically, but for the economy as a whole.

The National Business Coalition on E-Commerce and Privacy, of which I am the Executive Director, is comprised of 15 widely recognized companies dedicated to the pursuit of a balanced and uniform national policy pertaining to electronic commerce and privacy. We are engaged in virtually every sector of the economy and in every geographic location in the country, with over 40 million customers. We deliberately created a diverse coalition because the privacy issue is not just restricted to the financial services industry or the health care community, but touches on every sector of our economy.

We believe that we are the only coalition whose membership includes financial and non-financial companies. Our wide range of companies are in manufacturing, like General Motors and John Deere Corporation; retail, like Home Depot; hospitality, like Six Continents Hotels; media, like General Electric; as well as some insurance and financial services companies such as Charles Schwab. These and our other members are all top competitors in the e-commerce marketplace, who use the Internet as an essential component of their ability to deliver goods and services to their customers.

Our members have spent decades developing respected brand names and cultivating mutual trust with their customers, and I can assure every member of this Subcommittee that we are strongly committed to ensuring the privacy of our customers both on-line and off-line.

It is for that reason that we are very encouraged by the provisions of HR 4678. We believe this bill moves the privacy debate in a positive and useful direction, and the Coalition would especially like to thank you, Mr. Chairman, for the enormous amount of work that you and your staff have put into analyzing the complexities of the privacy issue and in crafting this legislation.

The Coalition is pleased that HR 4678 lays out a clear-cut and balanced privacy policy for the nation. By requiring the prominent posting of, and by requiring adherence to, a company's privacy policies, it is our view that HR 4678, more than any other piece of legislation currently before the Congress, assures that consumers have the information that they need in order to make informed choices about the use of personal information that pertains to them. A well-informed consumer is the heart of the matter because in a free market economy, knowledge empowers the customer. And we believe that the simple and straightforward step of letting consumers know how information is going to be used is the single most important and useful thing that we can do in the area of privacy.

I will focus my remarks today on three areas that our Coalition deems especially important: 1) the creation of uniform national privacy standards; 2) the equal treatment of off-line and on-line information; and 3) private rights of action. We are pleased to see that HR 4678 deals with each of these vital issues in a balanced and sensible way.

By creating uniformity of state and local privacy laws, we believe HR 4678 demonstrates an appropriate appreciation of the nature of e-commerce and the modern economy. An economy in which orders for new products and services can be made at the touch of a button. An economy that allows a customer in Oregon to purchase a product in Florida in a matter of mere seconds. An economy that is, in a very real way, an economy without borders.

A patchwork of state and local laws would pose an enormous burden to, and fragmentation of, our economy. This would be a significant disincentive for companies to participate in the e-commerce marketplace, especially smaller companies, since they would be forced to navigate a sea of sometimes conflicting state and local privacy laws. Furthermore, the costs of complying with such conflicting laws would, more likely than not, be passed on to the consumer.

Mr. Chairman, in the 50 states this year, over 548 privacy bills were introduced in the state legislatures. That's 548 different approaches to what 50 different state jurisdictions ought to do about the single issue we're discussing here today.

And if that weren't enough, numerous local jurisdictions are now also jumping in and beginning to tackle the question of privacy. For example, in the State of California, San Mateo County and Daly City have both just passed their own privacy laws, with San Francisco, Berkeley, Marin County, Contra Costa County, and Alameda County all expected to do so in the coming weeks. And that's within just the San Francisco Bay Area. Surely there will be more after that. Remember, there are almost 100,000 local government jurisdictions in the United States. I'm not sure I want to even contemplate how a company could comply with 50 states multiplied by 100,000 localities multiplied by a minimum of 548 different privacy policies.

Obviously, this is a recipe for a disjointed and inefficient marketplace. We, therefore, wish to strongly impress upon the Congress the urgent need to pass legislation with strong Federal preemption of both state and local laws. We believe that only by effectively providing a uniform privacy standard across the nation, will the Congress be able to avoid the problems that would accompany a multitude of legal requirements, with all of the ultimately unworkable administrative requirements that would imply.

I would also add, Mr. Chairman, that those who argue that they seek a Federal privacy law to create "a floor but not a ceiling," are begging a fundamental question of fairness. If privacy is to mean anything it is as a guarantee of certainty that consumers may know the rules of the road wherever they go in our economy. Far from being a protection of privacy, the "floor and not a ceiling" argument will result in confusion and conflicting standards that will benefit some consumers and punish others almost at random because of the mere accident of geographical location. In the world of floors and ceilings, where you live will be more important to your privacy than who you are.

Secondly, the Coalition is greatly pleased to see that HR 4678 treats information gathered on-line and off-line in the same way. Every one of our member companies operates both on-line and off-line, as does, I assume, almost every major American company, as well as a number of smaller ones. While we appreciate that those Members of Congress who seek to make a distinction between on-line and off-line information believed that they are assisting certain portions of the business community, the truth is that doing so, in fact, would be enormously burdensome and presents some very real difficulties.

To begin with, as a general rule, all information collected by companies either on-line or off-line is stored in the same system. Often no distinction is made based on where the information is collected. To create such a distinction in law would be to invite enormous record keeping and financial burdens for private industry, to no practical real world benefit for the consumer.

Furthermore, to create such a distinction becomes an exercise in the most profound hair splitting. Is information collected in person and then stored online considered online or offline? What if the information is collected over the telephone, or through a computer? Or transmitted from a telephone to a computer? These are the kinds of Solomonic judgments that will keep the courts busy for years if a distinction is made between on-line and off-line information.

By treating similar information gathered on-line and off-line in the same way, HR 4678 sensibly balances the needs of industry with the privacy of the consumer, and assures the protection of both with a minimum of ambiguity.

Thirdly, we are greatly pleased that HR 4678 does not permit private rights of action at a time when everyone agrees that our society is already far too litigious. The Coalition is well aware that this matter of private rights of action will be highly controversial and is an outgrowth of broader legal reform issues facing the Congress. But the likely result of a private right of action would be to dissuade companies from relying on e-commerce, or more likely, it would cause them to hedge their bets against frivolous lawsuits by adding costly procedures and protections. Such procedures and protections would not measurably aid consumers, but their costs would be passed on in the form of higher prices and reduced service.

In the context of privacy, there is concrete evidence to show that existing law has more than sufficed to protect consumer interests. The Federal Trade Commission has recognized that existing enforcement authority deals with most violations of pri-

vacy law and opening the door to private rights of action would simply create an environment conducive to even more unnecessary lawsuits in an already clogged and expensive legal system. I would also point out that under this bill, the states would still have existing private rights of action and the litigation authority already vested in them through the mini-FTC Acts.

Instead of creating a new private right of action, HR 4678 more appropriately creates a Self Regulatory Organization (SRO) process in which arbitration may be binding. This possibility of binding arbitration is critical—otherwise the SRO process would represent little more than yet another expensive layer of compliance.

Mr. Chairman and Members of this Subcommittee, HR 4678 is a reasoned and measured step forward in the privacy debate, and the most promising alternative currently pending in the Congress. We would like to suggest, however, some potential sandtraps to avoid and some drafting improvements to HR 4678, where possible.

For example, we would highlight the need to apply the opt-out provisions of the bill to the use of information, rather than to the collection of information, as the bill currently requires. Likewise, our Coalition companies, who all deal in both the business-to-business and the business-to-consumer environments, would like it to be made more explicit that HR 4678 applies to business-to-consumer relationships and not to business-to-business transactions. With regard to remedies and enforcement, we believe that it would be helpful to explicitly prohibit class action lawsuits. Finally, unnecessary access provisions are best avoided because they could ironically create perverse incentives for companies to centrally maintain exactly the sort of customer profiles that we all seek to avoid.

Mr. Chairman and Members of this Subcommittee, once again, on behalf of the National Business Coalition on E-Commerce and Privacy, I would like to congratulate you on your leadership in successfully moving the privacy debate forward and in drafting HR 4678. We believe that with this legislation, you have taken a singularly positive step, and that you have struck a prudent and sensible balance between the privacy of the consumer and the needs of the business community. We hope to be able to continue to work with you as the privacy debate develops, and I would now be happy to answer any questions that you may have.

ATTACHMENT

NATIONAL BUSINESS COALITION ON E-COMMERCE AND PRIVACY

Member Companies: American Century Investments; AMVESCAP; CheckFree; CIGNA; Deere & Company; Dupont; Fidelity Investments; Fortis, Inc.; General Electric; General Motors; The Home Depot; Investment Company Institute; MBNA America; Charles Schwab & Company; and Six Continents Hotels

Mr. STEARNS. Yes, thank you, John.

Ms. Whitener. Welcome.

STATEMENT OF REBECCA WHITENER

Ms. WHITENER. Thank you, Mr. Chairman. It is a pleasure to be here today to discuss H.R. 4678, the Consumer Privacy Protection Act of 20020.

As Director of Privacy Services for EDS, I am responsible for the global strategy, the service line offering development and the methodology for EDS clients' focused privacy services.

Mr. Chairman, H.R. 4678 is a culmination of many hearings and discussions with people of different points of view. You have proceeded carefully and are to be commended for that approach. Your bill understands that the protection of privacy and data and the ability to share information are good for business and consumers alike.

EDS's Chairman and CEO, Dick Brown, is chairman of the Digital Economy Task Force of the Business Roundtable. That task force has made several recommendations on how we should proceed in ensuring that any legislative remedies do not impede electronic commerce.

First, do not hinder self-regulation efforts of industry to give consumers informed choice. By and large, industry has done a good job. If a company decides to share information in a perceived detrimental way, the market is pretty quick to act.

Second, ensure consistency and certainty in the marketplace through a national standard in rules. Without strong Federal preemption, there will be confusion among consumers, and business will reconsider engaging in electronic transactions.

Next, have one Federal agency responsible for regulating consumer privacy. Again, it is unrealistic to expect business and consumers to coordinate with multiple entities.

Four, treat e-commerce as any other form of commerce. The Internet is becoming so ingrained in business processes that e-commerce should not be singled out for any special regulatory treatment.

Fifth, keep a level, consistent playing ground between government and business. Do not prohibit the selling of information by ABC Book Company while allowing the Department of Motor Vehicles to sell driver's license information.

Finally, there should not be any new private right of action. It is just not necessary. The market and existing laws and regulations will do the job.

Mr. Chairman, H.R. 4678 goes a long way to meeting those requirements, and it encompasses much of what EDS has included in its global privacy and data protection policies. We are especially pleased to see that you have addressed security concerns in your legislation. Cyber security continues to be a growing problem and there are significant indications that more should be done to protect data and networks.

The numbers are staggering. In 2000 computer, viruses worldwide cost $17.1 billion in damages. EDS alone encounters more than 650 attempted break-ins and three new viruses every day on servers that it runs for 2,500 clients. A major virus like "Code Red" or "ILOVEYOU" costs billions to eliminate, the release last week of the President's National Strategy to Secure Cyberspace is a step in the right direction. It highlights many of the areas that must be addressed so that consumers can be confident that their transactions and information shared with government and businesses are secure.

Now onto some specific comments about section 105: In paragraph a(2) we agree with your requirement that senior management consider and improve an information security policy. Security awareness needs to be raised in the consciousness of senior management, and this will go a long way to that end.

Paragraph a(3)(B) makes a great deal of sense. Most organizations have someone responsible for IT security, but in many cases they aren't designated or there are unclear lines of responsibility.

Paragraph b(1), there are a number of sources that can be used for timely notification. We believe in flexibility as to the source of a notification and a corrective action taken, which is more clearly outlined in the exceptions in 105 b(2). This will provide a broadened approach based on company policy.

Paragraph b(1), corrective action implies that there is an effective process within an organization to monitor threat warnings and

know when to effectively apply remediation. This is a critical security capability.

In paragraph c the process for how the Commission will base the decision to hold the organization culpable in violating section 105 is unclear. We agree on the importance of the role placed on self-regulatory programs as defined in section 106.

In e, the requirement for regular compliance testing which shall take place not less frequently than every 4 years ensures self-reviews and self-certifications are accurate. Companies should be given the choice of addressing this compliance testing through their own internal audit programs, through privacy consultants and through public accounting firms.

We would be glad to work with your staff on these points.

Mr. Chairman, we appreciate the opportunity to testify on H.R. 4678. We want to continue working with you next year on this legislation. If it becomes necessary to pass a consumer privacy bill, then we want to make sure that it supports the growth of additional economy rather than placing roadblocks in the way and limiting those who can enjoy the benefits of the new economy.

Thank you.

[The prepared statement of Rebecca Whitener follows:]

PREPARED STATEMENT OF REBECCA WHITENER, DIRECTOR OF PRIVACY SERVICES, EDS SECURITY AND PRIVACY SERVICES

Thank you Mr. Chairman.

It is a pleasure to be here today to discuss HR 4678, the Consumer Privacy Protection Act of 2002.

I am Rebecca Whitener, Director of Privacy Services for EDS. In that capacity I am responsible for the global strategy, service line offering development, and methodology for EDS client-focused Privacy services. Prior to joining EDS, I was a co-founder and Chief Operating Officer of Fiderus, a Security and Privacy Consulting firm, and before that a Principal in charge of global privacy services at IBM. In my career, I have worked with companies around the world to develop business solutions for security and privacy. In 2000; I had the privilege of serving on the Federal Trade Commission Advisory Committee for Online Access and Security.

Privacy is one of those issues that generate a great deal of passion in any discussion. We Americans have always viewed privacy as a core principle of our society and democratic way of life. We hold privacy dear and defend it with great vigor when we believe it is threatened.

But the Digital Economy, with all its promises, poses interesting dilemmas on our view of privacy. For instance, do we consider an online bookseller sending us an e-mail about a release from our favorite author an invasion of privacy or effective marketing? Do we feel that the selling of information to a third party so that we can be made aware of a new product is an abuse of consumer trust or an important source of information?

Mr. Chairman, HR 4678 is the culmination of many hearings and discussions with people of different points of view. You have proceeded carefully and are to be commended for that approach. Your bill understands that the protection of privacy and data and the ability to share information, are good for business and consumers alike.

EDS' Chairman and CEO Dick Brown is chairman of the Digital Economy Task Force of the Business Roundtable. That task force has made several recommendations on how we should proceed in ensuring that any legislative remedies do not impede electronic commerce.

First, do not hinder self-regulation efforts of industry to give consumers informed choice. By and large, industry has done a good job. If a company decides to share information in a perceived detrimental way, the market is pretty quick to act.

Second, ensure consistency and certainty in the marketplace through a national standard in rules. Without strong federal preemption there will be confusion among consumers, and business will reconsider engaging in more efficient, electronic transactions. Many states are now pursing their own legislative remedies and the patchwork of laws that may emerge will surely be a roadblock to the Digital Economy.

Next, have one federal agency responsible for regulating consumer privacy. Again, it is unrealistic to expect business and consumers to coordinate with multiple entities.

Fourth, treat e-commerce as any other form of commerce. The Internet is becoming so ingrained in business processes that e-commerce should not be singled out for any special regulatory treatment. Unfortunately, there are those who seek to discriminate against this way of doing business.

Fifth, keep a level, consistent playing ground between government and business. Do not prohibit the selling of information by the ABC book company while allowing the Department of Motor Vehicles to sell drivers' license records.

Finally, there should not be any new private right of action. It is just not necessary. The market and existing laws and regulations will do the job.

Mr. Chairman, HR 4678 goes a long way to meeting these requirements. And it encompasses much of what EDS has included in its Global Privacy and Data Protection Policies.

There are, however, several specific issues I would like to highlight in certain sections of the bill.

In Section 101, Privacy Notices to Consumers, subsection b (Forms and Content of Notice), point two could also include a physical mail address as an option for obtaining a privacy statement. In that same subsection, point three would be strengthened if it read "If the notice is required under subsection (a)(2), a statement that there has been a material change in the organization's privacy policy, and where in the privacy policy the change(s) have occurred.

A comment on Section 109, Effect on Other Laws, subsection d. This is most welcome as we see states passing inconsistent privacy laws. The other thing we are seeing is that some counties and even cities are contemplating passing laws because they don't think the state laws do the right job. If cities start doing the same thing then we will never know what law prevails. Preemption must be part of any legislation.

In the Improved Identity Theft Data section, a reflection of some of the best practices that are starting to appear in the proposed state measures may be useful, particularly as they relate to the use of social security numbers.

In Section 304, Harmonization of International Privacy Laws, Regulations and Agreements, the approach is on target. Businesses should have the freedom to operate globally under harmonized laws. Processes that leave the door open for a claim of inadequacy and that continue a bilateral agreement do little to promote e-commerce.

We are especially pleased to see that you have addressed security concerns in your legislation. Cyber security continues to be a growing problem and there are significant indications that more should be done to protect data and networks.

The numbers are staggering. In 2000, computer viruses worldwide cost $17.1 billion in damages. EDS alone counters more than 650 attempted break-ins and three new viruses every day on servers it runs for 2500 clients. A major virus like Code Red or ILOVEYOU costs billions to eliminate.

The release last week of the President's National Strategy to Secure Cyberspace is a step in the right direction. It highlights many of the areas that must be addressed so that consumers can be confident that their transactions and information shared with government and business are secure.

As part of our education effort on the urgency of protecting our economic infrastructure, we are submitting a high level security and privacy checklist that can be used by companies, organizations and governments. It may seem simple and straightforward but we find a number of entities needing advice about the basic steps.

Now on to some specific comments about Section 105.

In paragraph a(2) we agree with the requirement that senior management consider and approve an information security policy. Security awareness needs to be raised in the consciousness of senior management and this will go a long way to that end.

Paragraph a(3)(B) makes a great deal of sense. Most organizations have someone responsible for IT security but in many cases they aren't designated or there are unclear lines of responsibility.

Paragraph b(1): There are a number of sources that can be used for timely notification. We believe that flexibility as to the source of the notification and the corrective action taken, which is more clearly outlined in the Exceptions in 105(b)(2). This will provide a broadened approach based on company policy.

Paragraph b(1): Corrective action implies that there is an effective process within an organization to monitor threat warnings and know when to effectively apply remediation. This is a critical security capability.

In Paragraph c, the process for how the Commission will base a decision to hold the organization culpable in violating Section 105 is unclear.

We agree on the importance of the role placed on self-regulatory programs as defined in Section 106. In (E) the requirement for "regular compliance testing which shall take place not less frequently than every 4 years" to ensure self-reviews and self-certifications are accurate. Companies should be given the choice of addressing this compliance testing through their own Internal Audit programs, through privacy consultants, and through public accounting firms.

We would be glad to work with your staff on these points.

Mr. Chairman, we appreciate the opportunity to testify on HR 4678. We want to continue working with you next year on this legislation. If it becomes necessary to pass a consumer privacy bill then we want to make sure that it supports the growth of the Digital Economy rather than placing roadblocks in the way and limiting those who can enjoy the benefits of the new economy.

I will be happy to answer any questions.

Thank you.

Mr. STEARNS. Thank you.

Ms. Barrett.

STATEMENT OF JENNIFER BARRETT

Ms. BARRETT. Thank you, Mr. Chairman.

Mr. STEARNS. I also want to thank you. I think you came the farthest to be here this morning.

Ms. BARRETT. Thank you. I guess I did.

Thank you, Chairman Stearns and members of the subcommittee. Thank you for the opportunity to again participate in your hearings and today share the perspective of three companies on Titles I and III of H.R. 4678. The companies are Acxiom Corporation, a leading provider of innovative data management services and technology; Experian Marketing Services, a division of Experian North America, a leader in enabling organizations to make fast, informed decisions to improve and personalize relationships with their customers; and third, Trilegiant Corporation, one of the Nation's largest direct mail marketers and member service providers. Our clients represent a who's-who of America's leading companies, and we are always proud of the reputation for helping them sell better products, smarter, faster and at a lower cost.

We strongly support a balanced approach to the use of personal information. We believe that the inappropriate use of information to defraud or discriminate must be illegal. At the same time, the free flow of information this Nation enjoys today has greatly contributed to our economic growth and stability. Because of information sharing, consumers have greater choice in variety, goods and services cost less, and transactions are completed faster and more easily.

First, we want to commend the committee for the extensive and thoughtful approach that it has taken in drafting this legislation. This committee has studied the complex issues involving consumer privacy to a greater degree than any other body of Congress, and your understanding of these issues is reflected in the bill.

One of the key questions in today's debate about privacy is whether legislation should be specific to the on-line sector or whether legislation should be particular, technology neutral, covering both on- and off-line. It is difficult to argue that a corporation's policies should be different in these two worlds since every growth-oriented company inevitably combines data from both. How-

ever, there are practical and important differences in how notice can be delivered and choice can be exercised.

In order to be fair to all mediums, the standard for providing a policy must be upon request. The interactive nature of the Internet allows a consumer to make an immediate informed choice about information use. However, this interactive model is difficult, if not impossible, to achieve in the off-line world.

We believe section 101 of the bill is intended to recognize and allow for these practical differences, and we want to continue to work with the committee to ensure that this upon-request distinction is clear in the law so that businesses have the necessary flexibility to conduct successful marketing campaigns in this difficult economic environment.

With regard to self-regulatory programs, section 106 of the bill recognizes the important role that these initiatives have played. Seal programs such as BBBOnline and TrustE, along with the Direct Marketing Association's "Privacy Promise" represent effective self-regulatory standards for on-line, off-line and telephone-based relationships. These practices have a proven record of success and conform nicely to the provisions in H.R. 4678, and we therefore support the bill's language with regard to approved self-regulatory programs.

Enforcement is one of the most difficult aspects of privacy that we have to deal with. We believe H.R. 4678 has proposed a reasonable enforcement mechanism by building on existing proven methods. Far too often legislation is simply not enforced for one reason or another. However, an increasing number of recent successful enforcement actions have been taken by the Federal Trade Commission demonstrating its effectiveness in the privacy area.

Furthermore, with the straightforward nature of the bill, the three companies agree with the committee that the need to prescribe regulations is not necessary to enforce this title. Since there are in excess of 15 Federal privacy-related laws in the U.S., it is critical that any broad-based piece of legislation recognize and respect these existing laws and not create conflicting requirements.

There are specific practices that need to be treated differently from general information collected and used by commercial entities, such as affiliate sharing of credit information within a financial institution, as covered under the Fair Credit Reporting Act, and the sharing of sensitive information about children, covered under COPPA.

Section 109 recognizes these specific situations and provides the right kind of harmonization with other existing laws.

Section 109(d), Preemption of State Privacy Laws, is a necessary requirement for both consumers and business. Nothing will be more confusing to consumers than to have differing privacy laws in each State or locality. As we have seen with financial laws recently passed in North Dakota and the rush to enact similar laws at the local level, such as those in Daly City, Contra Costa County and Berkeley, California, a myriad of conflicting State or local laws make it imperative that a preemptive bill of this nature become law.

There are three risks if States and localities are permitted to continue to enact their own privacy laws. First, is that the State

and local governments lack the dedicated resources to conduct a thorough analysis of the issues that this committee has done. And, in addition, privacy becomes a very political issue.

Second, for consumers, understanding their rights and being able to easily enforce them when an infraction occurs will be extremely difficult, which in turn seriously diminishes the effectiveness of the law.

And third, local law enforcement historically has not focused on these kinds of issues, while the FTC has the resources and needed expertise.

In short, without preemption, consumers will be confused and the effectiveness of enforcement will be reduced.

Finally, I would like to comment on one aspect of the bill that is not found, and this is the issue of access. We believe that by not requiring—including the requirement for consumer access, H.R. 4678 has properly recognized the inherent pitfalls of such a requirement. Each of the four fair information practices principles—notice, choice, access and security—must be applied uniquely to strike a balance between the value gained by consumers, business and society and the associated cost.

The primary purpose of access is to assure that information a company maintains about an individual is accurate. However, access for the sake of curiosity is never justified. Today, without even a legal mandate, companies provide consumers ready access to current account information. Coupled with the consumer's ability to opt out of having his or her name shared for unrelated purposes and the underlying concern about privacy and accuracy are thus satisfied.

In conclusion, while the three companies I represent today might not agree on all the detailed provisions of H.R. 4678, we believe Titles I and II represent a very balanced approach to protecting consumers' privacy while allowing information flows that bring value to the consumer. I do, however, urge the committee to work closely with the credit bureaus and their trade associations to make sure that Title II is effective in preventing identity theft.

Mr. Chairman, thank you for the opportunity today to testify on behalf of Acxiom, Experian Marketing Services and Trilegiant. I request our formal statements be entered into the record and am pleased to answer any questions.

[The prepared statement of Jennifer Barrett follows:]

PREPARED STATEMENT OF JENNIFER BARRETT, CHIEF PRIVACY OFFICER, ACXIOM CORPORATION

Chairman Stearns, Ranking Member Towns, and members of the Subcommittee, thank you for the opportunity to participate in this timely hearing and to share the perspective of the Companies on Titles I and III of H.R. 4678—the "Consumer Privacy Protection Act of 2002". The three corporations listed in the caption sheet strongly support a balanced approach to the use of personal information. Descriptive information on these companies may be found in the appendix attached.

I will not make specific comments about Title II. Instead, I urge the Committee to work closely with the Credit Bureaus and their trade associations to make certain Title II is effective in preventing identity theft and improves the remedies available for those whose identity has been stolen.

Information products from our three companies fill an important gap in today's business-to-consumer relationship. In our information-based economy, companies succeed not just by meeting their customers' expectations, but by exceeding them with superior products and services of the highest quality. Businesses do not in-

stinctively know everything their customers want and thus need information to better understand what consumers both want and need. Companies such as Acxiom, Experian and Trilegiant are the vehicles by which businesses acquire or better use this vital consumer information.

The efficient flow of consumer information to businesses has significantly contributed to our nation's economic growth and stability by (1) enhancing variety in consumer goods and services; (2) facilitating lower domestic prices as compared to foreign markets; and (3) accelerating the speed and ease with which transactions can be completed. This flow should be permitted to continue.

Notwithstanding these successes, the inappropriate use of information to defraud or discriminate against consumers should be illegal. H.R. 4678 is a bill that makes every effort to balance these concerns, and we are pleased to be here today to comment specifically on a number of aspects of the bill.

Comprehensive Coverage of Both Online and Offline Practices

In the debate about data privacy, public policy makers are asking some very good questions regarding whether legislation should be specific to the online sector or technology neutral covering both online and offline practices.

It is difficult to argue that a corporation's policies governing the collection and use of personally identifiable information should be different in the online and offline environments. Further, even if legislation was focused only on online information, the offline environment would be affected equally, since online and offline data is inevitably combined at some point by every company.

Even so, there are practical differences in the online and offline worlds that policy makers must carefully consider for legislation that is technology neutral. Self-regulatory regimes already in place recognize these practical differences, so policy makers should look to these practices as the basis of any future legislation deemed necessary.

Most of the clients of our three companies, as well as our data sources, operate in multiple environments, too. For example, many catalog companies have an online catalog, and many retailers are becoming dominant forces on the Internet. In fact, only a very few companies exist solely in an online environment today—and even these companies depend on offline information, which they merge with online information, to increase efficiency and to stay competitive.

However, there are important differences in how notice can be delivered and choice exercised in the online and offline environments. Understanding these differences is at the heart of the online/offline debate because self-regulatory practices or legal standards must allow enough flexibility to provide consumers effective notice and choice across different media.

In order to be fair in all mediums, the standard for providing a full statement of information practices, usually referred to as a privacy policy, must be "upon request."

Online Notice

In an interactive online environment, an "on-request" standard can easily be provided by a conspicuous link to a privacy policy. The interactive nature of the Internet also allows a consumer to make immediate, informed choices about how his or her information can be used. In the marketing industry, "opt-out" is the standard for informed consent, but the interactive nature of the Internet is also allowing new voluntary methods of permission-based marketing to flourish as well. This interactive nature has resulted in the wide spread acceptance of online privacy standards like those proposed in Title I. Nearly 100 percent of the 100 largest consumer websites have a link to a privacy statement.

Offline Notice

However, this interactive model is difficult, if not impossible, to achieve in the offline marketing context. In the telemarketing environment, delivering the same kind of notice and gaining the same kind of consent would be financially onerous, could destroy otherwise successful marketing campaigns, and could result in very negative customer relations.

In the offline environment, there must be flexibility to deliver notice and choice, upon request, through the mail in paper form. Alternatively, businesses should be able to direct consumers to a telephone number or website to access a company's policy. Also, retailers should be allowed to deliver notices at the checkout counter. In other words, businesses must have the flexibility to adopt practices that best meet the medium in which they are engaged, even though notice and choice about marketing information should be the policy in all mediums.

We believe Sections 101 (a) and (b) of H.R. 4678, *Privacy Notices to Consumers, Notice Required and Form and Contents of Notice,* are intended to recognize and

allow for these practical differences in collection, notice and choice methods that exist in the online, offline and telephone environments. We want to continue to work with the Committee to ensure this "upon request" distinction is clear in the law, so that businesses have the necessary flexibility to conduct successful marketing campaigns in this difficult economic environment.

Self-Regulatory Programs

Section 106, Self-Regulatory Programs, further recognizes the important role of self-regulatory programs that have served both the consumer and the business community well in areas of information use where legislation has not previously existed.

Such programs as the online seal programs from BBBOnline and TrustE, along with the Direct Marketing Association's "Privacy Promise," represent very effective self-regulatory standards for online, offline and telephone based relationships. These practices generally require companies to provide consumers choice through an opportunity to "opt-out" of information sharing, to develop appropriate guidelines to keep the information secure, offer the consumer third party recourse for settling disputes, and the option to go to the Federal Trade Commission under Section 5(a)(1) of the Federal Trade Commission Act (15 U.S.C. 45 (a) (1)) where prior efforts to resolve the conflict have failed.

All of these practices, which are in effect today and have a proven record of success, conform nicely with the provisions in H.R. 4678, and we therefore support the bill's language with regard to self-regulatory standards.

Enforcement

We believe H.R. 4678 has proposed a reasonable enforcement mechanism in Section 107, *Enforcement,* by building on existing and proven enforcement methods. By doubling the amount of fines that may be imposed, this approach to enforcement becomes an even more effective deterrent.

Enforcement is one of the hardest aspects of privacy with which to deal. Far too often, legislation is not enforced for one reason or another. However, an increasing number of successful enforcement actions have recently been undertaken by the Federal Trade Commission. Such actions have demonstrated the effectiveness of the FTC in dealing with privacy and security issues.

Furthermore, with the self-regulatory choices and the straightforward nature of the provisions of H.R. 4678, the Companies agree with the Committee that the need to prescribe regulations is not necessary to enforce this title. The regulations in effect already exist in the Federal Trade Commission Act.

Harmonization with Other Laws

Since there are in excess of fifteen (15) federal privacy-related laws in the U.S., it is critical that any broad-based legislation, such as H.R. 4678, recognize and respect these existing laws and not create conflicting requirements that do not serve either the consumer or the business community.

There are specific practices that need to be treated differently from general personal information collected and used by commercial entities, such as affiliate sharing of credit information within a financial institution covered under the Fair Credit Reporting Act, and the sharing of sensitive information about children under the age of 13 under the Children's Online Privacy Protection Act.

In Section 109, *Effect on Other Laws,* H.R. 4678 properly recognizes these various laws and the requirements they each impose and offers the right kind of harmonization.

State Preemption

Section 109(d), *Preemption of State Privacy Laws,* is a necessary requirement both for the consumer and the business community. Nothing will be more confusing to concerned consumers, nor create more inefficiency to commerce, than to have differing privacy laws in each state or locality. As we have seen recently in North Dakota, and at the local level in Daly City, Contra Costa County and Berkeley, California, there appears to be a rush to enact unduly restrictive financial privacy laws. We suggest that these laws serve no other purpose than to dramatize the need for federal preemption, which H.R. 4678 offers.

If states and localities are permitted to continue enacting their own versions of privacy laws, several risks exist. First, in light of the fact that no state or locality is likely to have the necessary resources to conduct a comprehensive and thorough analysis of the issues surrounding the use of information such as this committee has conducted, plus the fact that the privacy issue is a very highly charged political issue, legislation passed by states and localities will almost surely result in serious unintended consequences. Second, for consumers, to understand their rights and be able to easily enforce their rights when they believe an infraction has taken place

will be extremely difficult, thereby diminishing the effectiveness of any enforcement action. Third, local law enforcement has not historically focused on these kinds of issues and the Federal Trade Commission has more resources and more expertise to deal with consumer complaints regarding privacy than any state or local authority. In short, without state preemption, consumers will be confused and the effectiveness of enforcement will be reduced.

International Issues

Title III—*International Provisions*—offers a good first step to address the growing concern of companies doing business outside the U.S. regarding the wide variety of privacy laws enacted in other countries.

Dealing with information flows across borders is an extremely complex issue and we have far too few facts on which to evaluate effective solutions. The bill's requirement that the Comptroller General of the United States conduct a study and make recommendations regarding remediation of discriminatory activities should provide the facts needed to identify solutions that will work.

Access to Information

Few would argue that the four Fa ir Information Practices Principles—notice, choice, access and security—are not important consumer rights. Unfortunately, these principles are usually recited without considering their true complexity. Practical approaches such as H.R. 4678—whether statutory or self-regulatory—recognize that each of these principles must be applied in sensible ways appropriately tailored for the purpose for which the information is used.

The application of each principle must strike a balance between the value gained by consumers, businesses and society and the costs associated with each. Sometimes that balance prohibits application of one or more of the fair information principles. For example, under the Fair Credit Reporting Act (FCRA), the nation's oldest privacy statute, consumers do not have a choice about being included in the national credit reporting system. If choice were an option, those who are lax on paying their bills would probably choose not to have that information disclosed to potential lenders which would result in increased lending risk for creditors and increased credit costs for consumers. In effect, there would be fewer financial service products for consumers.

The principle of access, arguably the most complex issue in the debate about consumer privacy, must be thoughtfully applied because it raises significant privacy, data security and cost considerations for consumers, businesses, and society in general. Unfortunately, perhaps because of the complexity of this issue, many legislative proposals dispense with the access principle by simply citing the obscure standard that "reasonable access" should be provided upon the consumer's request. While sounding sensible on its face, such an undefined standard delegates too much authority to regulators and the courts to develop public policy about consumer access.

As explained below, we believe that, by not including a requirement for consumer access, H.R. 4678 has properly recognized the inherent pitfalls of such a requirement.

Allowing consumer access, by the very nature of the process, makes the data less secure. As a result, appropriate authentication and verification systems would have to be implemented. Providing access also means that information held by an organization must be collected into personal, comprehensive profiles, which raises new privacy concerns. Finally, the costs associated with data collection, new security systems for authentication, and customer service staff necessary to administer disclosure, dispute and correction systems, can be enormous.

The primary purpose of access is to make certain the information a company maintains about an individual is accurate. For example, if a company's use of inaccurate or fraudulent information could cause harm to an individual through overbilling, or is used to make a decision that could deny a consumer a benefit or service such as credit, insurance or employment, then access should be provided. In these cases, it is in the best interest of both the consumer and the business to be sure the personal information about a consumer is correct.

However, access for the sake of curiosity is not justified when the costs to society and the threat to personal privacy are significant. In such instances, access should be discouraged if there is no legitimate identified harm to an individual such as a denial of a benefit or service.

Today, even without a legal mandate, almost every company provides consumers ready access to current account information, the very information which, if inaccurate, could result in a benefit or service being denied. This kind of targeted access to personal information reflects business' interest in accurate, up-to-date records for billing purposes, as well as a customer-focused response to consumer demand. Many

Internet-based companies offer access not only to account and billing information but also to customer-supplied information used to predict consumer preferences.

Providing access to consumers would be of little benefit, and such access likely would pose a greater threat to privacy than currently exists. The nature of information in marketing databases would limit identity authentication largely to name and address (which is widely available in public sources, such as telephone directories) and, therefore, would greatly limit the ability of businesses to validate consumer identities for disclosure purposes. Accordingly, access requirements should be constructed so as to balance the benefits to consumers against the security risks to them, and the costs to companies that hold the data.

Allowing access to marketing databases would be enormously expensive. While that expense is justified and necessary with regard to information governed by the Fair Credit Reporting Act, it is of questionable value for data used only for marketing purposes.

A consumer's current ability to opt out of having their name shared for direct marketing purposes satisfies the underlying concern about privacy and accuracy without imposing undue and unnecessary costs to businesses or risks to consumers that would result from access requirements.

H.R. 4678 has rightly not included a provision for access in the bill.

Conclusions

While Acxiom, Experian and Trilegiant do not agree on all the detailed provisions of H.R. 4678, we believe the bill, in its current form, and subject to the our comments herein, represents a well-intentioned, balanced approach to protecting consumer privacy while allowing information flows that bring value to consumers and to our economy. We look forward to working with you to ensure these intentions are realized throughout the legislative process.

Mr. Chairman, thank you for the opportunity to appear today on behalf of these three companies, Acxiom Corporation, Experian Marketing Services and Trilegiant. I am prepared to furnish any additional information to the Committee, and answer any questions you may have.

APPENDIX

The Companies include some of the most prominent organizations in the country involved in helping facilitate the appropriate use of information in ways that bring value to both the consumer and the business community.

Acxiom Corporation

For over thirty years, Acxiom Corporation has provided data management services and technology. The company helps both large and small businesses sell better products and services smarter, faster, and at a lower cost. Acxiom's business includes two distinct components: database management services and information products. Database management services, representing almost 90% of the company's revenue, assist businesses in better managing their customer information, helping them save costs and secure a better return on their marketing efforts. Acxiom's information products—directories, customer enhancement and list products—provide needed intelligence to help businesses overcome the time and distance of less-personal customer relationships.

Acxiom has approximately 5,000 employees worldwide, has processing centers in Arkansas, Illinois, Arizona and California, and has operations in the UK, Australia, France and Japan.

Experian Marketing Services

Experian is one of the world's leading information solutions companies. Experian Marketing Solutions enables organizations to make fast, informed decisions to improve and personalize relationships with their customers. This is done by combining decision-making software and systems with some of the world's most comprehensive databases of information about consumers, businesses, and property.

Experian Information Solutions is a consumer reporting agency that enables businesses to make objective, safe, secure loans and minimize other credit-related losses, while providing consumers instant access to credit. Experian also provides reference services, analytic services, and consulting solutions. Experian employs 6,500 people in North America, with major facilities in Costa Mesa, CA; Allen, TX; Denver, CO; Atlanta, GA; Mt. Pleasant, IA; Schaumber, IL: Lincoln, NE; Parsippany, NJ; Albany, NY; New York City, NY; Rye, NY; and Rutland, VT.

Direct Marketing Services

Experian direct marketing services help bring businesses and their customers together. Businesses rely on Experian to help them better understand their markets and the characteristics of the people who do business with them. Understanding the marketplace makes possible faster, more efficient product development and delivery, better retail outlet and service center locations, improved customer service, more cost-effective advertising, and lower costs for consumers. By identifying the characteristics of consumers likely to be interested in certain kinds of products and services, Experian helps marketers more efficiently reach consumers who are most likely to be interested in a business's products or services.

Credit Reporting

Experian and the companies from which it was formed have provided credit reporting services for more than 100 years. Today, hundreds of millions of credit reports are provided to lenders annually. The ability of creditors to check a person's credit references in an instant enables them to make rapid, sound, and objective lending decisions. That ability helps consumers get the credit they need and deserve faster and cheaper than anywhere else in the world.

Customer Relationship Management

Experian helps businesses establish and develop long-lasting customer relationships through responsible information use. We help businesses get a clearer picture of their customers across multiple business units and market segments. We help companies understand why certain kinds of people shop with them and what the customer needs. With that clearer understanding, Experian then is able to provide information services that help businesses initiate relationships with new customers, assist the businesses in developing new, desirable products and services, and aid in providing pleasant shopping and effective customer service. The result is a better shopping experience for consumers and more profitable operation for businesses.

Automotive Information Services

Experian Automotive Information Services specialize in the collection and dissemination of vehicular data from each of the 51 United States jurisdictions. The information is utilized to provide valuable services to auto dealers, manufacturers, consumers and advocacy organizations, advertising agencies and internet information sites, law enforcement and tollway authorities. Detailed vehicle history reports enable consumers to make informed used-auto purchasing decisions. Manufacturers rely on our services to manage recalls and conduct market analysis to manage product supply and improve service.

Electronic Commerce Services

Experian's electronic commerce division helps businesses establish a presence in the electronic marketplace, develop relationships with online consumers, and ensure consumers and businesses enjoy positive, safe transactions.

Individual Reference Services

Experian reference services help people, businesses, non-profit organizations, government agencies, law enforcement, and other organizations identify, locate, and verify the identity of individuals. The most recognized individual reference services are the telephone book and directory assistance—services you use every day. They usually include only names, addresses and telephone numbers. More sophisticated reference services may include information about whether you own a home or rent an apartment, how long you have lived in the same location, and if there are additional household members. Sensitive identifying information such as your Social Security number, drivers license number, and date of birth is included in some reference services. These services, however, are limited to use by law enforcement, government agencies, and other organizations with a legitimate and appropriate need for such information.

Trilegiant Corporation

Trilegiant Corporation is one of the country's largest direct mail marketers. Trilegiant offers consumers the opportunity to join various membership clubs that provide valuable services, significant discounts and other member privileges. Trilegiant's membership clubs provide a wide array of financial and consumer-based individual services, including those relating to shopping, travel, auto, personal finance and other membership programs that make their lives more convenient and secure. We were a pioneer in the direct marketing and membership services business and have been active for over 27 years, and we currently have over 23 million members in the U.S. who enjoy our services. Trilegiant partners with many of the

nation's leading financial, retail and media entities to enable them to enhance their customer loyalty and brand affinity and to generate additional revenue.

Each year, Trilegiant mails hundreds of millions of pieces of consumer correspondence, receives tens of millions of inbound telemarketing calls, and conducts millions of outbound telemarketing calls. Trilegiant also is a major on-line marketer and partners with many of the country's largest on-line businesses and markets its services through hundreds of millions of on-line impressions.

Trilegiant has over 3,000 employees in facilities across the nation.

Mr. STEARNS. By unanimous consent, so ordered. And I thank you.

Mr. Misener.

STATEMENT OF PAUL MISENER

Mr. MISENER. Mr. Chairman and Mr. Boucher, Mr. Bass, thank you very much for inviting me to testify today.

Amazon.com is the Internet's leading retailer. As I described in detail in my testimony before this subcommittee last year, Amazon.com uses consumer information to personalize the shopping experience at our on-line store and thus help our customers find and discover anything they may want to buy.

At the same time, Amazon.com is pro-privacy. We make ever effort to provide our consumers outstanding privacy notice, choice access and security.

Mr. Chairman, through your steadfast leadership and the dedicated efforts of the members and extraordinarily talented staff of your subcommittee and the full committee, you have amassed what likely is the world's most comprehensive legislative data base on consumer information privacy. You have held now seven highly informative hearings and countless meetings with company association representatives, public interest advocates and academics. Your willingness to listen impartially to all parties is well known and greatly appreciated. It is not surprising therefore that you have introduced, with bipartisan support, such an excellent bill, H.R. 4678.

The essential purpose of your bill, if I may summarize it, is to provide consumers a baseline of information privacy protection regardless of the specific type of information involved, regardless of the medium through which it is collected and regardless of where a consumer is located in the United States. This approach works very well with the existing U.S. Privacy law, which provides additional protections for particularly sensitive information, such as medical and financial records and particularly hazardous situations such as unsupervised children online.

As I will describe in detail momentarily, H.R. 4678 includes the three indispensable components about which I testified in your subcommittee last year. H.R. 4678 goes even further by addressing, head on, the issue consumers often cite as their principal, quote, "privacy concern," which is identity theft. All in all, Mr. Chairman, H.R. 4678 is an excellent bill.

I must explain, however, that Amazon.com is not actually seeking privacy legislation. For several reasons, we believe it would not be proper for us to do so. First, if we were to argue that a bill must be passed, we might incorrectly be viewed as suggesting that a bill is necessary in order to make our company protect consumer privacy. But Amazon.com already provides excellent privacy protections to our customers.

Second, Amazon.com's arguing that a bill must be passed could be misinterpreted to mean that we want Congress to force other companies to offer privacy protections at the level we already do. Frankly, however, we think our companies neglect consumer information privacy at their peril. The companies simply must offer excellent privacy practices or else they will lose business.

Third, if we actively seek passage of a Federal bill, it might be said we merely wish to preempt State legislation in this area. Although it is true that State-by-State legislation of consumer information privacy easily could produce an untenable and unconstitutional crazy quilt of rules with which an on-line company might find it difficult or impossible to comply. States, thus far, have heeded our warnings in this regard.

Finally, by arguing that a bill must be passed, Amazon.com might mislead some observers into thinking that we believe the bill is necessary to improve consumer confidence on the Internet. Although we are aware of intuitive and compelling arguments that legislation is necessary to boost consumer confidence, we are not nearly so sure this is true, just as in the off-line retail world, consumers know there are both safe and unsafe places to shop.

In sum, Mr. Chairman, we did not come before you today requesting privacy legislation. Others have made a strong case for a new law. But for the reasons I have just articulated, Amazon.com is not prepared to make the same case. Nonetheless, Mr. Chairman, if you and your colleagues determine that general consumer information privacy legislation is needed, Amazon.com fully supports H.R. 4678 to meet this need.

In my remaining time, I would like to offer our support in particular for three essential aspects of H.R. 4678. Without any one of these components, Amazon.com, and I suspect many other companies, could not support this bill. First and foremost, H.R. 4678 addresses consumer information privacy holistically without regard to the medium through which the information is collected. This parity among media is both wise and fair.

It is wise because there is no reason for legislation to treat, for example, the privacy of the person's mailing address different if it were collected at an on-line Web site instead of at a mall kiosk or over the phone.

Parity is fair to on-line business because the information privacy practices of competitors that happen to operate through different communications media would be treated the same. And most importantly, parity is fair to consumers because it would address 100 percent of their retail transactions, rather than the mere 1 or 2 percent conducted online.

Amazon.com also supports H.R. 4678's national approach to consumer information privacy. The inherent interstate nature of Web-based commerce demands a national solution. Your bill recognizes this fact by preempting relevant State law.

Finally, Amazon.com supports the bill's faith in the consistency and balance of a public enforcement mechanism. Consumers need a readable, not legalistic, privacy notice. Only a regulatory body such as the Federal Trade Commission is well positioned to balance the competing goals of legal precision and readability.

Let me summarize by saying that although we are not explicitly seeking privacy legislation, Amazon.com is, on behalf of our company and customers, proud to support H.R. 4678, which wisely and fairly addresses consumer information uniformly among all methods of collection, establishes a national system that avoids a hodgepodge of State and local rules and employs the consistency and balance of a public enforcement mechanism.

Thank you again, Mr. Chairman, for your attention to the facts and details of consumer information privacy. On behalf of our company and customers, Amazon.com sincerely appreciates your perspicacity.

And last let me thank you for inviting me to testify. And I look forward to your questions.

[The prepared statement of Paul Misener follows:]

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

Chairman Stearns, Mr. Towns, and members of the subcommittee, my name is Paul Misener. I am Amazon.com's Vice President for Global Public Policy. Thank you very much for inviting me to testify today.

Amazon.com is the Internet's leading retailer. As I described in detail in my testimony before this subcommittee last year, Amazon.com uses consumer information to personalize the shopping experience at our online store and, thus, to help our customers find and discover anything they may want to buy. At the same time, Amazon.com is pro-privacy: we make every effort to provide our customers outstanding privacy notice, choice, access, and security.

Mr. Chairman, through your steadfast leadership, and the dedicated efforts of the members and extraordinarily talented staff of your subcommittee and the full committee, you have amassed what likely is the world's most comprehensive legislative record on consumer information privacy. You have held seven highly informative hearings and countless meetings with company and association representatives, public interest advocates, and academics. Your willingness to listen impartially to all parties is well known and greatly appreciated.

It is not surprising, therefore, that you have introduced, with bipartisan support, such an excellent bill, H.R. 4678. The essential purpose of your bill, if I may summarize it, is to provide consumers a baseline of information privacy protection, regardless of the specific type of information involved; regardless of the medium through which it is collected; and regardless of where a consumer is located in the United States. This approach works very well with existing U.S. privacy law, which provides additional protections for particularly sensitive information (such as medical and financial records) and particularly hazardous situations (such as unsupervised children online).

As I will describe in detail momentarily, H.R. 4678 includes the three indispensable components about which I testified to your subcommittee last year. Specifically, your bill would address consumer information uniformly among all methods of collection; it would establish a national system that avoids a hodgepodge of state rules; and it would employ the consistency and balance of a public enforcement mechanism. H.R. 4678 goes even further by addressing head-on the issue consumers often cite as their principal "privacy" concern: identity theft. It also wisely would begin the process of examining how best to harmonize privacy protections worldwide. All in all, Mr. Chairman, H.R. 4678 is an excellent bill.

I must explain, however, that Amazon.com is not actually seeking privacy legislation. For several reasons, we believe it would not be proper for us to do so. First, if we were to argue that a bill must be passed, we might incorrectly be viewed as suggesting that a bill is necessary in order to make our company protect consumer privacy. But as I briefly outlined earlier, and described in detail in my testimony last year, Amazon.com already provides excellent privacy protections to our customers. In fact, H.R. 4678 likely would not require Amazon.com to alter its privacy practices in any substantial way: we simply do not need a new law to force us to provide outstanding consumer privacy protections.

Second, Amazon.com arguing that a bill must be passed could be misinterpreted to mean that we want Congress to force other companies to offer privacy protections at the level that we already do. After all, it is a centuries-old tradition for market-leading companies to seek regulations that mirror their current practices, if for no

other reasons than to impose additional costs on existing competitors and market entry costs on potential competitors. Frankly, however, we think other companies neglect consumer information privacy at their peril: Companies simply must offer excellent privacy practices or else they will lose business, regardless of whether a law requires it.

Third, if we actively seek passage of a federal bill, it might be said that we merely wish to preempt state legislation in this area. Although it is true that state-by-state legislation of consumer information privacy easily could produce an untenable and unconstitutional "crazy-quilt" of rules with which online companies might find it difficult or impossible to comply, states thus far have heeded our warnings in this regard. A national privacy scheme, based on explicit preemption of state laws, is an essential component of any federal legislation but, obviously, until state laws are passed, no such preemption is necessary.

Finally, by arguing that a bill must be passed, Amazon.com might mislead some observers into thinking that we believe a bill is necessary to improve consumer confidence on the Internet. Although we are aware of intuitive and compelling arguments that legislation is necessary to boost consumer confidence, we are not nearly so sure this is true. Just as in the offline retail world, consumers know there are both safe and unsafe places to shop.

In sum, Mr. Chairman, we do not come before you today requesting privacy legislation. Others have made a strong case for a new law but, for the reasons I have just articulated, Amazon.com is not prepared to make the same case.

Nonetheless, Mr. Chairman, if you and your colleagues determine that general consumer information privacy legislation is needed, Amazon.com fully supports H.R. 4678 to meet this need. This bill is an excellent vehicle by which Congress could address the consumer information privacy concerns various parties have raised, and Amazon.com could continue to serve our customers well if it were enacted.

In my remaining time, I would like to offer Amazon.com's support for three particular and essential aspects of H.R. 4678. Without any one of these components, Amazon.com—and, I suspect, many other companies—could not support this bill.

First and foremost, H.R. 4678 addresses consumer information privacy holistically, without regard to the medium through which the information is collected. This parity among media is both wise and fair. It is wise because the personal consumer information collected offline (to the extent the terms "offline" and "online" have any meaning in today's world of communications convergence) is as sensitive as or, often, is more sensitive than, information collected online. There is no reason for legislation to treat, for example, the privacy of a person's mailing address differently if it were collected at an online website instead of at a mall kiosk or over the phone.

This parity also is wise because online transactions often provide more consumer privacy protections than offline transactions. Indeed, brick-and-mortar retailers know their customers' physical characteristics, including race, sex, weight, complexion, et cetera, but online retailers cannot. And unlike their online competitors, brick-and-mortar retailers also know their customers' geographic location; we online retailers, on the other hand, do not know from where our customers access our Website.

Parity also is fair to online businesses, because the information privacy practices of competitors that happen to operate through different communications media would be treated the same. And, most importantly, parity is fair to consumers, because it would address 100% of their retail transactions rather than the mere one or two percent conducted online. Significantly, parity also would address the privacy concerns of those persons on the unfortunate side of the digital divide, not just those people who shop online. This bears repeating: an online-only bill would have the perverse effect of providing no privacy protections to those on the unfortunate side of the digital divide.

In sum, H.R. 4678 wisely and fairly addresses consumer information privacy without regard to the medium through which it is collected.

Amazon.com also supports H.R. 4678's national approach to consumer information privacy. It would be difficult or impossible for nationwide entities such as our company to comply with a "crazy-quilt" of state consumer privacy legislation. The inherent interstate nature of Web-based commerce—a single Web page is viewable from anywhere in the world—demands a national solution; your bill recognizes this fact by preempting relevant state law.

Finally, Amazon.com supports the bill's faith in the consistency and balance of a public enforcement mechanism. Consumers need readable, not legalistic, privacy notices. Only a regulatory body such as the Federal Trade Commission is well positioned to balance the competing goals of legal precision and readability. Indeed, despite the bill's emphasis on the readability of privacy notices, private litigants would

have no interest in protecting readability. If private enforcement were authorized, companies like Amazon.com might be forced to adopt Balkanized, legalistic privacy notices at the expense of consumer accessibility. Only a public enforcement mechanism, such as that included in H.R. 4678, would foster a tenable balance between the competing goals of accuracy and readability.

Let me summarize by saying that although we are not explicitly seeking privacy legislation, Amazon.com is, on behalf of our company and customers, proud to support H.R. 4678, which wisely and fairly addresses consumer information uniformly among all methods of collection; establishes a national system that avoids a hodgepodge of state and local rules; and employs the consistency and balance of a public enforcement mechanism. As I mentioned earlier, it also sensibly addresses consumer identity theft and the international aspects of privacy policy.

Thank you again, Mr. Chairman, for your attention to the facts and details of consumer information privacy. On behalf of our company and customers, Amazon.com sincerely appreciates your perspicacity.

Lastly, thank you for inviting me to testify; I look forward to your questions.

Mr. STEARNS. Nice to see you again.

Mr. Rotenberg, you have the platform. You are probably one that can enlighten us a little differently.

STATEMENT OF MARC ROTENBERG

Mr. ROTENBERG. I have somewhat different views, Mr. Chairman, yes. And I would like to thank you and Mr. Boucher not only for the opportunity to be here this morning, but also to recognize the extensive work that has been done by this subcommittee and the members and the staff to tackle this very difficult issue.

And I don't think anyone on the panel would disagree that this is a difficult issue. At the same time, it is an important issue, and I would certainly like to be able to join the other witnesses this morning and say that we have a good bill and we are ready to go forward. But that is not my view, and I don't believe that is the view of other consumer privacy organizations on the left or the right that have considered this issue.

This is not just a concern, also, of the Washington policy groups. I think the reason that these witnesses are here today asking for this legislation is because over the last several years, all across this country, Americans have said to their elected officials, we need protections for privacy; we are concerned about how companies are using our personal information; we want to be able to do business, but we also believe there should be some accountability.

And they have turned to the courts and the State legislatures and the attorneys general, and even the counties, to get some protection from privacy; and they are getting it because the American legal system allows the States to protect the interests of their citizens through law, through court decisions, through the efforts of the attorneys general.

I think it is extraordinary that in North Dakota there was actually a referendum on the question of opt-in and financial privacy, and a referendum in that State passed because people in that State feel very strongly about protecting the privacy of their financial information. I think 10 years ago if you had said "opt-in" to anybody in North Dakota or anywhere else in this country, they would have no idea you were talking about privacy. That is how strongly people feel about this issue.

Now the industry groups have come to Washington and they have said to you, in effect, we can't take this avalanche of privacy concerns. We can't face potential action in 50 different States. Of

course, they never stopped to think that consumers in the self-regulatory environment face not 50 different privacy policies, but perhaps 500 or 5,000, because under the self-regulatory approaches that the bill endorses, companies are free to create whatever policy they wish. And every customer dealing with any company would have to consider each single interaction, what that policy means and whether it protects their privacy.

So let's look closely at the provisions in the bill and ask the question, Is what people across the country are being asked to trade, which are the rights and State laws and the aggressive action of State officials, a fair deal?

The act provides no access to the personal information that is acquired by companies on customers, and being acquired by companies on behalf of other companies. Acxiom, for example, is an extraordinary firm. I don't mean to single them out, but they are here this morning. They provide what they call a 360-degree view of customers. They want to know everything about you. And they will make that information available not only to businesses like Citibank for e-mail solicitation, which the Wall Street Journal—the Wall Street Journal recently raised questions about; they also now make it freely available for the FBI to do intensive data mining on American citizens. Commercial information is now being provided by Acxiom routinely for criminal investigations.

And I would like you to at least consider on this access question—perhaps you or members of your staff would make a request to Acxiom and ask them to provide you the information that they have about you and your family members, that they are providing to law enforcement and other businesses.

There is nothing in the bill that prevents that current practice. There is no private right of action, of course, in the bill, which many of the witnesses here this morning are very pleased about. Because, of course, that means that there is no real accountability.

Every single privacy complaint under this bill must go toward the Federal Trade Commission which even—even if it were more extensively staffed and really, you know, up to taking on individual consumer privacy complaints, couldn't begin to address the range of concerns and issues that Americans have expressed about the privacy issue.

And the bill provides no remedies to consumers. In other words, once consumers have gone through all the steps of the self-regulatory program—of the appeal within the self-regulatory program of the complaint to the FTC, at best, the FTC might decide that the company is no longer eligible to be a member of the self-regulatory program. And in my opinion that is an inadequate remedy.

I think we need real privacy protection. I think American consumers are asking for real privacy protection, and I think over the long term it will benefit American businesses and allow commerce both online and offline to thrive. But regrettably, I don't think this is a bill that would do it; and I am sorry to say that because I know we have spent a lot of time on this one, and we would certainly like to see a bill that would provide that protection.

So thank you very much.

[The prepared statement of Marc Rotenberg follows:]

PREPARED STATEMENT OF MARC ROTENBERG, EXECUTIVE DIRECTOR, ELECTRONIC PRIVACY INFORMATION CENTER

My name is Marc Rotenberg. I am the Executive Director of the Electronic Privacy Information Center in Washington. I am on the faculty of Georgetown University Law Center, where I have taught Information Privacy Law since 1990. I am co-author of a forthcoming casebook with Professor Daniel J. Solove on Information Privacy Law (Aspen Publishing). I have also recently been named chairman of the American Bar Association Committee on Privacy and Information Protection, though my comments today reflect only my views and not those of the ABA.

I appreciate the opportunity to testify before the Subcommittee today on HR 4678, the "Consumer Privacy Protection Act of 2002." I am well aware of the extensive work of the Subcommittee on privacy issues during this Congress. Therefore it is with some misgivings that I say to you today that this bill will have little support among consumer or privacy organizations, privacy experts, or the general public.[1] In many respects it seems crafted to protect privacy violators from legal accountability. On almost every key provision it favors industry over the consumer, the invasion of privacy over the protection of privacy. While it is true that is a sweeping measure in the sense that it applies to all data collection organizations, both off-line and on-line, the intent appears to be to insulate companies from any real accountability for what they might do with the personal information they acquire. Given the important tradition in the United States of safeguarding privacy as new technologies emerge, as well as the testimony provided by several witnesses on the need to protect privacy going forward, I can only hope that a better bill will be introduced in the future.

"Protection of Individual Privacy in Interstate Commerce" (Title I)

The substantive provisions of the measure are set out in Title I. Simply stated they require a company to adopt a privacy policy that can say virtually anything and can be changed at any point in time to say anything else. Under Title I of the Act, if a company states that it takes sensitive personal information and puts in on the Internet for all to see, it will be in compliance with the Consumer Privacy Protection Act. A company can adopt a policy that states that it will zealously protect sensitive personal information, acquire customer data, then change its mind, and post it on the Internet. It too will be in compliance with the Consumer Privacy Protection Act.

There is an interesting section that attempts to limit the sale of personal data to third parties, but this provision is easy to defeat by simply offering the consumer a benefit, such as the service originally sought. A companion provision that seeks to limit "other information practices" is also almost meaningless because consumers will not have access to any relevant information to make an informed decision and even if they go to the effort of exercising this right, the company can exercise its

[1] The bill appears to ignore the testimony of every public interest advocate appearing before the Subcommittee. My own testimony of June 21, 2001 advocated a system of rights similar to the Cable Communications Policy Act of 1984, one that includes notice, opt-in, access, and a private right of action. Ed Mierzwinski's testimony of April 3, 2002, on behalf of the US Public Interest Research Group, called for a law that incorporated a system of FIPs. Specifically, Mr. Mierzwinski testimony called for collection limitations, comprehensive notice, opt-in, guarantees of accuracy and security, no preemption, and a private right of action. Frank Torres' testimony of April 3, 2001, on behalf of Consumers Union, broadly outlined current problems in HIPAA and the GLBA. Mr. Torres recommended comprehensive notice, full access and correction rights, and opt-in consent. More than thirty organizations across the political spectrum endorsed a set of principle at the beginning of this Congress on which to base federal privacy legislation:

1. The Fair Information Practices: the right to notice, consent, security, access, correction, use limitations, and redress when information is improperly used,
2. Independent enforcement and oversight,
3. Promotion of genuine Privacy Enhancing Technologies that limit the collection of personal information,
4. Legal restrictions on surveillance technologies such as those used for locational tracking, video surveillance, electronic profiling, and workplace monitoring, and
5. A solid foundation of federal privacy safeguards that permit the private sector and states to implement supplementary protections as needed.

Many good proposals from leading US academics were apparently also ignored. Professor Joel Reidenberg, testifying on March 8, 2001, said that the "United States is rapidly on the path to becoming the world's leading privacy rogue nation." Reidenberg recommended that the Congress promote the negotiation of a "General Agreement on Information Privacy." As for public opinion, polls consistently find strong support among Americans for privacy rights in law to protect their personal information from government and commercial entities. See EPIC, "Public Opinion and Privacy" (http://www.epic.org/privacy/survey/default.html)

right to "terminate its compliance with the limitation" on thirty days notice. (This section might be called the "Now you see it, now you don't" privacy provision.)

The Act would create policies for policies—a form of bureaucratic red tape for consumers—without ever giving a consumer access to personal information held by the company. Does a company have inaccurate information about you? You'll never know. Does it discriminate against you because of confusion about names, incorrect addresses, or bad information provided by a third party? You'll have no idea. There is nothing in the bill that even attempts to hold companies responsible for the accuracy of their information on consumers.

The bill places enormous confidence in self-regulatory programs. It imposes only the most modest obligations on these consulting firms. The generous eight-year certification period for self-regulatory companies contrasts sharply with the thirty days notice provided to consumers about material changes in privacy polices permitted under the Act. This deference to self-regulation is extraordinary, considering not only that Truste continued to approve Microsoft even as its Passport service was found to violate the FTC Act, as well as the clear experience in this last few years of abuse stemming from industry self-policing.

The Act noticeably creates no safeguards on disclosure of personally identifiable information to law enforcement agencies. In other words, individuals who provide information to businesses will have no protections against fishing expeditions by the police. Virtually every other privacy law in the United States sets out a Fourth Amendment standard to regulate police access to personal information held by third parties. The purpose is not to prevent law enforcement access or to frustrate criminal investigations, but rather to ensure that when police go to a private business in search of information about customers or clients they do so with something that approaches probable cause or reasonable suspicion that a crime has been committed. Under the "Consumer Privacy Protection Act" there will be no new safeguards established to protect consumers from searches that might otherwise be overly board, intrusive or unlawful. Under this approach, video rental records will remain protected under a 1988 Act, but there will be no similar protection for new services offered over the Internet or the extensive record of purchases and interests collected and maintained by Amazon.

The Act forcefully creates no private right of action. This goes far beyond any reasonable concern about large damage awards. There are any number of alternative approaches that would preserve a private right of action. It is possible for example, to allow individuals go into small claims court and seek relief as they do currently and effectively under the Telephone Consumer Protection Act. Alternatively, the state attorneys general could be empowered to enforce rights created by the federal statute as others have proposed, or damage awards could be capped. The point is that there are many ways to make a private right of action work.

The absence of a private right of action is all the more problematic because as the bill is currently structured there are no procedural rights for consumers who file complaints at the FTC nor are there any formal means of reporting or appeal if the FTC fails to act on a complaint. What happens, for example, if a drug company discloses the names of Prozac users on the Internet, a complaint is filed, and the FTC chooses not to act? It is clear that that the company's action violates the FTC Act as the FTC has already found, but if the Commission chooses, for whatever reason, not to pursue the complaint, that is the end of the matter. This grants the agency unprecedented discretionary authority.

Having constructed a bill that effectively provides no substantive rights for consumers, the Act preempts states that are seeking to provide greater protection to their citizens. It even preempts state common law which is an extraordinary step for the Congress. Has this Committee concluded that there should be no state remedies anywhere in the United States for breaches of privacy committed by an organization that collects personal information? That would be an extraordinary assault on both the common law and our federal form of government.

International Provisions

The purpose of Title III is apparently to raise questions about the enforcement of the Safe Harbor Arrangement and other international agreements that the United States has pursued to support the protection of privacy. As currently drafted, the section asks the Comptroller General to review these various arrangements to determine whether such laws, regulations or agreements "result in discriminatory treatment of United States entities."

Members of the Subcommittee should realize that *the Safe Harbor Arrangement addresses concerns that European governments have raised about privacy protection for their own citizens.* Safe Harbor came about to assist US businesses who had complained that it would be difficult to comply with privacy law in Europe. The con-

cerns of European officials about US practices have been substantiated in the United States by both state attorneys general and the Federal Trade Commission. For example, European privacy officials raised concerns that the Microsoft Passport service violated European law, but it was ultimately the US Federal Trade Commission that found that Microsoft violated Section 5 of the FTC Act. Earlier, European officials asked the Doubleclick company to modify its Internet advertising practices to comply with European privacy laws, but it was US officials who ultimately clamped down on the company's plans for invasive profiling of Internet users.

Do we really want to be in the position of objecting to the efforts of foreign governments to safeguard the privacy rights of their own citizens when US officials have expressed similar concerns? This is not a wise or forward-looking policy.

I'd also like to bring to the attention of the Committee the important role that the United States has historically played in helping to enforce international standards for privacy protection. The Department of State, under both political parties, has supported the international human rights community by monitoring compliance with the International Covenant of Civil and Political Rights. The ICCPR includes a critical provision on unlawful surveillance and police practices that threaten political freedom all around the world.

As the web site of the Department of State currently notes:

> The protection of fundamental human rights was a foundation stone in the establishment of the United States over 200 years ago. Since then, a central goal of U.S. foreign policy has been the promotion of respect for human rights, as embodied in the Universal Declaration of Human Rights. The United States understands that the existence of human rights helps secure the peace, deter aggression, promote the rule of law, combat crime and corruption, strengthen democracies, and prevent humanitarian crises.[2]

Section 1, paragraph f in the annual report prepared by the State Department addresses specifically "Arbitrary Interference With Privacy, Family, Home, Correspondence." For example in the 2002 report on China, the State Department notes that:

> The Constitution states that the "freedom and privacy of correspondence of citizens are protected by law." Despite legal protections, authorities often do not respect the privacy of citizens in practice. Although the law requires warrants before law enforcement officials can search premises, this provision frequently has been ignored; moreover, the Public Security Bureau and the Procuratorate can issue search warrants on their own authority. Authorities monitor telephone conversations, facsimile transmissions, e-mail, and Internet communications. Authorities also open and censor domestic and international mail. The security services routinely monitor and enter the residences and offices of persons dealing with foreigners to gain access to computers, telephones, and fax machines. Government security organs monitor and sometimes restrict contact between foreigners and citizens. All major hotels have a sizable internal security presence.[3]

Now I agree that the United States should look more carefully at some of the current international agreements that impact privacy, but the commercial agreements such as Safe Harbor, which are intended to safeguard privacy and facilitate trade, are the wrong place to start. I would urge the Comptroller General to consider whether such proposals as the Council of Europe Cybercrime Convention would violate the privacy rights of American citizens that would otherwise be protected under US law and the US Constitution.[4] That proposal, which some in the Administration continue to promote as if it were national law, even though it has never been introduced in the Congress let alone ratified by the United States, contains many provisions that deeply implicate American Constitutional values.[5]

---

[2] Department of State, "Human Rights," http://www.state.gov/g/drl/hr/ (last visited September 21, 2002)

[3] Department of State, "China (includes Hong Kong and Macau)," http://www.state.gov/g/drl/rls/hrrpt/2001/eap/8289.htm

[4] Council of Europe Committee of Ministers, 109th Sess, Convention on Cyber-Crime (adopted Nov 8, 2001), available online at http://conventions.coe.int/Treaty/EN/WhatYouWant.asp?NT=185.

[5] See, e.g., id. Arts. 2-11 (requiring member country statutory criminalization of offenses such as hacking, the production, sale or distribution of hacking tools, and child pornography, and an expansion of criminal liability for intellectual property violations. The treaty's intellectual property provisions significantly expand criminal liability for intellectual property violations and tilt copyright law away from the public interest: U.S. intellectual property law contains a delicate balance between the rights of intellectual property holders and the rights of the public through the First Amendment and the law of "fair use" of copyrighted materials, but the Cyber crime

Continued

It is the Cybercrime Convention, not the Safe Harbor arrangement, that poses a direct threat to the interests of the United States and American citizens. It is that proposal that should be given careful scrutiny by the Congress.

Conclusion

This has been a difficult year on the privacy front. The country faces new challenges after September 11. Even so, many of us have been heartened by the efforts of government officials to safeguard this essential American value. A secretive federal court has spoken out against the misuse of the Foreign Intelligence Surveillance Act. The House leadership has taken strong stands on such issues as Carnivore, TIPS, and video surveillance. The White House has indicated its reluctance to endorse a national identity card. The Federal Trade Commission has issued important orders on Microsoft, Eli Lilly, and proposed a new rule on telemarketing. The state attorneys general have acted to protect consumers against egregious practices that have led to the disclosure of medical records, financial information, and the misuse of student records.

Even the President's Critical Infrastructure Protection Board, charged with safeguarding the nation against future terrorist threats said in the recent report on the National Strategy to Secure Cyberspace:

> The nation's Strategy must be consistent with the core values of its open and democratic society. Accordingly, *Americans must expect government and industry to respect their privacy and protect it from abuse.* This respect for privacy is a source of our strength as a nation; accordingly, one of the most important reasons for ensuring the integrity, reliability, availability, and confidentiality of data in cyberspace is to protect the privacy and civil liberties of Americans when they use—or when they personal information resides on—cyber networks. To achieve this goal, the National Strategy incorporates privacy principles—not just in one section of the Strategy, but in all facets. The overriding aim is to reach toward solutions that both enhance security and protect privacy and civil liberties.[6]

This was an extraordinary statement coming from an organization tasked with protecting the country from cyber warfare and future acts of terrorism. Still, they seemed to leave little doubt that the protection of privacy could not be sacrificed even as the country works to strengthen cybersecurity. Certainly, there could be a similar commitment to protect privacy in less critical circumstances.

Thank you for your attention. I would be pleased to answer your questions.

Mr. STEARNS. Thank you Mr. Rotenberg. I mean we have, we are interested in people that don't agree with the bill obviously too. And so we appreciate your comments.

I would ask unanimous consent to put in the record the support we have got, a letter from Acxiom and Computer Systems Policy Project and National Business Coalition on E-Commerce Privacy. Without objection, so ordered and we will make it part of the record.

[The information referred to follows:]

Convention criminalizes copyright infringement with no mention of fair use); id. Arts 16-22 (requiring participating nations to grant new powers of search and seizure to its law enforcement authorities, including the power to force an ISP to preserve a citizen's internet usage records or other data, and the power to monitor a citizen's online activities in real time—while including no provisions to protect citizens' privacy. In the United States, the treaty requires the U.S. to authorize the use of devices like Carnivore, the FBI's "Internet-tapping" surveillance system.); id. Arts 23-35 (requiring law enforcement in every participating country to assist police from other participating countries by cooperating with "mutual assistance requests" from police in other participating nations "to the widest extent possible." This obliges American law enforcement to cooperate with investigations of behavior that is illegal abroad but perfectly legal in the U.S.). The Administration has stated that "The Convention will help us and other countries fight criminals and terrorists who use computers to commit crimes . . ." Promoting Innovation and Competitiveness: President Bush's Technology Agenda, at http://www.whitehouse.gov/infocus/technology/tech3.html.

[6] p. 43 (emphasis added).

ACXIOM
LITTLE ROCK, AR
August 1, 2002

The Honorable CLIFF STEARNS
United States House of Representatives
2227 Rayburn House Office Building
Washington, DC 20515

I just want to take this opportunity to thank you for the hard work that you and your staff have put into coming up with a balanced approach to a key aspect of the privacy issue. Your work helps to ensure consumer privacy, while protecting the economy, by allowing the exchange if critical data while not compromising personal information. I believe that your legislation, H. R. 4678, weighs competing concerns, in an extremely difficult environment, and gives privacy advocates, the business community and regulators the capacity to work through many of the problems raised without undue burdens on the consumer.

While we might recommend some adjustments, it does provide a workable framework that is fair and will not result in the curtailment of critical data flows that are essential to our nation's economy. Without a doubt, a competing version currently moving in the Senate will have broad, unintended ramifications that will ultimately hurt both consumers and businesses.

Therefore, I want to express my support for H. R. 4678 and again thank you and your staff, particularly Ramsen Betfarhad, for the tireless effort given in crafting this balanced and effective piece of legislation.

Sincerely,

CHARLES MORGAN
Company Leader

HIGH-TECH LEADERS PRAISE STEARNS' PRIVACY BILL;

CSPP SAYS LEGISLATION "STRIKES THE RIGHT BALANCE"

Washington—The Computer Systems Policy Project (CSPP), a coalition of CEOs from the nation's leading high-tech companies, offered its support for bipartisan information privacy legislation unveiled today by House Energy and Commerce, Trade and Consumer Protection Subcommittee Chairman Cliff Stearns (R-Fla.).

"The issue of privacy is of paramount importance to CSPP members," said Phil Servidea, vice president of government affairs for NCR and co-chair of the CSPP Networked World Committee. "The bill proposed by Chairman Stearns is a step in the right direction, offering a baseline of protection to Americans doing business both online and offline, as well as effectively balancing consumer and business interests, and state versus federal jurisdiction."

"CSPP is grateful to Chairman Stearns for his thoughtful consideration of this complicated issue," said Ken Kay, executive director of CSPP. "We look forward to continuing to work with Chairman Stearns and Congress on privacy legislation that protects consumer privacy in accordance to the principles supported by our member companies."

The goals of the Stearns' legislation, the *Consumer Privacy Act of 2002,* are inline with many of the principles for privacy legislation articulated by CSPP last year. The legislation applies to both online and offline transactions, builds on industry's existing self-regulatory programs, establishes a national legal framework assuring protection, and enables consumers to control how their information is used. It calls for Federal Trade Commission (FTC) enforcement and penalization for privacy violations, as opposed to creating new opportunities for litigation. The legislation would double existing FTC fines for such transgressions. Finally, the Stearns bill calls for organizations to implement security policies to prevent the unintended compromise of personally identifiable information.

CSPP believes that consumers will be well served by a privacy protection regime that includes such industry best practices, vigorous FTC enforcement and baseline federal legislative protection. The CSPP companies have labored for several years at defining privacy risks and identifying legislative requirements.

Founded in 1989, CSPP's current members are: *Michael S. Dell,* chairman and chief executive officer of Dell and chairman of CSPP; *Craig Barrett,* CEO of Intel Corporation; *Carleton S. Fiorina,* chairman, president and chief executive officer of Hewlett-Packard Company; *Christopher B. Galvin,* chairman and chief executive officer of Motorola; *Louis V. Gerstner, Jr.,* chairman of IBM Corporation; *Lars Nyberg,* chairman and chief executive officer of NCR Corporation; *Joseph Tucci,* CEO of

EMC; and *Lawrence A. Weinbach,* chairman and chief executive officer of Unisys Corporation.

NATIONAL BUSINESS COALITION ON E-COMMERCE AND PRIVACY

June 18, 2002

Honorable CLIFF STEARNS
Chairman
Subcommittee on Commerce, Trade and Consumer Protection
U.S. House of Representatives
2227 Rayburn House Office Building
Washington, D.C. 20515

DEAR MR. CHAIRMAN: On behalf of the National Business Coalition on E-Commerce and Privacy, we would like to take this opportunity to express our views regarding HR 4678, the Consumer Privacy Protection Act of 2002.

The Coalition is comprised of major U.S. corporations from diverse economic sectors that strongly support a balanced and uniform national policy pertaining to electronic commerce and privacy. Our member companies are top competitors in the e-commerce marketplace and actively use the Internet to deliver goods and services to our customers. We are committed to ensuring the privacy and security of the information gathered from our customers, both on-line and off-line.

Mr. Chairman, we congratulate you on your leadership in successfully moving the privacy debate in a more positive and useful direction, and we thank you for your impressive effort in holding a series of important hearings on the various aspects of the privacy issue.

As you know, the Federal Trade Commission has stated that there is no need for the Congress to pass general privacy legislation. While Federal legislation is not necessary at this time, this situation would change dramatically if the states begin to pass legislation. If Federal legislation becomes necessary to preempt a patchwork of conflicting privacy laws at the state level, then HR 4678 certainly represents a reasonable and measured step forward in the privacy debate for the following reasons:

- *By effectively providing a uniform privacy standard across the nation, HR 4678 would avoid the danger of a fragmented e-commerce market, with all of the ultimately unworkable administrative requirements that would imply.* The preemption of state laws is absolutely critical to the continued growth of e-commerce. Having to adapt to as many as fifty different state laws would be enormously burdensome and would be a significant deterrent to the further development of e-commerce.
- *HR 4678 properly emphasizes providing notice of privacy policies to consumers and allowing customers to opt-out of having information about them shared with others.* We believe that this represents a reasonable and practical balance between consumer rights to the privacy and security of their data and transactions, and the legitimate uses of information by business to improve the quality, efficiency, and cost effectiveness of products and services that consumers desire. And requiring companies to prepare and implement information security policies will help assure consumers that the information about them is secure.
- *HR 4678 recognizes the importance of treating all business-to-consumer information in a similar manner—regardless of whether the information is acquired on-line or off-line.* As a general rule, business makes little distinction between information that it gathers on-line as opposed to that gathered off-line. To treat these two types of information differently would result in significant administrative burdens and legal liabilities—the costs of which business would be forced to pass on to the consumer.
- *HR 4678 avoids private rights of action and the potential for frivolous lawsuits.* As the FTC has recognized, existing enforcement authority is sufficient to deal with most violations of privacy laws and opening the door to private rights of action would simply create an environment conducive to unnecessary lawsuits. The only qualification we would add is that we would like to see class actions expressly banned.
- *Finally, it is important that HR 4678 addresses the issue of foreign privacy laws, especially since such laws may effectively be barriers to free trade.* Harmonization of national privacy laws is essential if the free flow of information that benefits businesses and consumers alike is to be maintained. A thorough study of the consequences of foreign laws like the European Union Privacy Directive, as well as their impact on U.S. competitiveness, is a critical first step to furthering e-commerce in a way that is fair to American business.

By adhering to the principles outlined above, HR 4678 is, on the whole, a fair and balanced approach and the most reasonable alternative currently pending in the Congress. As you know, we strongly oppose other proposed legislation, S. 2201, that is not consistent with these principles, and we are unable to support any bill that goes beyond what is now contained in HR 4678. We look forward to working with you to further refine and clarify HR 4678 if Federal legislation becomes necessary (for instance, in order to preempt incompatible state laws or to regulate unscrupulous actors).

We appreciate your willingness to work with us on this issue, and also very much appreciate the time your staff has taken to talk with us about this important subject. If you have any further questions, please contact John Schall at (202) 756-3385.

Sincerely,

JOHN SCHALL,
Executive Director

SUSAN PINDER,
Chair

Coalition Members: American Century Investments; AMVESCAP; CheckFree; CIGNA; Deere & Company; Dupont; Fortis, Inc.; General Electric; General Motors; The Home Depot; Investment Company Institute; Charles Schwab & Company; and Six Continents Hotels.

Mr. STEARNS. In this debate we are going to have a lot of people that support it and a lot of people who don't. And I think everybody who is on this subcommittee, including the full committee chairman, is on the bill except one. So these folks have a different approach.

So there is going to be a lot of debate here and we welcome that and we appreciate your comments. We may not necessarily agree, but we like to hear your comments.

As all of you know there is a bill in the Senate, and what I would like to do is start from my left to right and say the bill that we have, which is H.R. 4678, how does it compare with the comprehensive legislative proposals in the 107th Congress. What I am trying to do through this hearing is establish a baseline so we can say this is what is good about the bill, perhaps this is where the controversy is; so then I can go back to those folks who don't agree and be prepared to convince them to come on board and to show why they should.

So perhaps you could help me with actually making a comparison of my bill with perhaps Senator Hollings, Fritz Hollings' bill, and say what you are concerned about. Now, Mr. Rotenberg is going to say Mr. Fritz Hollings' bill—he is going to praise it. But I would like to, if I could, to put you all on the spot and ask that you tell me this morning about my bill or that bill or any bill that is in Congress, how it compares and why ours is better or not from your standpoint, because then what I would do is take the coalition of people that support it and say why we think this is better. Is that possible for you folks to take a shot at?

Mr. PALAFOUTAS. If you want this, Mr. Chairman, you are going to get it. I happen to go back to Mr. Rotenberg's comment about your bill and the private right of action, and I will just mention one thing about the Hollings bill. The private right of action does cause us a great deal of problems, and while there may be——

Mr. STEARNS. And I am not here to—you know, on the House floor you can't say anything negative about the Senate. You are called out of order. And I am not here to talk in a way that is negative, but just to say that from a policy perspective that this is something we are concerned about and why, you know. And—all

seven of you are going to have a different opinion, but that would put on the record our sticking points, because Senator Conrad Burns over there is the ranking and he has supported the bill. So Republicans and Democrats are not going to agree on this, as I said earlier.

Mr. PALAFOUTAS. Well, I too am not going to say anything negative about Chairman Hollings. I think one of the concerns—and I will pass the microphone down—is the private right of action. Mr. Rotenberg makes a good point about the Federal Trade Commission, and I think the Federal Trade Commission is the proper place to do it. They may need some beefing up on this. I know some members of their staff are here, and I won't say anything negative about the Federal Trade Commission either. But that is a concern for us in the bill, and we appreciate your bill puts the enforcement action in the bill.

Mr. SERVIDEA. Mr. Chairman, I am pleased to answer this question because I think until you decide what it is you are trying to regulate, what it is trying to legislate about, you basically have nothing. And I think the biggest single deficiency with respect to Senator Hollings' bill is the fact that the scope is so narrow as to apply only to on-line transactions. I think to pass that kind of legislation would be disingenuous as far as the American consumer is concerned. American consumers' personal data is their personal data. Doesn't matter where it is, doesn't matter how they released it, they should be protected.

Unfortunately, at the very end of the day, Senator Hollings put sort of a Band-Aid kick-off to the Federal Trade Commission to study offline. But the bill is basically an Internet regulatory bill. That is the biggest deficiency, frankly, is the scope of the bill. Second, I would comment that there is more than one privacy bill in the Senate, and Senator Feinstein's bill is an excellent bill.

Mr. SCHALL. Mr. Chairman, I would point out that the National Business Coalition on E-Commerce and Privacy actually sent a letter of opposition to Chairman Hollings on S. 2201 and we would be happy to furnish that to this committee because it delineates our five points of opposition. I will mention them here. First of all, S. 2201 is confusing in that it really creates four different categories of information: There is sensitive information, nonsensitive information, and there is not quite so sensitive information. I don't know if anyone can make sense of those.

Second, the point made already is online only. I think it is a disservice to the American economy to only focus on what is 1 or 2 percent of consumer transactions in the economy, and also keeping in mind the logistical problem that companies really don't sort information by where it comes from.

The third point is that S. 2201—and I don't know if it is intentional or inadvertent, it really empowers ways to revisit laws existing on the books in terms of GOB and HIPAA. I think—why, even some Democrat Senators on the committee—Senator Breaux raised some concerns about the bill. I am not sure one wants to take an on-line privacy bill, as S. 2201 would be, and have that revisited.

The fourth point is really remedies. There is far too much private rights of action. We have concerns about the strict liability and liquidated damages provisions.

Last, the preemption provisions in S. 2201 are truly inadequate, and I would hope when the Senate Commerce Committee revisits it, it looks at the model this committee used in H.R. 4678, because the preemption provisions are so much more sensible in this bill.

Ms. WHITENER. I would like to go back to a letter that was sent by our CEO in his role as chairman of the Digital Economy Task Force, Business Roundtable, outlining some concerns with this particular legislation, and I will just kind of summarize.

The creation again of that new private right of action when sensitive information is compromised is considered unnecessary and will have many unintended and negative consequences. The provision will open a Federal class action floodgate that will hinder further innovation by businesses that fear any change in their on-line information management practices will be met with lawsuits. S. 2201's mandating opt-in for sensitive information could place improper burdens on consumers. Mandating opt-in may be intrusive and inconvenient and could remove opportunities for consumers.

The legislation ignores the significance of providing consumers with effective and credible options to make informed choices regarding the use of their information. S. 2201's access requirement will increase costs for businesses while reducing consumer information security. Though the provision mandates more consumer access to private records, the result could actually reduce consumer information security requiring simultaneous reasonable access, and security could increase identity theft and place obstacles in front of the companies desiring to take innovative security steps.

S. 2201 inadequately preempts inconsistent State laws. The bill's preemption language would only impact personally identifiable information which is collected and used online. The legislation does not effectively address the problem of inconsistent legislation and legislation imposed by State governments in a meaningful way.

S. 2201 on-line and off-line information collection is technically infeasible and economically unreasonable. Companies that digitally collect personal information will be held to a different and higher standard than those in more traditional businesses. The bill creates separate but unequal burdens and regulations, and conflicting privacy standards particularly, in which consumer information is collected both online and offline.

In summary, the Digital Economy Task Force of the Business Roundtable summarized the legislation to be fundamentally flawed, overly burdensome, and promises to impede technological innovation and electronic commerce, plus it will raise the cost of compliance and encourage endless litigation and force many of the most innovative traditional electronic commerce companies which are usually small businesses, to abandon the promise of a digital economy.

Ms. BARRETT. Thank you, Chairman. I think there are seven key differences between your bill and the Senate bill, and I am not going to go back over all. Obviously the on-line versus—on-line/off-line nature of the bill. The second is the private right of action. The third is the preemption. And I think in preemption, we really do need to look at it both from the business community's perspective as well as from the consumers' perspective and how confusing it is for the consumer who works in one county and works in one State

and lives across the State line to deal with a myriad of privacy laws. The fourth is enforcement and self-regulatory efforts, which I commented on. The fifth is harmonization with other laws where we have specific laws recently enacted.

Mr. STEARNS. Particularly with international.

Ms. BARRETT. International, health care, financial services, children, the list goes on and on. And I think it is critical that we recognize the appropriateness of those laws.

The notice and choice provisions of your bill do work in an on-line and off-line environment. And I think it is important that we look at notice and choice across mediums. I don't think we can sit here today and foresee where technology will take us and what new mediums we may be dealing with. And when we look at legislation which is specific to one medium, I think we have serious unintended consequences down the road when the technology changes. And the last is the access provision which I commented on in my testimony.

Mr. MISENER. Mr. Chairman, I agree that the biggest concern with where S. 2201 began was with the focus exclusively on on-line transactions. And then in April's hearing, at which I also testified, I believe the committee frankly was moved by some of the testimony which described how the bill would only touch 1 or 2 percent of consumer transactions and could do nothing for those on the unfortunate side of the digital divide.

By the end of the hearing, every member of the committee had spoken in favor of looking at off-line privacy as well. So I would like to think that there is movement to sort of coalescing around an agreement which incorporates a holistic view of consumer information privacy.

Mr. ROTENBERG. Mr. Chairman, I think it is important to understand first of all that Senator Hollings' bill in the 107th Congress S. 2201, is very different from the bill in the 106th Congress, and that a lot of progress was made to try to resolve some of the differences between consumer groups and business. And, frankly, we agreed to a lot of things which I felt was possibly going too far on many of the key issues.

On the opt-in issue we said maybe for most transactions opt-out was more sensible if it could be made to work. On the private right of action we recognized that there had to be some limitations. And, frankly, we are not in favor of creating a private right of action that enriches lawyers. We would much rather see consumers' interests protected, and that is the issue that we focused on. On the preemption issue there was also some effort to allow some action for States, and at the same recognizing a need for national standards.

So my sense about S. 2201, in fact it was a sensible compromise where both sides gave up something—and I am trying to figure out on the spectrum where we would put 4678. It seems to be the counter position from the Hollings bill in the 106th Congress.

Mr. STEARNS. That is how you would put it in the spectrum?

Mr. ROTENBERG. Yes, sir, I think I would. Because as I said, there are two very different bills that have come out of that committee, and the current one is not the one that was in the previous Congress. The other point——

Mr. STEARNS. Do you support the one in the 106th?

Mr. ROTENBERG. Yes.

Mr. STEARNS. That was better from 107th?

Mr. ROTENBERG. From a privacy viewpoint, yes. It gave more rights to consumers. The bill that was reported out of the Senate Commerce Committee, as I said, was significantly scaled back. It did not include a lot of the provisions.

Mr. STEARNS. But your organization supports the Senate bill.

Mr. ROTENBERG. Well, I testified on that bill, and I think we said largely that it could be made to work.

Mr. STEARNS. With some minor changes, you would support, your group would support that bill.

Mr. ROTENBERG. I think if enforcement is serious and there is a cooperation on both sides, it could be made to work. But it is a very different bill from the one we were looking at a couple of years ago. The other point——

Mr. STEARNS. Do you think he should have dealt with off-line and on-line privacy the same?

Mr. ROTENBERG. This is the point I wanted to get to. And I have to say as the debate has progressed, I think the case has been made particularly well, you know, on this side that off-line does need to be addressed. And I think in this respect, you know, the Senate bill probably does come up short, and I imagine from the business perspective it doesn't seem like a sensible distinction.

I have to say our concern on the Senate side is that many who said, if you are going to pass a privacy bill you need to do both, was that the people who took that position really didn't want a privacy bill. And my view is if you are going to take the position you need to do both, I think you have to be prepared to back the bill. You can't say let's make the problem so large we can't solve it. That is not an approach to finding a solution.

Mr. STEARNS. Mr. Schall mentioned two local communities in California now have passed privacy bills. Are you concerned about the balkanization in this country—different States and communities having different thoughts?

Mr. ROTENBERG. I am primarily concerned about the protection of privacy in America. And what is extraordinary to me is how hard people across this country are working to protect their privacy. I haven't seen an issue in the last 10 years that has generated this type of activity at the local level. And I think that should send a message to the Congress that people want a strong bill.

Mr. STEARNS. I thank my colleague for his patience and recognize the gentleman from Virginia.

Mr. BOUCHER. Thank you, Mr. Chairman, and I want to express my appreciation also to the witnesses who testified today. You have prepared thoughtful testimony and you have delivered it well and we appreciate your contributions to this ongoing discussion.

I want to direct my question to the international provisions that are contained in the bill and get the views of witnesses with respect to those. Several years ago there was a carefully negotiated safe harbor achieved between the United States and the European Union. It was designed to enable the continued flow of data between the European operations of American companies and their American operations, notwithstanding the fact that American law

does not contain the formal privacy requirements that are extended by the European Union, which has very thorough privacy guarantees, well beyond what American law provides and beyond in fact what this bill provides.

It was a carefully negotiated agreement. Many Members of the U.S. Congress were involved in the discussions that led to that agreement. In fact, Mr. Goodlatte and I, the co-chairs of the Congressional Internet Caucus, testified before the European Parliament at one point, urging support for and implementation of the safe harbor. And it was implemented. I am sure our testimony had little to do with that result, but we were very pleased when that result was achieved.

My general reading is that this safe harbor arrangement has been working well, and we now have more than 240 American companies that have registered under it and have agreed to the conditions that are contained in the safe harbor. And I think people on both sides of the Atlantic are relatively pleased with the results of that arrangement.

The last thing that I would like to see is something contained in this bill, were it to achieve passage, to adversely affect the safe harbor arrangement. And I would like your views about whether or not these international provisions might do that. The international provisions are designed to address the concern that some companies have voiced that there are other European policies that have a discriminatory effect with respect to American companies that adversely affect American companies in comparison with their European counterparts. Some have suggested that some of these European policies are intentionally designed to favor the European companies, that these are not inadvertent consequences of the implementation of the European policies.

So there is a level of concern about this discriminatory effect on the part of some American companies. That concern has been reflected in the international provisions in this bill, which are quite explicit about what American agencies are supposed to do in the event that the U.S. Administration finds that there is a discriminatory effect. And point in fact: At one point the bill even says that no Federal agency may continue any action to enforce even agreements that the United States has entered into if those agreements lead to some discriminatory effect.

Now, bearing in mind that the safe harbor arrangement continuation depends entirely upon the voluntary willingness of the European Union to continue it, I am wondering how irritating you think this provision might be and whether it might at some point—would lead the European Union to suggest that——

Mr. STEARNS. Will the gentleman yield?

Mr. BOUCHER. Let me just finish the question and then I will yield.—to suggest that perhaps if we are going to behave this way, we are going to have some different view of whether the safe harbor ought to be continued.

I would be happy to yield.

Mr. STEARNS. I am going—we are going to take a 5-minute break. I have to make one call and a lot of the members haven't come in. We don't have votes until late tonight. We are going to

take a 5-minute break and we will be right back and that will give you a chance to ponder his question.

[Brief recess.]

Mr. BASS [presiding]. Sorry for the momentary interruption. We are all playing musical chairs. The chairman had to go down to make an opening statement. I am not sure he mentioned that. If he did, we certainly apologize for the interruption, and I would continue to preside until he runs. My understanding is that Mr. Boucher asked a question and we were waiting for a response.

Mr. BOUCHER. Mr. Palafoutas, let us begin with you.

Mr. PALAFOUTAS. To say we have a concern is to say just that, and the bill recognized that, in that the Secretary of Commerce has the responsibility, if the bill is enacted, to see if this harmonizes. Our concern is predicated in some respect on the meeting Chairman Stearns had with the privacy officers of the EU back in January. And they have a different view of what is going on in terms of privacy. And as you mentioned, I think the number is 242 companies have signed up under the directive, and we are not sure how the Europeans will respond. From our standpoint we just don't know. I am sure others have other opinions.

Mr. BOUCHER. When you say you don't know, let me plumb that a little more deeply. Are you a little bit apprehensive if we enact this provision into law that the Europeans could potentially respond by being less interested in the continuation of the safe harbor provision? It is purely voluntary on their part.

Mr. PALAFOUTAS. Yes.

Mr. SERVIDEA. I think to start out, I would say, yes, we do share the concern that perhaps it could disrupt what we think is probably an arrangement that is working well at the moment. As you pointed out, there are over 240 U.S. Multinational companies who have decided to voluntarily certify into safe harbor. And I think we have to start from the premise that the European governments have certainly the right to protect their individual citizens' privacy just as you do, you know, U.S. Citizens. And we can do that with them under individual legal contracts with each of the data protection ministries or we can do it under the Safe Harbor Agreement. The Safe Harbor Agreement happens to be a much more efficient way to do that instead of having to deal with 15 different data protection directives on perhaps a very specific—sectoral-specific contracts. We can certify under the safe harbor to all of that and have the U.S. Regulatory agencies being the enforcement mechanism. We think it is working well and we would not like to see it disrupted. We think sections 302 and 303 possibly could do that. Section 304, which calls on the Secretary of Commerce to work on harmonization, we think is probably worthwhile.

Mr. BOUCHER. I share the view you have expressed, and I would hope as we examine these provisions once again in anticipation of enacting the measure during the next Congress, we could revisit these international provisions. And if you would be so good perhaps as to communicate this view somewhat more persistently during the drafting process, I think that would be beneficial to all parties concerned.

Mr. Schall.

Mr. SCHALL. I am glad you brought up the international provisions, because I think the whole international question is important to this debate and you should be commended for your leadership with our European counterparts on this issue and also for going the extra mile with some of our companies in talking through how some of this works.

With respect to the safe harbor—and I must say over the course of the history of the National Business Coalition on E-Commerce and Privacy, we have had some companies who are in the safe harbor—lots of companies who decided not to be in it. What we are concerned about is there is a level playing field between us and the Europeans. And I think that is why the call for the study in here is probably worth doing. In fact, it is sort of perhaps surprising that a study of this sort wasn't done before when we first entered into the safe harbor during the previous administration.

Clearly, we all need to remember you are dealing with a whole different culture over there in terms of both enforcement and litigation, much more haphazard enforcement on the European side than we see over here, and a very important distinction in the litigation culture where, by and large, loser pays over there. Tremendous disincentive to bring lawsuits. Obviously, we don't benefit from that approach over here. Perhaps if we did, we would have a different view.

A lot of the companies decided not to pursue the safe harbor, hoping that model contracts would end up being better, and then we of course subsequently discovered that the model contract that the Europeans decided to draw them out were not better, in fact were worse, and you have been a part of that discussion as well.

I would, however, share your concern with the particular provision in this bill that has Congress dictating to the Secretary of Commerce on how to enforce those provisions. I think that would probably raise a constitutional concern, so I think that is worth looking at, though I think the study itself would simply benefit everybody.

Mr. BOUCHER. Anyone else care to comment on that?

Ms. WHITENER. I won't restate some of the comments made here. I would like to point out in section 304 we believe the approach is on target. Again, some of the issues that have been raised we certainly do feel would warrant perhaps some additional discussions. But in general, we believe that businesses should have the freedom to operate globally under harmonized laws, and if you have processes that leave a door open for a claim of inadequacy, that it does little to promote e-commerce.

Mr. BOUCHER. Section 304 just deals with the general efforts to provide notice to other countries about problems that we have and generally would be in pursuance of harmonization. That is not the more troubling section that actually would inhibit enforcement of agreements we already have in place. Anyone else care to comment?

Ms. BARRETT. I would like to say I am commenting on behalf of Acxiom and not the three companies that I testified. Acxiom is a member of safe harbor, and we do business in almost all of the European countries and have found it to be extremely beneficial in facilitating relationships both within Europe—global companies

working with information flows across those borders. We certainly would not want to approach any kind of study with a "let's find problems" kind of attitude. If it is a balanced study and it does get to the facts and identifies any issues or any problems that exist, we think it might be very appropriate. But we need to be cautious about the tone in which we approach it.

Mr. BOUCHER. I think we agree, and I detect a consensus everywhere and I share this, that we ought to have the study provisions. The real troubling provisions are those that would inhibit enforcement of agreements already in place, and perhaps we could do without that, while promoting harmonization and promoting a study of the effect the policies that Europe has with respect to American companies. And if there is discriminatory effect, we ought to talk about it and try in a persuasive way to remedy those problems.

Thank you very much for your comments on this. Mr. Chairman, I don't have any other questions. Let me simply say—the other chairman is not here, but let me again say that I think Mr. Stearns has done an outstanding job in plumbing the depths of a very complex subject. The hearings he has held are unprecedented in our Congress on the question of privacy assurance. We have built a tremendous committee record on this subject and I think we are ready to act in the next Congress. And with the support of those at this table and with good consultation from those who may not agree with all of the provisions, Mr. Rotenberg, hopefully in the next Congress we can achieve the enactment of a measure that assures for American consumers greater privacy protection.

Mr. BASS. Thank you, Mr. Boucher. I am sure that the other chairman will appreciate your kind remarks.

I was wondering if each of you could comment on the cybersecurity provisions of the bill.

Mr. PALAFOUTAS. The short answer is we appreciate those provisions and we think that they need to be in the current form, because people are concerned about the things that come up about their identity and the security of personally identifiable information. So from my company standpoint, these provisions are good.

Mr. SERVIDEA. I will take a pass on that, if I can.

Mr. SCHALL. We are glad there is a security component in the bill. You know, it is funny; we all bandy about the word "privacy" in this debate. But in a very real way, privacy is a misnomer, in that in the most fundamental sense this is a debate about data management and security. And I think a lot of the concerns that real people genuinely have when they think in the world of privacy are really security concerns about their data, how it is stored, and how it gets used.

So I have to commend Mr. Stearns and the staff and the members for putting in a security component in the bill, because in fact I think the terms do get conflated in some sense, and it is important to realize that a lot of what we talk about when we are talking about privacy, we really mean security. And for there to be a security component in the bill I think draws it out in a very important way.

Ms. WHITENER. Well, certainly in the testimony that I gave, I sort of concentrated a little bit on this area of security—because,

again, in viewing the importance of security, it is critical—is the underlying actual foundation of being able to enable your privacy policies. We work together with clients when we are looking at security, and we are looking at privacy issues certainly to look at the security in place, and it is critical.

We believe that what is built into this bill from the standpoint of the development of a policy, that consideration of a policy and the approval of the policy by senior management is also very critical because that does raise the awareness to the levels at which a company can begin to realistically assess the risk associated with the security within the organization and begin to make decisions about generally the costs and the benefits and how to mitigate the risk and to how to best absorb the risk, transfer the risk, or how to deal with it just as any other business risk. But it is critical that senior management understand and appreciate the risk that security brings to their organization, and so we certainly support that.

We also support the fact of a designation of someone within the organization to have that as a responsibility. As I mentioned, many organizations have someone within their IT or within the organization that has either a part-time or some role centered around security. But it is very important within a company for there to be a channel, a point person for when there is an incident; that someone knows who to go to to report it to, and someone who has ultimate accountability for the security programs. So we are in support of the security that is within this bill.

Mr. STEARNS. I don't know—I guess—let me ask Mr. Rotenberg a question. You mentioned something about the sharing of information dealing with law enforcement agencies. And is there any prohibition dealing with marketing information?

Mr. ROTENBERG. I am sorry?

Mr. STEARNS. In other words, you are concerned and want that there should be more prohibition in dealing with law enforcement agencies. You mentioned Acxiom and how they are sharing their information.

Mr. ROTENBERG. I didn't say prohibition, Mr. Chairman. In my testimony I tried to explain that typically what is done in a privacy law is to create a fourth amendment standard, so if there is probable cause or reasonable suspicion, the police will get access to records that are held by the business. And I think that is the appropriate standard and that is the traditional standard. There is—my concern here is that first of all there is no standard for law enforcement access in the bill.

Mr. STEARNS. You would like us to incorporate some standard, then?

Mr. ROTENBERG. Yes. As I said, it could be borrowed from almost any privacy law. It is done in everything from video rental records and e-mail to cable subscriber and financial that could be done here.

Mr. STEARNS. I guess Acxiom—maybe your comment, too, about what he just suggested.

Ms. BARRETT. Well, we certainly agree that the use of information by law enforcement when it is warranted cause is appropriate. And I am speaking on behalf of Acxiom. We do not believe that, you know, law enforcement should have unfettered access to all

kinds of commercial information, nor do we provide or participate in such practices.

Mr. STEARNS. Mr. Bass, would you like to——

Mr. BASS. One last question briefly. How will the provisions of the bill that we are deliberating on relate to provisions passed in Gramm-Leach-Bliley and other privacy-related aspects of HIPAA?

Mr. SERVIDEA. I think the bill does a pretty good job of specifying that the existing legislation that deals with specific sectors such as health care and financial services, that those bills take precedence over this bill. And I thought that the statement of the, if you will, preemption of those bills was pretty explicit and the list is pretty thorough. So—and we support that.

Mr. BASS. Any other comments?

Thank you, Mr. Chairman.

Mr. STEARNS. The gentleman from Oregon.

Mr. WALDEN. Thank you very much, Mr. Chairman. I wanted to ask, following up on Mr. Palafoutas' testimony, this issue of the EU safe harbor provisions, can you give me a little better understanding in terms of what we might need to do in this bill to make that work?

Mr. PALAFOUTAS. As we discussed before, ours is a concern about the EU and their response to this particular bill. I think it is a matter that we want to rise to the level of conversations with members of the privacy officers and the various customers to see how they react to that, because it is a problem in that there is uncertainty there. And that is the only problem there is the uncertainty.

Mr. WALDEN. Do you think you can get over that issue? What does it take to get over that?

Mr. PALAFOUTAS. I think the bill provides for some of that, with the Secretary of Commerce taking a look at this. And even preliminary discussions, the chairman has had these discussions in the past with the DPAs. I have had them in here in January and we had some pretty open discussions at that time. They are willing to talk about it because this is of great importance to them, although they have a different perspective on privacy from what we do in the United States.

Mr. WALDEN. Anyone else want to comment on that issue?

Mr. SERVIDEA. I would like to say that Congressman Boucher really kind of hit the nail on the head. Certainly a study, an effort to determine where we don't have harmonization, could be valuable. I think the difficulty with this is that it kind of puts down the gauntlet and says if we can't get harmonization, then we are going to stop enforcing the Safe Harbor Agreement. And I think throwing down that gauntlet is extremely unfortunate. So I would suggest taking out that provision of the bill which is section 303, would be very helpful and probably would avert a problem with the European Union, and God knows we have enough problems with those folks already. This seems to start us down the road of where we went with FSC. We put the threat down and then it just becomes increasingly a problem. And I think for most American corporations right now, safe harbor is a working option and we would not like to see it disrupted.

Mr. SCHALL. If I could jump in there, I think one thing important not to lose when we are looking at how we interact with the EU

is some sort of holistic approach of how this comes together. And I think that is what is to be credited in this bill in asking the GAO to look at it, because we have only ever looked at pieces. The 15 major companies in my coalition, all are multinational and almost all deal in Europe, including actually America's biggest employer in Europe, General Electric. Because of the difference in the enforcement culture, because of the difference in the litigation culture where loser pays over there, it is a very different environment. And I don't think anybody has walked through yet how those differences impact our companies in operating with that data.

And also remember, too, we only ever looked at a piece of it. Safe harbor which frankly has not really been huge companies—240 companies is obviously much fewer than the Department of Commerce would have ever predicted and many fewer than the Europeans would have hoped, you know; even safe harbor doesn't include financial services companies that are still hanging out there because the Europeans refuse to accept the fact that Gramm-Leach-Bliley as passed by the Congress and signed by the President is American law and ought to be deemed adequate for EU purposes. So there are always still financial companies still hanging out there. They don't have a safe harbor to go into. And I have both financial and nonfinancial companies in our coalition. I think what is important not to lose here is the bill, asking someone let us finally do this work that we probably should have done 4 years ago that tries to get a holistic look and evaluation of this situation.

Mr. WALDEN. Anyone else have a comment on that? Mr. Schall, can you explain your understanding of what is being considered in San Mateo, California, and is this permissible under other privacy laws such as the privacy protections within Gramm-Leach-Bliley?

Mr. SCHALL. What we see happening in California right now, San Mateo County and Daly City have already both passed their own separate opt-in privacy laws. They took us a model bill that was in the California legislature statewide and did not pass in the California assembly. So these local jurisdictions have begun to pass it. Actually five other counties and cities in that area will do so in the coming weeks. Those bills actually differ from one to the other, even though they are generally sort of similar in opt-in, but they have different remedies, different enforcement provisions.

Actually it is an interesting situation. Daly City is in San Mateo County and San Mateo County passed a bill and then Daly City passed a bill and they are not identical. What we see is now with the potential of who knows how many local jurisdictions passing conflicting privacy laws, I don't know how you comply with that. Certainly there is a court challenge already to those under both the National Bank Act and the Fair Credit Reporting Act. I think the Fair Credit Reporting Act challenge is a strong one, but the Fair Credit Reporting Act would only apply to sharing with affiliates so it would not—even if it was found valid by the courts—would not throw out the entire law. And I think because of that, what you are going to see is a lot of these popping up.

I think under recent Supreme Court rulings you would have to come to the conclusion that Gramm-Leach-Bliley may well not preempt them. Unless there is a specific prohibition on jurisdictions within States, then you probably haven't preempted locals from

doing that. I think now we have this situation and I think that is frankly why we are going to need a bill because you have already seen some localities passing bills.

Mr. WALDEN. Given—do you believe that this bill's provision's banning private rights of action and preempting State action can be interpreted to permit or allow class action lawsuits in States?

Mr. SCHALL. Right now?

Mr. WALDEN. No. Under this legislation.

Mr. SCHALL. I don't see anything under this legislation, on the advice of counsel—and perhaps others know better—I don't see anything in this legislation that changes what is existing private-rights-of-action State AG authority under existing mini-FTC acts passed by each of the 50 States and District of Columbia. I don't think anything here changes what is already existing in terms of what can be done at State and local levels in terms of enforcement under mini-FTC acts.

Mr. WALDEN. That is all the questions I have.

Mr. STEARNS. I thank my colleague. Let me just before we wrap up, just touch a little bit, Greg, on what you just talked about, which I think is going to be the hard fight, because you have a lot of policy decisions but then you come down with one or two political ones. And this banning the private right of action and preempt State action is going to be the political fight, because there are people who fundamentally think they should be able to go to the Federal courts and be able to sue. And so that might be an area where we are going to have to find some kind of compromise to get this through. As you know, with a political consensus issues work through themselves successfully and that is why we have the ballot instead of the bullets. So it is really a remarkable process so I am very sensitive to that.

I guess a question, Mr. Schall just touched on—I will go back to you—if we have in the bill this banning private right of action and preempting State action and maybe someone else—Mr. Rotenberg, you can help me out, too—would that eliminate class action suits at the State level? Could that eliminate all possibilities of States attorneys general getting together and working to do something? I am not a lawyer, but it would seem to me that we are trying to keep it on the State level and not on the Federal level. But there might be ways for attorneys general in class action suits to get together.

Mr. Rotenberg, let me have you start, because you are probably more supportive of this.

Mr. ROTENBERG. I appreciate your comment, Mr. Chairman, and I really do want to emphasize that my position and the position of the privacy community generally is not to enrich lawyers.

Mr. STEARNS. Oh, no.

Mr. ROTENBERG. And I want to make sure how strongly we believe this. I went up to New York to participate in a Federal Court proceeding as an intervenor to object to a settlement in a case where the lawyers were getting paid and nothing was being provided to the consumers for a breach of privacy, and I said to a Federal judge I thought this was not appropriate. So I would look for approaches that address the concerns of the business community about not being exposed to class action liability. I think you know

the opportunity under the Telephone Consumer Protection Act, for example, which allows people to get damages of $500 if they go through all the steps of notifying the company first and then going to small claims court is not about approach for privacy issues. And I think there are also ways in terms of the State attorneys general to allow them to enforce rights set out under Federal statute, which was the approach that was ultimately settled upon in the revised Hollings measure.

So I think there are ways here in the middle area to address concerns on both sides, but I believe very strongly the flat prohibition on private action joined with this very strong preemption is really shutting the door on privacy claims.

Mr. STEARNS. Well, I am sensitive to that. We have this and we support it, but I am looking for possibilities, if I can get a markup out of my subcommittee and get it to the full committee. I mean, to get a lot of the Democrats on board is going to require some compromise in that area, and I see that as one of the problems, early on problems, so any solution that you have.

Mr. Schall, I will let you answer first.

Mr. SCHALL. Well, I am glad Mark Rotenberg and I agree that this should not be a trial lawyers enrichment act. As we read the bill, there is nothing in your bill that bans class actions. So no, they would not——

Mr. STEARNS. They could go to the States?

Mr. SCHALL. Absolutely. And that point is definitely worth underscoring. States still have the opportunity to act under this bill through mini-FTC acts that have been passed by all 50 legislatures and the District of Colombia, and indeed if States want to go back and revisit mini-FTC acts that they passed, they are free to do that as well. So State attorneys general have the ability to act in private rights of action at local levels.

What this bill does not do, and I think exactly is the right decision, is not create some new Federal private right of action for this bill, leaving the enforcement authority to the FTC where I think it legitimately belongs. So nothing in this bill changes what is already there in terms of class actions and State attorneys general under mini-FTC acts.

Mr. STEARNS. Mr. Misener.

Mr. MISENER. Mr. Chairman, we have testified on a number of occasions that we oppose private rights of action in this new kind of a privacy law. And certainly we would also oppose class actions. To us it is a subset of private rights as a specific type of action, and we ought not have newly granted private rights under this kind of a bill. This isn't though, however, a traditional case of businesses just being afraid of the trial bar and issuing any kind of private rights for fear of large judgments and that sort of thing. It really goes to the ultimate goals of this legislation. And it seems to me that the ultimate goal is giving consumers informed choice about their private information: what they have done with it, where they provide it, where it goes thereafter. And that kind of informed choice relies on information and having the consumer truly be informed of what is going on.

I think it would be easy for companies, responsible companies like the ones that come and testify before your subcommittee, my company certainly, to write a very thorough legalistic privacy notice that would withstand any kind of a private challenge. It would hold up and it would be 5, 15, 20 pages long, small type, and all those sorts of things, but the fact of the matter is consumers will never read that. What they want to read is something really clear, bullet points, couple pages long, that is understandable and in English.

Mr. STEARNS. Or their lawyer can read.

Mr. MISENER. And so I guess our concern, Mr. Chairman, is if we are subjected to the class action bar, to the plaintiff's bar in general, what we will find is that companies will back off and make their policies a lot less readable for the sake of legal defensibility. It seems to me a public enforcement mechanism, such as through the Federal Trade Commission, could take into account those competing goals of precision and readability.

Mr. STEARNS. Anyone else wish to comment on that? I will close with asking each of you perhaps just the cost of implementation of H.R. 4678; you know, do you see any large costs for implementation of this bill? And you might just say what you would foresee if you had to implement the one on the Senate side, just to give me an idea of some—I don't know if you can quantify it, but you might be able to speak in broad terms—is this going to cause an enormous additional cost for you and your companies?

Mr. PALAFOUTAS. As you know, Mr. Chairman, the most visited Web sites already have a clearly defined privacy policy and do all that they can to protect consumers' privacy. I think in terms of cost to the companies, I don't see a great cost. I think it is of great importance to consumers that they do this certainly across State boundaries; and that is the biggest thing that this bill does, just to make it seamless. You take a look at the local municipalities—now the States, consumers can have certainty on interstate commerce. This is going to continue. The one big cost that consumers talk about is they want a free Internet. We don't talk about that other side.

If you were to do a survey of everybody here on the panel and ask are you concerned about privacy on the Internet, of course we are concerned about it. But as Mr. Rotenberg said earlier, there is a tradeoff, and part of the tradeoff is still get my name, address, and telephone number for certain uses. But I think your bill brings certainty into the marketplace, and anytime there is certainty in the marketplace, that is a good thing and a plus for industry and a plus for consumers.

Mr. SERVIDEA. Mr. Chairman, I don't—speaking for NCR and for the rest of the companies—I don't really foresee a great expense involved in implementing H.R. 4678. I think most of the companies have already put in place the provisions that you are asking for here. I think with respect to the Senate bill, I think because of the fact that it differentiates so much between different types of information, as was pointed out—sensitive information, insensitive information, on-line information versus off-line information, whereas most of our systems, most of our practices and procedures, are to treat data—as I said, data is data and we treat data pretty much

the same way. If we had to go back and try to refigure out how we are going to treat it, that is where the cost would come from.

Mr. SCHALL. Sure, there are costs, and I would suspect we will all find they are much higher than we think, but we consider them to be legitimate costs. But I will give one example. One of our coalition companies, Check Free—California passed the law that this is how you deal with Social Security numbers in terms of financial transactions—required a change in the management system, $250,000 just in that State. One State, one company, and multiply that by every company in every State, sure the costs add up. But we considered the costs that would be associated with the changes outlined in this bill obviously are far lower than what you would see in the approach in S. 2201; higher costs which frankly wouldn't result in any added benefit to consumers, and I think that is the real problem.

And then to underscore the other point, what would be most expensive for us and, of course, possibly impossible to comply with and no benefit to consumers, is to have some patchwork. We have to have any number of information systems to meet those particular regulations.

Ms. WHITENER. I think most companies, as we look back at the ones who have been out front in this issue and have been moving forward with very effective security and privacy practices, have found that their investment in these practices has actually been creating returns, and that it can be used as a business enabler.

Mr. STEARNS. Cost of doing business.

Ms. WHITENER. It is a cost of doing business today. Companies need to understand what their customers and consumers are asking for, what their needs and expectations are, and they have got to be able to respond quickly to those needs and expectations. And certainly privacy and security are certainly two of the demands that they are facing. So if you take away any type of compliance-driven initiatives, many companies today are working to meet their customers' expectations for security and privacy, and they are finding that as they implement effective information handling and security behind that, that that is enabling business processes and content sharing and more effective opportunities for revenue enhancements than it had before. So if we look at the costs there, I do believe that you can see some rationalization of the costs as an investment and very proactive business practices.

Ms. BARRETT. On behalf of Acxiom Corporation, the costs are minimal to implement this bill. Most of the provisions are already industry practices and certainly practices that we think are appropriate practices and that build consumer confidence. And I would echo the comments just previously made, that it is really about trust and not about compliance when it comes to building relationships with consumers.

I think that where the cost of this bill may be borne by companies that have not participated in self-regulatory programs or other programs and activities, then they will have the costs to implement the kinds of notices, choices, and security practices that many of us have had in place for a number of years.

Mr. MISENER. Mr. Chairman, it is unlikely that H.R. 4678 would cause us to expend much and many resources to comply. It is not going to cause us to change our practices in any substantial ways. In fact, it is not even clear that S. 2201 would have those direct material costs on a company like Amazon.com, which already has had excellent privacy practices in place for quite some time. The costs of S. 2201 are not in the implementation side but more in the litigation side, defensive side. Defensive in two senses: One is defense from the litigators, and Mark will tell me who are consumers and not litigators.

But the point is that consumers don't view privacy as a vector, nor should they. Otherwise, we would wall ourselves off in cinderblock. They want a combination of privacy, convenience, selection, personalization, all the things that go along with that. And our goal is to try to serve the overall customer desire for shopping.

The other aspect of this, of S. 2201's potential costs on us, would simply be the competitive costs. If we are competing with on-line retailers, including the largest company in the entire world, if the same regulations are not applied to them as would be applied to us, we can see substantial competitive risks as well.

Mr. STEARNS. I assume you will send a letter of support for the bill then? We will use your testimony as an endorsement somewhat.

Mr. ROTENBERG. I am still working on my letter, Mr. Chairman.

Mr. STEARNS. We will be waiting.

Mr. ROTENBERG. I think it is very important to keep in mind costs to consumers, because ultimately when you are talking about the protection of privacy, you are talking about the concerns that consumers have about the loss of privacy. And there can be hard costs in identity theft, which State attorneys general say now is the No. 1 white collar crime in America. There can be soft costs in the sense that the businesses you are dealing with in trying to establish relations of trust are routinely taking your personal information and selling it to third parties for other purposes. Now, it is hard to put a price tag on that, but it is very real—I think the large problem here that needs to be solved.

But I think what unites the consumer groups and business groups is the belief that the cost to consumers to participate in new services should not be their loss of privacy. They should not be asked to trade their privacy to be able to take advantage of opportunities in the marketplace. And so I think we need a bill that minimizes that cost and lets people participate and safeguards their privacy.

Mr. STEARNS. I thank all of you for attending our hearing. And as we move forward, any of you who have not written a letter of support, we would appreciate it because that works in getting Members to come on the bill.

The second point I would make is that what Mr. Shaw mentioned in California, there is going to be much more of an impetus to this get bill marked up and get it to be visible. I invited the chairman up. He is down in an oversight hearing on Global Crossing. But the bottom line is I need to convince more Members and the leadership of my party how important it is to get this as a benchmark before

we get all these communities and 50 States out there with a bill which will cause—talk about costs that was alluded to.

So again, I think we made a good start and a lot of your testimony will help, I think, clear a lot of issues for Members and we will keep working on this. And with that the committee is adjourned.

[Whereupon, at 11:25 a.m., the subcommittee was adjourned.]