# INFORMATION PRIVACY: INDUSTRY BEST PRACTICES AND TECHNOLOGICAL SOLUTIONS

## HEARING

BEFORE THE

SUBCOMMITTEE ON
COMMERCE, TRADE, AND CONSUMER PROTECTION

OF THE

COMMITTEE ON ENERGY AND
COMMERCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTH CONGRESS

FIRST SESSION

JUNE 21, 2001

**Serial No. 107–38**

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
73–730PS WASHINGTON : 2001

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

## COMMITTEE ON 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
STEVE LARGENT, Oklahoma
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

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*

NATHAN DEAL, Georgia
*Vice Chairman*
ED WHITFIELD, Kentucky
BARBARA CUBIN, Wyoming
JOHN SHIMKUS, Illinois
JOHN B. SHADEGG, Arizona
ED BRYANT, Tennessee
STEVE BUYER, Indiana
GEORGE RADANOVICH, California
CHARLES F. BASS, New Hampshire
JOSEPH R. PITTS, Pennsylvania
GREG WALDEN, Oregon
LEE TERRY, Nebraska
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:

Cerasale, Jerry, Senior Vice President, Government Affairs, Direct Marketing Association, Inc ..... 59
Cole, Steven J., Senior Vice President and General Counsel, Corporate Secretary of the Council of Better Business Bureaus, Inc ..... 66
DeVault, Jerry R., National Director, Innovative Assurance Solutions, Ernst & Young ..... 73
Hsu, Stephen, Co-Founder, Chairman and CEO, SafeWeb, Inc ..... 29
Hughes, J. Trevor, Director, Privacy Compliance, Engage, Inc ..... 55
Rotenberg, Marc, Executive Director, Electronic Privacy Information Center ..... 76
Schlosstein, Frances, Vice President, Business Development and Marketing, Webwasher ..... 25
Schwarz, John, CEO, Reciprocal ..... 32
Wallent, Michael, Product Unit Manager, Internet Explorer, Microsoft Corporation ..... 18

# INFORMATION PRIVACY: INDUSTRY BEST PRACTICES AND TECHNOLOGICAL SOLUTIONS

---

**THURSDAY, JUNE 21, 2001**

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

The subcommittee met, pursuant to notice, at 10 a.m., in room 2123, Rayburn House Office Building, Hon. Cliff Stearns (chairman) presiding.

Members present: Representatives Stearns, Deal, Shimkus, Bryant, Bono, Terry, Bass, Tauzin (ex officio), Towns, DeGette, Doyle, Harman, Markey, and Eshoo.

Staff present: Ramsen Betfarhad, majority counsel; Mike O'Rielly, majority professional staff; Brendan Williams, legislative clerk; and Bruce M. Gwinn, minority counsel.

Mr. STEARNS. Good morning. The Subcommittee on Commerce, Trade, and Consumer Protection will come to order.

I wish, of course, to thank all of those in attendance, especially our distinguished witnesses. Welcome to the subcommittee's hearing. We entitled it "Information Privacy: Industry Best Practices and Technological Solutions." It could also be entitled "Software Solutions and Self-Determination."

This hearing is the fifth in a six-part series of hearings examining information privacy. The series is scheduled to conclude next month. My colleagues, I am confident that this morning's hearing, as with the four preceding it, will add to an already rich record on the issues of information privacy.

The record developed by this subcommittee on information privacy is the most comprehensive in Congress and enjoys both an impressive range and depth. I invite all members to review the record before formulating their thoughts and positions on the issue of information privacy.

Today's hearing adds a new and important dimension to the existing record—private sector response to privacy concerns. That response engenders two components—technological solutions and voluntary industry information privacy standards. I am particularly pleased that this morning we will witness the demonstration of just a handful of technological solutions that are now available to the American consumer.

In my view, these solutions designed to reach information privacy concerns of the consumer are a critical ingredient of whatever is a recipe to the final solution of our problem. Technological solutions are such a critical ingredient for three reasons among many.

First, nothing offers a consumer greater control over his information privacy destiny than technology. Using some of the filtering software being demonstrated today, I, as an internet user, can determine how much personal information I want to share and for what purpose.

For example, I can determine to accept a "good cookie," one that makes surfing a website seamless and efficient, as easily as I can decide to reject a "bad cookie," one designed to track my online movements for purposes I don't care for.

The second reason why technology is a critical part of any response to information privacy concerns is the fact that technology responds to change much faster and with greater responsiveness and precision to the new and continually evolving privacy concerns than any other way of addressing information privacy concerns.

Innovation and technological change has, and continues to be, a hallmark of the American experience and its culture. Technology has helped us combat many ills of society, albeit not by itself. Moreover, solutions to privacy concerns have the advantage of precision, not too dissimilar to laser surgery. A tech solution can remove the bad cells with minimal, if any, damage to the good cells surrounding the bad.

Finally, the incentive for the creation and constant improvement upon technological tools, getting at consumers' information privacy concern, is a great one. It is the mighty dollar. When there is a consumer concern such as privacy, a marketplace is created. Where there is a market, there are dollars to be made. Where there are dollars for whatever reason, there is creativity, innovation, speed, and efficiency.

The second component of the private sector response to the American consumers' information privacy concerns is the adoption of self-regulatory measures. Today's witnesses will highlight a number of voluntary self-regulatory programs adopted by direct marketers, online advertisers, and retailers.

Moreover, we will hear about a new field in "assurance services," privacy assurance. No one is under the illusion that altruism has brought about this movement in self-regulation. After all, substantial costs are associated with the deployment, implementation, and adherence to these self-regulatory standards governing consumer information privacy practices.

Rather, it seems that many, if not the majority, of companies dealing with individual consumers have reached the conclusion that being responsive to their customers' information privacy concerns is simply "good business." Now, how successful have they been? I don't know.

What I do know is that some companies have chosen to use their privacy policies as a means of gaining a competitive advantage vis-a-vis their competitors. Such competition ultimately empowers a consumer to vote with his dollars as to what are his or her information preferences.

In my many years of public service, I have yet to find an important complex public policy concern that has lended itself to a panacea quick-like solution. Information privacy concerns are no exception. Private sector solutions, such as technology and self-regulatory practice, however, do go a long way toward mitigating those concerns.

So I look forward to our witnesses' testimony, and we are just delighted to have them. And I will offer the ranking member, the distinguished member from New York, Mr. Towns, an opening statement.

[The prepared statement of Hon. Cliff Stearns follows:]

PREPARED STATEMENT OF HON. CLIFFORD STEARNS, CHAIRMAN, SUBCOMMITTEE ON COMMERCE, TRADE, AND CONSUMER PROTECTION

Good morning. I wish to thank all in attendance, especially our distinguished witnesses. Welcome to Commerce, Trade, and Consumer Protection subcommittee's hearing entitled, Information Privacy: Industry Best Practices and Technological Solutions. This hearing is the fifth in six part series of hearings examining information privacy. The series is scheduled to conclude next month. I am confident that this morning's hearing, as with the four preceding it, will add to an already rich record on the issue of information privacy. The record developed by this subcommittee on information privacy is the most comprehensive in Congress and enjoys both an impressive range and depth. I invite all members to review the record before formulating their thoughts and positions on the issue of information privacy.

Today's hearing adds a new and important dimension to the existing record: private sector response to privacy concerns. That response engenders two components: technological solutions and voluntary industry information privacy standards. I am particularly pleased that this morning we will witness the demonstration of just a handful of the technological solutions now available to the American consumer. In my view, technological solutions designed to reach information privacy concerns of the consumer are a critical ingredient of whatever is the recipe to the solution for the problem.

Technological solutions are such a critical ingredient for three reasons, among many. First, nothing offers a consumer greater control over his "information privacy destiny" than technology. Using some of the filtering software being demonstrated today, I, as an Internet user, can determine how much personal information I wish to share and for what purpose. For example, I can determine to accept a "good cookie—one that makes surfing a website seamless and efficient—as easily as I can decide to reject a 'bad cookie'" one designed to track my online movement for a purpose I don't care for. The second reason why technology is a critical part of any response to information privacy concerns is the fact that it responds to change much faster and with greater responsiveness and precision to the new and continually evolving privacy concerns than any other way of addressing information privacy concerns. Innovation and technological change has and continues to be a hallmark of the American experience. Technology has helped us combat many ills of society, albeit not by itself. Moreover, technological solutions to privacy concerns have the advantage of precision. Not to dissimilar to laser surgery, a tech solution can remove the bad cells with minimal, if any damage, to the good cells surrounding the bad. Finally, the incentive for the creation and constant improvement upon technological tools getting at consumer's information privacy concerns is a great one. It is the mighty dollar. When there is a consumer concern such as privacy, a market place is created. Where there is a market, there are dollars to be made. Where there are dollars, for whatever reason, there is creativity, innovation, speed and efficiency.

The second component of the private sector response to the American consumer's information privacy concerns is the adoption of self-regulatory measures. Today's witnesses will highlight a number of voluntary self-regulatory programs adopted by direct marketers, online advertisers and retailers. Moreover, we'll hear about a new field in "assurance services," privacy assurance. No one is under the illusion that altruism has brought about this movement in self-regulation. After all, substantial costs are associated with the deployment, implementation and adherence to those self-regulatory standards governing customer information privacy practices. Rather, it seems that many, if not the majority, of companies dealing with individual consumers have reached the conclusion that being responsive to their customers information privacy concerns is simply good business. Now, how successful they have

been, I don't know. What I do know is that some companies have chosen to use their privacy policies as a means of gaining a competitive advantage vis-à-vis their competitors. Such competition, ultimately empowers the consumer to vote with his feet and/or dollars as to what are his or her information privacy preferences.

In my many years of public service, I have yet to find an important and complex public policy concern that has lent itself to a panacea like solution. Information privacy concerns are no exception. Private sector solutions such as technology and self-regulatory practices, however, do go a long way towards mitigating those concerns.

Thank you. I look forward to the testimony.

Mr. TOWNS. Thank you very much, Mr. Chairman. I have a prepared opening statement, but I would like to just put it in the record and just make a couple of comments.

Mr. STEARNS. Without objection, so ordered.

Mr. TOWNS. First of all, let me commend you, Mr. Chairman, for the way you are handling this situation. The fact that you are moving very slowly, you are listening, you are talking to a lot of people before moving forward. I think that is really the smart way to do it, and I want to commend you for that.

I also want to say that some people are saying that we should just leave this alone and it will sort of work itself out. But the consumers are out there saying, "We want to be protected." And I think that we need to take a very careful look and try to find out ways and methods that we can protect them.

And I feel very comfortable, Mr. Chairman, in the way you—again, the way you are moving, because, you know, we need to talk to people, we need to listen, and we need to visit. And I have been trying to visit as many companies as I possibly can, of course, in the New York area to talk to them to get their input in terms of how we should handle this situation.

I don't want us to make the mistake that Thomas Jefferson made. Thomas Jefferson read a pamphlet on how to swim and jumped in the water and almost drown—you know, kicking his leg and pulling his arm, and all of that. So I don't want to be guilty of that. I think that we need to make certain that we talk to people that are out there in the field on a day-to-day basis, in terms of—and involved in this issue.

And I think that if we do that, then I think that at the end of the day we can come up with something that will not put a whole lot of folks out of business, but at the same time be able to protect the consumer as well.

So I wanted to say to you, I salute you on that, and I am anxious and eager to hear from the witnesses because I think this is something that we must deal with eventually. No question about it. And on that note, I yield back.

[The prepared statement of Hon. Ed Towns follows:]

PREPARED STATEMENT OF HON. ED TOWNS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEW YORK

Mr. Chairman, thank you for holding this educational hearing on information privacy. I would also like to join you in welcoming the members of both panels assembled here today. I would especially like to welcome my friend, John Schwarz, the CEO of Reciprocal, which is located in New York's Silicon Alley. John has a great product to display for us today and I look forward to hearing from him as well as all the witnesses.

Mr. Chairman, I must say that I am heartened by the technologies assembled here today that will allow consumers more control over their personal identifiable information. I am particularly pleased with Microsoft including the Platform for Privacy Preferences or (P3P) into their latest edition of Internet Explorer. After seeing

a demonstration of this new technology integrated with the new Microsoft Operating System, I feel that consumers are going to be empowered like never before to not only further protect themselves but to further educate themselves on protecting their privacy, which is of the utmost importance.

I do not commend the P3P technology because it is an end all-be-all for privacy protection, but rather because Microsoft is truly the first company to offer a pragmatic solution which grants more power to the consumer while they surf the Internet.

The other technology that I want to bring to my colleagues' attention is that which is being used by Reciprocal. Reciprocal is a company, which currently protects Intellectual Property on the Internet by encrypting the content when it is purchased online. While Mr. Schwarz will explain this more in depth during his testimony, his technology *can be* and in the near future I believe *should be* used to help protect medical as well as financial records, in addition to other personal information belonging to consumers.

Companies need to feel that their efforts will not go unrewarded. Many of my colleagues are bent on legislating Internet privacy. While I would agree that minimum standards are needed, why limit an industry that continually awes consumers with each new product developed? Let's not put restrictions on the Internet or on the technology that is bettering our constituents' lives.

I look forward to hearing the testimony from our witnesses and yield back the balance of my time.

Mr. STEARNS. I thank the gentleman.

The gentleman from Illinois, Mr. Shimkus?

Mr. SHIMKUS. Thank you, Mr. Chairman. And I will be brief; we have two large panels. And I apologize for having to leave. Our State delegation is meeting on appropriation issues, and I get to chair that meeting at 11.

But I want to thank you for holding this hearing. I look forward to the demonstrations that I am going to be able to observe. We will have staff present.

Also, I am interested in hearing how the businesses depend on sharing personal information and their views of new privacy tools. We all know that our citizens want privacy protection. We also know that our citizens want to accrue all of the benefits of information sharing.

The question is: are these two issues mutually exclusive? Hopefully you will inform us that what is—what the consumers want is the best, and you are helping provide the technology through the business model to solve those issues. I hope you can answer those questions, and we look forward to hearing from you.

I yield back my time, Mr. Chairman. Thank you.

Mr. STEARNS. I thank the gentleman.

The gentlelady from California, Ms. Eshoo?

Ms. ESHOO. Thank you, Mr. Chairman. Good morning to you, and welcome to the witnesses. We are grateful to you for coming to Washington to enlighten us.

Today's hearing can provide very important information I think for all of the members of the subcommittee for our discussion on the need for privacy legislation. By examining some of the existing technological solutions and business practices, I think that we can learn and understand better and be able to gauge the type of legislation that the issue calls for.

I have introduced a bill, along with Congressman Chris Cannon from Utah, that achieves—at least we think it achieves a balance between the protection of online consumers and continued promotion of technological innovation relative to the evolution of e-commerce.

We want to be able to encourage the growth of the internet and e-commerce, and I think that the bill strikes that balance. It does this by establishing some basic minimum standards in the form of notice and choice, and at the same time leaving room for the industry to continue to develop its own privacy protection technologies, some of which we are going to see today.

We have to get this right legislatively. I think if there is anything that is built into legislation that allows for the unintended consequences that could happen we can really hurt what we are really attempting to grow. So I am very mindful of that, and I think anything that we do that—in haste, that we could live to regret it legislatively.

We know that all of our constituents feel very strongly about privacy. I think that privacy runs through the veins of the American people. We have always had a resistance and a suspicion of Big Brother, and I think that there are people out there today that have a sense that they are suspicious or afraid of Big Browser.

So we not only can collect information, it can be sold, it can be shared. There are some blessings to that, but there is a down side to it as well. So I think that today's hearing can go a long ways with the subcommittee so that we can then tell our colleagues about what technologies can do, but I also think that it will help build a foundation for legislation in the 107th Congress to provide the privacy that the American people feel so strongly about and insist upon justifiably.

So I look forward to hearing from the witnesses, and thank you, Mr. Chairman, for having this important hearing.

Mr. STEARNS. I thank the gentlelady.

My colleague from New Hampshire, Mr. Bass, is recognized.

Mr. BASS. Thank you very much, Mr. Chairman. And, again, I repeat, I appreciate these series of hearings. They have been tremendously informative for me as a newer member of the committee and my first exposure to what is an exceedingly complex and difficult issue.

I understand that before the Congress moves forward with any kind of government solution—if you want to give it a generic definition—we need to fully understand the scope of the problem, the players involved, and what reasonable role government can play, balancing the need to maintain a strong and vital economy on the internet, while at the same time protecting the rights of individuals.

I was, unfortunately, not able to come to the hearing that was held yesterday on—or Tuesday, rather, on Ford v. Firestone, because I was holding a cyber security/privacy conference of my own in my district, in which a number of individuals, some of whom are in the same business that you folks are in, and others that are—that run concerns that have a significant cyber exposure, to try to—we met to listen to speakers who made presentations to try to make sure that we understand, at least in my district, which is a very high-tech-oriented district, what the problems are and what the potential solutions are.

And without getting into some of the conclusions that were drawn by this conference that I had, suffice it to say that this hearing dovetails very well with the subject matter that I am personally

concerned with and that is the concern of a significant constituency in New Hampshire.

So thank you, Mr. Chairman, and I will yield back to you.

Mr. STEARNS. The gentleman yields back.

The gentleman from Massachusetts, the ranking member of the Telecommunications Subcommittee, Mr. Markey?

Mr. MARKEY. Thank you, Mr. Chairman, very much. And we welcome all of you best practices people, and, you know, congratulations. We are going to give you each gold stars on your forehead today for your excellent work. And you are going to actually set a standard for this committee as to what we can expect everyone else in the industry to do.

Obviously, we're not going to pass any laws that will punish you, because you all do good work. But because you know better than we do how many really bad people are out there online, which is why all of your technologies are necessary, we are going to have to pass laws to protect the public against them. But you don't have to worry because you all are meeting the standards for protection of the public.

That is the good news about your testimony today, that this technology is there, that public privacy can be protected, that it is not hard for the industry to do this. That is the good news, that you have the strongest case that can be made to pass legislation, that we need legislation, that we have to give everyone the minimal rights to be able to protect their information.

After all, we have done it before. You know, people's tax returns are protected, their cell phone records, their telephone records, their cable records. None of this is publicly available. None of it can be disseminated without the express permission of the individual.

We were doing that in an analog world. Now that we have you digital geniuses here to help us to explain—there are some people, believe it or not, who will tell us you can't do it in a digital world, even though they did it in an analog world. You know, how foolish, how anti-technology, huh? How antediluvian they all are. Because we all know that we have moved, actually, from the world of Big Brother to Big Browser.

The real threat now is less what the government can do to you, but what corporate America can do to you, as these corporate data-mining giants seek to combine every piece of information about you so that they actually wind up knowing more about yourself than you do or any other member of your family.

Now, we should give every American, obviously, the right to protect against that kind of invasion, because that is—that is the central right that every American has. That is what distinguishes us from the rest of the world.

And it is sad to think that the Europeans are ahead of us in granting these kinds of rights, because we have—that is why we fled all of these nice, European countries, most of us in this room, our grandparents, because we weren't given these rights to protect our religion, to protect our ethnic background, to protect our privacy, from what the king—from what these despots might try to do to us. So we thank you for illustrating how this is possible.

And I think, Mr. Chairman, in conclusion, we need three levels of protection. One, we need for every American to have the right

to access to these technologies—P3P, any other technology that can wall out any of this information. We need individuals to themselves try to protect themselves.

But at the third level, you have to realize that there are still going to be corporate or individual attempts to intrude upon our privacy. And as a result, there has to be a minimal floor of privacy that every American is entitled to, legally and enforceably.

And only at the point at which all three components are in place simultaneously will there be a set of privacy protections which can protect the public. But I want to thank all of you, because there are many people, by the way, who don't want to testify here today, who will contend that what you are saying is really impossible, too difficult, can't do it, technologically impossible to protect privacy, too complicated for industry.

Even as industry says, "We can move your information from here to Kuala Lampur in the blink of an eye. And isn't it great, this information age?" And then when you say, "Oh, by the way, can you just let me check off someplace where I don't want it disclosed," they go, oh, the horror, the technological complexity of adding that one extra little box. I don't know how we are going to do it. It is a little bit—I will just conclude on this.

It is a little bit like this hearing that we had last week where, you know, you have got the Energy Department here saying, "Yes, it is possible to deploy a Star Wars technology that can be deployed in outer space with nuclear powerplants in outer space, and lasers and beams and coordinated on the ground, and knock down every Chinese and Russian missile in under a minute and a half."

And we can do this all in the next 4 years, and actually we don't even need the anti-ballistic missile treaty, and we can abrogate our relationships with just about every other country in the world, and we know it is technologically possible.

And then you say to them, "Well, can we improve the efficiency of air conditioners?"

And they go, oh, the horror. The horror of trying to improve air conditioners so that we can deal with the electricity crisis. Okay?

So you are proof positive of something that is working in the marketplace that—complemented with a legal minimal set of enforceable protections that every American can sleep at night knowing that if somebody tries to do something to them that there will be a way in which the law can protect them.

Thank you, Mr. Chairman.

Mr. STEARNS. Thank you.

The gentleman from Nebraska, Mr. Terry, is recognized for an opening statement.

Mr. TERRY. Thank you. I appreciate your holding this hearing. Welcome to all of our witnesses, and I yield back.

Mr. STEARNS. The gentleman yields back.

The gentlelady from Colorado, Ms. DeGette?

Ms. DEGETTE. Thank you, Mr. Chairman, for holding yet another informative hearing on a topic none of us ever tire of—privacy.

While I am always loathe to follow Mr. Markey, I still want to add a few words, although I am sure not as glibly as Mr. Markey often does.

Not too long ago, if an online business had a privacy policy, they were probably way ahead of the eight ball, regardless of what the privacy policy actually said. Now having a privacy policy is not so important as what that policy actually is. And, increasingly, consumers seem to know that.

During earlier hearings in this series on privacy, I remarked that I see privacy as an issue that can be used to great advantage by industry, if it realizes how important the issue is to consumers. And we all know poll after poll shows that personal privacy continues to be one of the top concerns of individuals ranking right up there with health care and social security. And in the technological age, privacy is an increasing concern of consumers.

If businesses, like those today will testify, institute straightforward and effective privacy policies, I think customers will beat a path to their door. And there are a lot of examples how this is already happening.

We need to address both the perceived and real fears people have with respect to privacy, though, particularly in this electronic age.

And I think this bears repeating today because the best technology and privacy policies in the world won't do much to further consumer protections if the consumer doesn't realize what is aware to him or her, or if they don't understand the vagaries of the particular technologies or policies they are dealing with.

From a business perspective, a lot of time and money can be invested in implementing a certain technology. And if the customers can't figure it out, or if the customers don't even know about the existence of the policy, then the business won't reap the benefits.

One of the programs that I read about in the testimony for today is the AICPA web trust program for online privacy. I recently talked about this program with some of my constituents who are members of the Colorado Association of CPAs, and they told me that when this program was first getting off the ground their members did not want to implement the system.

They thought it was a hassle. They thought it was expensive, and so on. Many of the CPAs still have not put the system into place, but those who have done so found they were more than earning back their investment because of the increased business that came their way because of higher levels of consumer confidence in the business.

So I think it is both the responsibility of business and a smart economic decision to make sure their privacy policies are fully accessible to their customers. The trick will be, as Mr. Markey pointed out, what do we do about the businesses who don't understand that this is both the right thing to do for consumers and also the economically prudent thing to do for their own business? And how do we protect consumers?

It is an ongoing discussion that we will have. There is no magic bullet, because of advances of technology. And I look forward to hearing from our witnesses and hearing some of the new advances, and I am happy to yield back, Mr. Chairman.

Mr. STEARNS. I thank the very distinguished colleague.

The gentleman from Tennessee, Mr. Bryant, is recognized for an opening statement.

Mr. BRYANT. Thank you, Mr. Chairman. I, too, look forward to hearing from our witnesses today as we continue our look into the issue of information privacy.

It is good to see the private sector respond to the concerns of so many—that so many people have about the internet, and this hearing is a great opportunity for us to learn more about the technologies developed and how it provides consumers with the protection that they want.

In previous hearings, I have learned that each user has a different opinion of what a violation of a person's privacy entails. It is good to know that technology such as Webwasher, Zero-Knowledge, P3P, and Microsoft Internet Explorer have been developed so each user can choose what kind of protection she wants when using the internet.

I am particularly glad that the Better Business Bureau has taken the initiative as a third party to verify the security of various websites. I am also looking forward to hearing from the Direct Marketers Association and the National Advertisers Initiative, so that we can learn more about the efforts used by each to ensure that online advertisers don't overstep their bounds.

Internet users like to be aware of instances when their information is going to be shared, and I think most would like to have that option of opting out.

I also hope that today's hearing can serve effectively as a public forum to inform Americans about technologies, software, and assurances out there, which a person can utilize to prevent information about themselves and their internet habits from being known by parties without knowledge or permission of that user.

I also hope that this hearing will provide people with information so that a user can have more confidence in the security of internet.

With this, I would close my statement and thank the members of this panel for coming here today. Thank you.

Mr. STEARNS. I thank my colleague.

Mr. Doyle, Pennsylvania, is recognized for an opening statement.

Mr. DOYLE. Thank you, Mr. Chairman.

Good morning and welcome to all our invited guests and witnesses. I am looking forward to hearing what you as industry experts have to tell us regarding the viability and approach that your companies have employed to make electronic transactions via the internet more secure.

Many of my colleagues on this subcommittee are well aware that today's hearing is the fifth in a series that the Chairman has called to examine various aspects of internet privacy debate. Without a doubt, the majority of American consumers are concerned about the security of their personally identifiable information that can be gathered while online.

This subcommittee has heard testimony from previous witnesses who have conducted numerous surveys of online customers that speak to this fact. Additionally, we are here today to listen to the technological solutions and approaches various companies have developed or are in the process of developing to meet the privacy needs of online consumers.

Companies would not be developing and marketing these services if a market demand for such goods did not exist. The issue of con-

trolling the information that is gathered about consumers while online and how to go about limiting the distribution of this information is a fundamental consumer protection issue.

We have a significant challenge and a good deal of discussion ahead of us before we reach a conclusion as to the best way to ensure that personal information is protected online while not stifling the continued growth of e-commerce in America. Today we revisit the issue of proper industry self-regulation this subcommittee raised in another previous hearing, and hopefully we will see some definitive solutions to privacy protection.

I find it encouraging that the industry is responding to the challenges presented by internet privacy and is developing and implementing security software or protocols to address these concerns. It has been said that there is a buck to be made with the development of such services. After all, innovation and creative industry response to consumer needs has long formed the backbone of commerce in this country.

I am concerned that although privacy protection companies may prevent direct third-party access to personally identifiable information, the privacy protection software itself could be used to gather information which might be shared with affiliated third party companies.

I am quite sure that the representatives of the companies here today would never employ such tactics and are making great strides to combat this abuse. But without a basic framework of standards and regulations, other less responsible entities could exploit public trust for financial gain.

Mr. Chairman, I look forward to hearing about the software and the practices that our esteemed guests have developed to ensure that this scenario does not become a reality.

I thank you, and I yield back.

Mr. STEARNS. I thank my colleague.

And now we recognize for an opening statement the distinguished Chairman of the full committee, the gentleman from Louisiana, Mr. Tauzin.

Chairman TAUZIN. Thank you, Mr. Chairman.

As the committee knows, this committee requested that Chairman Stearns conduct a thorough review and educational process on the issue of privacy. And, Mr. Chairman, I want to compliment you on the fact that I think you have already outdone your assignment.

This has been an extraordinarily instructive series of hearings, and I think it is going to help our full committee at some point make some very good and wise decisions regarding privacy, not only online but for the general sake of the American public. And I thank you for this hearing today.

Today, as you know, we focus on two very important aspects of the question. In the privacy conference this committee conducted last year with the Chamber of Commerce, we first-hand saw and learned about some of the new technological developments of new equipment and software that, in fact, enable consumers to protect themselves online in various and in sundry ways.

And we have also learned that over the last year there have been a myriad of new products coming on board and new technologies

being developed. We will learn more about that today, and I thank you for arranging that, Cliff.

Second, we will learn a lot more about the practices in the self-regulatory regimes that exist in the marketplace by which the industry and its players are attempting to do what a good marketplace always does, and that is give consumers something they want.

And we know that consumers do want an assurance that privacy concerns are being addressed by the companies they deal with, and the people they will deal with online, and that these privacy concerns are taken seriously enough that consumers have some confidence in both the security of their transactions and the respect that will be given to information that consumers would rather not be used in ways that they would not approve of.

And so we will learn a lot today about the practices within the industry. Mr. Chairman, in your last hearing we learned why consumers have reason to be concerned, and that there are, in fact, some bad practices in the marketplace. We have learned recently, even worse, that Federal websites are filled with cookies, websites where consumers don't necessarily volunteer information but in many cases are obliged to give information to a Federal agency.

So we have got some real work to do in both the publicly owned websites of America and the Federal agencies and their relation to their consumers and to the consumers who enter the commercial online world and want and expect some degree of security and privacy in their transactions.

This will be a very illuminating hearing because it will help us understand what is, in fact, occurring out there, particularly over the last year, that will give consumers more and more control over this sensitive issue in their lives.

I also want to point out that while privacy concerns are not limited to online transactions, this exercise today will again give us more insight as to some of the broader issues of privacy concerns in the marketplace. And, again, I thank you for that.

Finally, I want to address one issue that has received a little attention lately, and that's the changes that have occurred in the other body, and as they affect the issue of privacy and legislating on privacy.

Let me assure all of you that the subcommittee chairman and I are committed to a very thoughtful, a very careful, and professional review of these privacy concerns, and that changes in the other body are nothing more than that—changes in the other body.

We intend to keep our course, and we intend to proceed very carefully in this area because we understand how delicately the information age depends upon a very careful cut between restricting information for the cause of protecting privacy and permitting the free flow of information for the sake of an information age that depends upon information.

We are going to proceed very carefully because our rule is to do no harm and to facilitate and to actually encourage the development of things we are going to learn about more today—self-regulatory practices, self-regulatory regimes, enforcement regimes, and technologies that empower consumers in this marketplace.

Thank you very much, Mr. Chairman.

[The prepared statement of Hon. W.J. "Billy" Tauzin follows:]

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

Thank you, Mr. Chairman, for holding this hearing. This is another step in the education process on this important public policy issue. You have certainly outdone yourself in an effort to provide the Subcommittee with a full background on the subject of privacy.

Today's hearing focuses on two important pro-active steps organizations are taking at their own initiative to help improve consumer privacy: developing technological privacy solutions and creating positive private sector practices and/or enforcement regimes. For a number of reasons, some valid and some invalid, current information exchange practices have generated increased concern by consumers about their ability to maintain their personal privacy. From the last hearing on privacy, we learned that consumer confidence is somewhat shaken by the privacy practices of some companies. Today, we get to look at what is being done about this.

With every problem, however, there is a corresponding opportunity. As with most things in the free market, someone is going to find a way to take advantage of this opportunity. The creative and innovative nature of technology is starting to take root to fill in the gap between the privacy protections consumers want and the information gathering and exchange that some companies practice. Specifically, some entrepreneurs and technology companies are developing products designed to further protect consumer privacy. Software and hardware solutions are sprouting-up in the marketplace to deal with consumer privacy interests. These solutions come in many forms with differing options and costs. From filtering products, to anonymous web-surfing, to browser notifications and standards, technology is just starting to enter this field. And this is just the tip of the iceberg. I expect many new technologies to be created to address this issue and meet consumer demand for privacy protections.

In addition, many American companies, recognizing it is in their best interest to address consumer concerns, have already taken steps to improve their privacy practices or provide necessary assurances to consumers of their practices. In other words, many companies want to promote consumer confidence by giving them what they want—better privacy.

Self-imposed privacy enforcement and assurance regimes have been created to promote company use of positive privacy practices—or industry "best practices." These regimes also come in many different forms and may target specific sectors of industry. Today, we will hear from a number of representatives about the steps they are taking, the companies they represent or oversee, the processes they use to approve and enforce their privacy practices, and more.

I think one important message to take from this hearing is the great work that is being done by the private sector to promote consumer confidence as it pertains to privacy. I appreciate the work of those companies that are developing technology and those organizations keeping privacy practices in line with consumer wishes.

I think the Committee can gain a valuable education by actually trying to use and implement the technology that is out there. And so, I will be asking the relevant interested parties, especially those not able to testify today, to work with us over the next few months to show us how your technology or industry best practice would work as they apply to this Committee's website. I recognize that the privacy debate is more than just what is happening online, but this should be a useful exercise. In a voluntary way, I am hopeful that we can explore the differing programs, including the seal and assurance programs, to learn how they work. We also need to learn more about which technologies the Committee could implement to ensure citizens feel comfortable with the Committee's privacy practices. In other words, show us first-hand what you have and what it really does.

Lastly, let me address one issue that has received added attention recently because of the changed perspective of the Other Body towards privacy. Let me assure everyone that the Subcommittee Chair and I are committed to a well thought-out, deliberate, rational process as it pertains to privacy and any potential fixes. The changes in the Other Body and its impact on privacy are just that—changes in the Other Body. We will continue along our own path.

I again thank the Subcommittee chair for holding this hearing and look forward to the testimony of the witnesses.

Mr. STEARNS. I thank the distinguished chairman.

We will now go to panel No. 1. Before I start, I would introduce or indicate to my colleagues that Mother Nature has prevented one

of our witnesses from attending. Mr. Austin Hill of Zero-Knowledge was unable to get a flight from Montreal to Washington last night because of electrical storms. Mr. Hill asked that his testimony be made part of the record in his absence. And without objection, it will be so ordered.

[The prepared statement of Austin Hill follows:]

PREPARED STATEMENT OF AUSTIN HILL, CO-FOUNDER, EXECUTIVE VICE PRESIDENT, AND CHIEF STRATEGY OFFICER, ZERO-KNOWLEDGE SYSTEMS, INC.

Thank you, Mr. Chairman and members of the committee. I applaud the Subcommittee's leadership in addressing privacy issues, and appreciate the opportunity to talk today about the role technology solutions play in maintaining information privacy in our global information society.

My name is Austin Hill, and I am the co-founder, executive vice-president, and chief strategy officer for Zero-Knowledge Systems. Zero-Knowledge is a provider of privacy-enabling technologies and services. We employ 175 people and are headquartered in Montreal, Canada with offices in Redwood City, California. Zero-Knowledge is the oldest and largest privacy technology and services company. We employ many of the world's leading privacy policy and cryptography experts, and have been working since 1997 on technological ways to prevent the erosion of privacy in the information society.[1]

As both a privacy advocate and entrepreneur, I will outline the factors creating our society's major privacy challenges, and detail where we have the technological tools to manage and secure information privacy.

INFORMATION PRIVACY: AN ENTREPRENEUR'S PERSPECTIVE

Four years ago, after successfully creating Canada's third largest ISP, my partners and I started thinking about Internet privacy. We saw studies showing that privacy was a growing concern for consumers and immediately recognized its importance to an emerging e-business sector.

Much of our inspiration was based upon the idea that technology will be everywhere: multiple networked devices, wireless location services, intelligent homes, and ubiquitous networks. We believed that if we, as a society, did not come to terms with how to safeguard people's personal information, the technologies that would soon become so pervasive would erode individual privacy. We also recognized that if information privacy was not addressed in a way that offered customer preference and choice while enabling businesses to build trusted relationships with consumers, all of the coming advancements in technology would not reach their full potential.

As a person who places a high value on individual privacy, I was deeply concerned. Yet, I also saw an incredible opportunity for privacy-enabling products and services. So, in 1997 my partners and I created Zero-Knowledge Systems to be the company that provides the solutions to ensure information privacy in our society.

At Zero-Knowledge we have long held the view that good privacy is good for business, and the more we talk with our customers at some of the world's leading companies, the more we see that industry leaders share this view.

The Gartner Group articulated it well in a recent report, saying: "The widespread adoption of the Internet and the web has shifted cultural attitudes toward privacy. Heightened privacy sensitivity will require online and offline businesses to re-examine existing information practices. Through 2006 information privacy will be the greatest inhibitor for consumer-based e-business."[2]

We are at the beginning of the information technology revolution and it is clear that privacy has emerged as both a major challenge and opportunity. Now is the time to build privacy into business, and the new products and services being deployed every day. On the positive side, businesses and policy-makers such as yourselves have recognized the problem and are actively looking for solutions. I firmly believe that Zero-Knowledge and other companies are well positioned to provide these solutions.

When examining what we need to address to provide the tools to assure information privacy, one must look at the information itself. How well an enterprise manages its personal information assets will determine the success or failure of critical e-business initiatives. A core business asset, personal information carries with it many challenges and opportunities.

---

[1] See http://www.zeroknowledge.com for more information.

[2] Please visit http://www.gartner.com

One must recognize the information explosion our society is in the midst of. UC Berkeley's School of Information Management and Systems stated that "(m)ore information will be created in the next 3 years than in the last 40,000 years." Between 1980 and 2000 we created 10 million terabytes of data. This includes music, books, credit, medical and personal records and other common data types. From 2000 to 2003 we will create 40 million terabytes of data.[3]

This is a truly astounding statistic. It becomes even more important to today's discussion when two more factors are taken into account.

The first is to again realize that the trend for technology is toward pervasive devices and ubiquitous networks. Everything from your car to your home and phone will talk to each other and share data. The combination of the two technological trends of information explosion and pervasive computing suggests that personal information will now need to stored and transferred in a variety of new manners. Information will not simply reside on a home PC, or a PDA, but will be stored on a variety of networks, and with a variety of different organizations. This data will then be shared via the fixed Internet, the mobile Internet, and emerging personal area networks such as Bluetooth and wireless 802.11 connections.

The second factor, and most relevant to your topic today, is that of all of this data the overwhelming majority of it will be personal information. Some estimates hold that over 80% of it will be personal information, including medical records, insurance records, educational records, personal communications, credit history, photos and home video, and government records.[4]

Zero-Knowledge believes that there are two classes of privacy-enabling products necessary to fully address information privacy in a climate such as this: (1) consumer-side privacy protection tools; and (2) corporate-side Privacy Rights Management technologies.

Examples of privacy protection tools include products such as anti-virus programs, firewalls, and encryption tools. The goal of privacy protection technologies is to stop people from invading your privacy. These types of tools place the burden of use on the consumer, but also empower them to take control over and protect their privacy. We will always have private data that only we as individuals can protect and so it is essential for there to be privacy protection tools available to consumers.

Zero-Knowledge has created the Freedom Internet Privacy Suite to empower Internet users to secure and protect their privacy when online. Its standard features include a firewall, ad manager, form filler, word scanner, and cookie manager. These features combine to enable an Internet user to control how and when their personal information is released, and to protect their PC from malicious hackers. We also offer Freedom's Premium Services, which add the industry's most robust private encrypted email and private browsing to the suite. These two services utilize the global Zero-Knowledge Network of servers that re-route and privatize the traffic of Freedom users.

Other privacy protection solutions are available to consumers and two of them are here to testify today, WebWasher and Microsoft with its P3P-enabled browser. Technologies such as these are essential to ensure that consumers have the tools necessary to protect their privacy.

The second class of privacy solutions I referred to, Privacy Rights Management (PRM) technologies, represent an essential framework for building information privacy into the enterprise.

In the information society, I must trust various organizations, businesses or individuals such as my doctor with my personal information. Hence, there is a requirement for those parties to be responsible and accountable for how they manage my data. Today, no tools exist for a business or organization to demonstrably protect and manage the personal information it has collected about its valued customers and employees.

Businesses must adhere to a complex and constantly emerging global framework of privacy regulations and have begun hiring Chief Privacy Officers (CPO) and other data protection officers to help with the task. I have spoken with many of these new CPOs at Fortune 500 companies and they all articulate the same concern: they don't have the tools to do their job. Imagine a Chief Financial Officer attempting to do her job without tools such as Enterprise Resource Planning software or even spreadsheets. It would be close to impossible. Unfortunately, that's exactly the position that every CPO is in today. There is, quite simply, a lack of tools for the job. This is where PRM technologies will be applied. The core idea behind PRM is that the enterprise needs a policy-based framework for data management and protection if

[3] Please visit http//www.sims.Berkeley.edu
[4] EMC, the leading data storage company, http://www.emc.com

it is to comply with regulations, mitigate risk, support customer preferences and build consumer trust.

There are several companies developing solutions that fit in the Privacy Rights Management framework. These include IBM, Novell, and Tivoli. PRM is an emerging category of enterprise software that will help close the current gap between stated policies, customer preferences and operational realities.

Privacy Rights Management: Software Solutions for the Global Enterprise

The proliferation of data systems in both the public and private sectors that handle sensitive personal information such as health/medical records, financial/credit records, and location-based profiles demand that proper controls be put in place to ensure this data does not fall into the wrong hands and is not subject to misuse. It is of great value for a business to have these controls in place in order to mitigate risk, reduce the cost of compliance and build consumer trust.

A comment I often hear from CPOs at major corporations is that they have no idea what personal information assets are present at their company, who has access to them and how the data is being used. As a case study, imagine a global corporation with operations in disparate countries and several divisions. As an incoming CPO you will need to first discover all of the personal information present throughout the organization. You will need to know who controls each repository of personal information, which people are allowed to access what information and in what cases this information is combined with other data resources.

Once that information is gathered you will have to assess which regulations apply to what kinds of data. For example, a Customer Relationship Management database located in Canada will be subject to the recently enacted Personal Information Privacy and Electronic Documents Act. Data held in a European country will be subject to the EU Directive. American companies also face privacy legislation at the local, state and federal level including the Gramm-Leach-Bliley (GLB) Act and Health Insurance Portability and Accountability Act (HIPAA). Combined with this global patchwork of regulations are the data and privacy policies present in your company.

As Chief Privacy Officer your next challenge is to apply and enforce data regulations and policies on the data and continually monitor and assess the data flows within the organization. A CPO also needs to grapple with issues such as providing consumers with access to certain types of data in order to foster trust, and restricting third party sharing of data in an environment where thousands of employees might have access to information assets that are spread across multiple applications. Some regulations such as HIPAA also call for businesses to obtain consent from consumers before sharing their data. Setting up a call center or mailing out hundreds of thousands of notices can be a costly exercise compared to having tools that can automate this procedure.

Zero-Knowledge Systems' Privacy Rights Management Suite is an enterprise software solution designed to enable the entire range of processes detailed above.

Our PRM Suite applies a policy-based framework to enterprise IT infrastructures for the responsible management of personal information, enabling business to mitigate risk, attain compliance and build consumer trust. The various components of the Suite are designed as tools to allow businesses to rollout their information privacy program in an efficient and reliable manner, and include:

- Discovery and inventory of personal information resources
- Definition and articulation of privacy policies in an application-readable form
- Policy implementation at the application and data store level
- System monitoring of personal information handling practices
- Enforcement of information privacy requirements
- Audit and assurance of information privacy practices

The Zero-Knowledge PRM Console, the first component of our PRM Suite to be released in Q4 of this year, enables the end-to-end management of information privacy within an enterprise. Information security and privacy officers can discover, inventory, and classify personal information (PI) assets while applying relevant global data regulations and corporate privacy policy. The Console works with existing IT resources such as customer and employee databases, Web servers, enterprise applications and access control solutions.

PRM Console features include:

- **Discovery and Inventory module:** Enables and centralizes the identification, classification and management of personal information throughout the enterprise
- **Modeling module:** Supports compliance efforts by enabling the application of rules based on regulation or corporate policy, and customer preferences to personal information

- **Reporting module:** Ensures privacy or security officers have the reports needed to facilitate management, auditing and verification

Underlying PRM is Privacy Rights Markup Language (PRML), a language specification designed to capture the complex relationship between business operations and personal information. PRML formalizes privacy policies and operational procedures across enterprise applications and data stores, producing detailed reports and requirements as output. PRML's underlying principles are based on the OECD Fair Information Practices and support a wide range of possible privacy policies and several forms of output, including XML and plain English. Future releases of PRML will provide automated enforcement within the enterprise IT infrastructure.

The goal of the PRM Suite is to define a standard of functionality that will secure personal information by providing data protection and security officers and CPOs with a toolkit to facilitate and reduce the cost of regulatory compliance, while supporting business objectives, and customer preference and choice. The PRM Suite takes advantage of a wide range of new and evolving technologies to support legacy enterprise applications while simplifying integration through a component-based application model. It supports applications ranging from traditional client-server applications delivered over corporate intranets to outward facing web services on the Internet.

If the developments of recent data and communication technologies are going to fulfill their promise, customers need to trust businesses with the collection, disclosure and use of their personal information. The Zero-Knowledge PRM Suite provides a cost effective means to implement privacy solutions that enable global and industry-wide compliance, which in turn fosters consumer trust, and enhances both the value of information assets.

## THE PROMISE OF PRM AND PRIVACY ENABLING TECHNOLOGIES

PRM technologies such as Zero-Knowledge's PRM Suite can be a major force in enabling businesses to build privacy into their operations and thus raise the bar for privacy in our society.

The Zero-Knowledge PRM suite empowers data protection and security officers with the tools to effectively address the intensifying demand for consumer privacy, to navigate complex global regulations, and most of all, to institutionalize the enterprise's commitment to protecting consumer privacy in a demonstrable manner. Specifically, the Suite allows for

- assessment and mitigation of risk across the entire organization
- simplifies compliance in a cost-effective manner
- assembles a dynamic inventory of company-wide information assets and practices
- enforces policy on personal information assets
- generates reports to facilitate auditing and assurance

The key to successful adoption of data protection and information privacy technologies within the enterprise is to assure that they support corporate objectives, do not hinder commercial activity or burden the enterprise with demands that cannot realistically be met. Privacy Rights Management technologies are being developed to privacy-enable everyday business operations in a way that is manageable and cost-effective to the organization, yet still meets the high privacy standards of consumers.

Business objectives like personalization, marketing, and online transaction and payments do not have to compromise consumer privacy. Analytical research, direct marketing, and trends in ubiquitous communications also need not be impeded by privacy objectives such as compliance, consent, notice, opt-in, access, or use limitation. Building trust with consumers, managing data security risks, and implementing sufficient safeguards can be achieved by aligning business and privacy into a single, coherent, strategy that combines effective policies and Privacy Rights Management technologies.

## STANDING AT THE CROSSROADS

As both an entrepreneur and privacy advocate I believe we are at a critical junction for privacy. We are currently experiencing the largest explosion of information in history. The new networks and devices being deployed will make personal information available anywhere, anytime. The overwhelming majority of this information being created and spread over a plethora of devices and networks will be personal information—and it will primarily reside with businesses and organizations, rather than with individuals themselves.

The information and networking explosion affects every individual, organization and business. Whether the net effect will be positive for information privacy or neg-

ative will depend on the policies we adopt, and the availability of technologies to enforce those policies.

I believe the combination of consumer privacy protection tools and Privacy Rights Management technologies within the enterprise provide an immediate and fundamental framework for addressing privacy in the information society. The combination of these privacy-enabling technologies with strong privacy and data handling policies is a powerful and effective approach.

In conclusion I want to articulate that over the past four years I have been encouraged by the positive steps industry leaders and policy-makers such as yourselves have taken. As a society, we have a critical challenge and opportunity in front of us, and I hope we can continue to work together to ensure information privacy and business can flourish together.

Again, I thank the Subcommittee for the opportunity to participate in today's hearing. This hearing provides a valuable opportunity to discuss the important role that technology solutions play in addressing both business and consumer needs with regard to privacy. Zero-Knowledge Systems looks forward to continuing to work with the Subcommittee in its review of privacy issues.

Mr. STEARNS. We have with us this morning on panel No. 1 Ms. Frances Schlosstein, VP, Business Development and Marketing, Webwasher, New York City; Mr. John Schwarz, CEO of Reciprocal of New York City; Mr. Michael Wallent, Product Unit Manager, Internet Explorer, Microsoft Corporation; and, last, Mr. Stephen Hsu, Co-founder, Chairman, and CEO of SafeWeb, Incorporated, Oakland, California.

We are delighted that you are here, and we look forward to your opening statement. And we will start with you, Ms. Schlosstein. Oh, we are going to start with Mr. Wallent, sorry, with the demonstration. Go ahead.

**STATEMENTS OF MICHAEL WALLENT, PRODUCT UNIT MANAGER, INTERNET EXPLORER, MICROSOFT CORPORATION; FRANCES SCHLOSSTEIN, VICE PRESIDENT, BUSINESS DEVELOPMENT AND MARKETING, WEBWASHER; STEPHEN HSU, CO-FOUNDER, CHAIRMAN AND CEO, SAFEWEB, INC.; AND JOHN SCHWARZ, CEO, RECIPROCAL**

Mr. WALLENT. I just want to ensure that the monitors are on before we—sorry for the delay, sir. Could we get a little bit more light, actually, so I can see my notes? Thank you.

Turn on the monitors. It should be on. Did it get unplugged? Okay. Okay. It is great working for technology companies.

Chairman Stearns——

Mr. STEARNS. Mr. Wallent, just pull the microphone just a little bit more closer to you. That would be helpful.

Mr. WALLENT. Certainly.

Mr. STEARNS. Yes, okay. Great. Okay.

Mr. WALLENT. Chairman Stearns, ranking member Towns, members of this committee, thank you very much for the opportunity to testify here today. My name is Michael Wallent, and I run the Internet Explorer team at Microsoft Corporation in Redmond, Washington.

We are currently working on Internet Explorer version 6, the next version of our popular browsing technology, which we had planned to release with Windows XP on October 25 of this year.

What I am going to show you today is a tool that gives consumers on a broad scale greater control over their online information than they have ever had before. One of the most frequent issues that we hear are concerns about online profiling or online

tracking, issues that many of the members here today raised in their statements.

This is the practice of collecting a history of a user's actions as they work across the web or across a series of sites. Once this information is combined with what is called "personally identifiable information," such as a name, an address, or a phone number, specific advertising or other services can be targeted directly to that consumer.

Most of this tracking is done from a technological sense through the use of a technology called cookies. Cookies are simply small pieces of information that the website leaves on the user's computer for later access. It is important to note that cookies are neither good nor bad. Without cookies, the web as we know it would simply not work.

There would be no customization, an important part of a consumer's web surfing experience. E-commerce would be accessibly difficult, and the economics of the web would be radically different. Before we get into details about cookie management, the topic I am going to talk about today, let me define a couple of terms.

First of all, you will hear a lot about what are called first party cookies. A first party cookie is simply a cookie that comes from the website that the consumer knows that they are visiting. I go to MSN. MSN serves me a cookie. It is a first party cookie.

The other concept you will hear is what is called a third party cookie. A third party cookie comes from some content on the page that the consumer may not know about. A very common example of this was seen with the online advertisers, such as Doubleclick, Avenue A, or Engage, many of which the services that even Microsoft uses today.

When a consumer goes to a website that has this online advertising, if that online advertiser serves a cookie, that is what we call a third party cookie. Third party cookies were, in fact, implicated in many of the online tracking issues that consumers brought to us. However, I will also note that third party cookies do have some very consumer beneficial features and some are very benign, and also, as I said, beneficial for those consumers.

Last summer we made a first attempt at providing some advanced cookie management for our customers. What we thought was is that whenever a consumer encountered one of these third party cookies that were at times implicated in online tracking we would simply ask the consumer, "Consumer: Would you like to accept this cookie or block this cookie?" When confronted with this choice, though, consumers didn't really have enough information to make that choice, and it was a confusing question. We didn't have the capabilities at that time to give consumers the information and the data they needed to answer that question. So they simply turned the feature off.

At the same time, and for quite some time now, we have been working with the World Wide Web Consortium or W3C on a standard called P3P, which, again, many of you mentioned here today. The goal of P3P is to provide a common language for a site to describe its data practices, such as what data it collects, who that data is given to, what the use of that data collection is.

It turned out that it was just this type of information that consumers needed to use to make better decisions about cookies. What we have now done in Internet Explorer 6's integrated P3P technology is provide a precisely controllable, non-intrusive model that gives consumers very easy-to-use cookie controls.

One of the important issues that we faced, though, was how to provide a heightened level of protection, what we call out of the box, by default, so people would be protected without any intervention on their behalf.

What we have come to, then, for this default or out of the box setting is that in order for these third party cookies to be used they must indicate—the company that provides the third party cookie must have a P3P compliant privacy policy. And if that privacy policy indicates that that site is reusing the consumer's personally identifiable information, they must allow the consumer to either opt in or opt out of that data practice, or, even with a privacy policy, that cookie is, in fact, blocked.

Let me show you how this works. We have some screen shots that we took very recently that we will show you here today. It is a little bit quicker than an online presentation.

So the first time a consumer connects to a website whose privacy practices do not match the consumer's settings, whatever they might be in Internet Explorer 6, this small window appears. The goal of this window is to educate the consumer about this new red-eye privacy icon that we see down in the bottom right corner of the screen. I don't know if the members can see that. There is an arrow, and I will point it out to you. We will blow it up.

See this little red stop with the "I." This is the new red-eye privacy icon. Whenever it disappears on a website, it indicates to the consumer that there is a fundamental mismatch between the privacy policy of the website and the consumer's current privacy preferences.

The other thing I would like to call out here is that the privacy defaults that Microsoft created are by no means the only choices that a consumer has. Here we see a dialog that actually gives consumers control over what their privacy settings are. By default here, we see that the setting is on medium, which has the behavior that I described to you earlier, which requires privacy policies and requires opt-out for any personal information reuse.

We have heard a lot of comments and feedback about opt-in privacy, and we felt it was very important to allow consumers a very easy mechanism for them to choose to move to an opt-in model. With this slider, if the user clicks up two notches, they go to high privacy. High privacy requires privacy policies across the board for all websites at all times.

And further than that, it requires that if there is any personal information reuse that the user has expressly opted in to that data reuse.

I would like to also point out that we also have a setting that we call accept all cookies or the lowest possible security setting, and this, in fact, is the status quo on the web with browsers today. Now, I would like to just show an example of what a consumer might encounter as they browse through the web at a later time.

I shot an example here, sir, of The Wall Street Journal. The Wall Street Journal I know is using advertising from Doubleclick. And Doubleclick, while we are working with them actively to deploy P3P-compliant privacy policies, has not yet done so.

Because The Wall Street Journal has this advertising from Doubleclick, Doubleclick is using third party cookies, and there is no privacy preference or privacy policy around those cookies. Those cookies are, in fact, blocked.

So we actually see here on the bottom right-hand corner of the screen the little red-eye privacy icon. This is something that we expect consumers to notice over time and be able to clearly tell when they go to a site that has a privacy policy that matches their settings, versus a privacy policy that does not match their setting, helping them really control their browsing experience.

And we can also see just in detail that the consumer can get a lot of information about what specifically was blocked on their behalf.

So while I am not showing it here today, we have many other features in Internet Explorer 6 that help consumers control their privacy, such as a mechanism to easily read the P3P policy and provide a very common format such that consumers can compare them between site to site. We have also ways for consumers to import custom privacy settings of their own that might be created by experts such as folks on the panel sitting here with me today.

We also have mechanisms that are very easy for the consumer to use to either block or opt out of specific sites, to either block or always allow that content.

We are actively encouraging websites to deploy these P3P-compliant privacy policies. Based on the feedback we have received so far, we hope and expect that many of the top 100 websites, as well as the vast majority of the online advertisers, to deploy P3P-compliant policies by the time we ship Internet Explorer version 6.

IE6 is not a silver bullet solution to all online privacy issues, though. But we believe it is a significant step, showing that technology can play a very critical role in addressing consumers' concerns. Fundamentally, we believe that we have done work that consumers want and it will delight them.

Thank you, and I look forward to your questions.

[The prepared statement of Michael Wallent follows:]

PREPARED STATEMENT OF MICHAEL WALLENT, PRODUCT UNIT MANAGER, INTERNET EXPLORER, MICROSOFT CORPORATION

Chairman Stearns, Ranking Member Towns, Members of this distinguished committee, thank you for the opportunity to testify before you today on subjects that are very important to consumers—Internet privacy and the tools that consumers can use to protect their privacy. My name is Michael Wallent, and I lead the Internet Explorer technology team at Microsoft Corporation. At Microsoft, we are not only dedicated to protecting consumer privacy, but from an even broader perspective, to building an online community that customers trust and to promoting vigorous growth of online opportunities for all.

OVERVIEW: THE MARKETPLACE IS DEMANDING BETTER PRIVACY TOOLS

Today I would like to share with you just one of the things our company is doing around the issue of online privacy. For several years, Microsoft has been at the forefront of promoting privacy online. We have been developing privacy best practices and procedures under the leadership of our Director of Corporate Privacy, Richard Purcell. We have been actively involved in coalitions such as getnetwise.org, which

focuses on building a safer web for our children. Elsewhere in the company, we are developing futuristic technological tools that have the potential to ultimately transform how online privacy protection is delivered to consumers. My division of the company, the Internet Explorer team, is just one place where privacy protection is a part of our basic objectives.

One of the great things about working on Internet browsing technology in general, and Internet Explorer specifically, is that almost everyone that I meet has used this web surfing capability in some way. Because the web is increasingly important in people's lives, one of the issues customers raise with us more and more is their desire to know that their privacy is being protected when they go online. When we receive such feedback, we attempt to the extent possible to incorporate features that meet this demand and that give consumers better control of their personal information. In the end, it's my job to build software that delights our customers. Because of consumer demand, I currently have about 25 people working on the privacy protections in Internet Explorer.

INTERNET EXPLORER 6.0: TACKLING ONLINE TRACKING

When we talk to our customers, one of the questions they raise most often is whether their web surfing activities can be tracked. It is an issue that the Microsoft Internet Explorer team has been working to address for about eighteen months now. Tracking or profiling is the practice of collecting a profile or history of a user's actions across a web site or series of sites. When combined with "personally identifiable information," such as name, address, phone number or other identification, whoever collects this profile can market or target advertising or other services specifically to a customer.

Much of the online tracking you hear about comes through the use of "cookies," small benign pieces of information that a web site stores on an individual's computer. It is important to note that cookies in and of themselves are neither good nor bad. Without cookies, the web wouldn't work as people expect it to. There would be no customization, no e-commerce and the economics of the web would be called into question. However, consumers should still be in control of this technology.

Since most online profiling comes through the use of cookies, Microsoft has been concentrating its privacy protection mechanisms in Internet Explorer around cookie management features, which we have designed to enhance notice and choice of the information practices of the web sites that consumers use. Based on our experience with a series of test versions of Internet Explorer and our work with the World Wide Web Consortium's (the "W3C's") Privacy Working Group, we believe that the next version of Internet Explorer—IE 6.0—will take significant strides in protecting consumers' privacy.

One of the most challenging things about building software for tens or even hundreds of millions of people all around the world is that it needs to work in a way that provides the protection consumers want, but without disrupting or slowing their web browsing experience. In some of the earlier test versions of privacy protections in Internet Explorer, we found that consumers were actually frustrated with tools that popped-up questions or prompted the consumer every time a cookie might be used for tracking purposes. It turned out to be too burdensome and confusing for consumers to understand exactly what was going on behind the scenes on their computers.

From the significant usability tests that Microsoft does, we know that if you constantly pop-up privacy questions, users either disregard them or perform whatever action is necessary to make these pop-ups go away. Obviously, this behavior undermines the goal of protecting the user more thoroughly. So we've been working to create a solution that helps consumers to control cookies. And we've been especially focused on so-called third-party cookies that can be used to track your activities across sites—that is, cookies that come from a party other than the site a consumer is visiting. Our tools help consumers better understand the source and purpose of the cookie, thereby giving the consumer more control over whether it is accepted or rejected. Our tools also offer a default level of privacy protection that is greater than exists on the web today, so that out of the box, users of Internet Explorer 6.0 enjoy protections they currently do not have.

PROTECTING PRIVACY THROUGH INDUSTRY STANDARDS

Before we get deeper into the details, let us focus on the role industry standards have played in getting us to where we are today. As my team of engineers was examining the best path to take to control cookies through Internet Explorer, we were simultaneously working with the World Wide Web Consortium on a technical standard called the "Platform for Privacy Preferences Project" or P3P. The goal of P3P

is to provide a common language for a site to describe its data practices—such as what data the site collects, how the site uses it, who gets access to it, how long the data is retained, what consumers should do if they have a privacy complaint, etc. The common language helps web sites describe the important aspects of their information practices according to a standardized road map.

P3P also provides a mechanism for a site to provide a machine-readable version of its data practices. The grand vision of P3P is that once sites code their privacy policies according to the standard, and consumers have P3P tools in their hands, consumers can automatically match their individual privacy preferences against the practices of the web sites they are visiting. If the web site satisfies the consumer's preferences, the consumer enters the web site without incident. If the site does not match the individual's personal setting, the consumer at least is warned of that fact before proceeding.

In Internet Explorer 6.0, we take a significant first step in promoting adoption of the industry's P3P standard by both web sites and consumers. By providing a default level of protection out of the box, we are creating incentives for web sites—and especially those that use cookies in a third-party fashion—to code their privacy policies in the P3P language. These incentives will exist because we anticipate that millions of web surfers will choose to upgrade to IE 6.0 in the near term and will automatically get the protections IE 6.0 offers.

USING P3P IN INTERNET EXPLORER 6.0

Again, based on our earlier research, consumers want to be able to automatically control the use of cookies based on the data practices of the site sending the cookie. The use of P3P technology to help solve this online tracking problem is a natural fit.

How will this work? You can actually test these tools now by downloading the public beta version of IE 6.0 at www.microsoft.com/windows/ie. But to go through them quickly, here is an overview. By default, in order for third-party cookies to be set to a consumer's computer, a third party that collects personally identifiable information must indicate, via a P3P-compliant mechanism, that the site offers "Notice" and "Choice." By notice, we mean that the site provides the consumer a machine-readable privacy policy in P3P format, which clearly states the information collection practices of that party. If there is no notice, third-party cookies from this site are blocked automatically by IE 6.0.

By choice, we mean that if a web site is reusing a consumer's personally identifiable information, then it must allow the consumer to "opt out" of or "opt in" to that data reuse. If personal information is being reused, and consumers don't have choice around that use, then the cookies from that third-party web site are blocked. This approach tracks the arrangement established last summer between the Federal Trade Commission and prominent web advertisers. The core of that arrangement is that a company that tracks users across sites, at a minimum, must provide notice of that practice and the choice of opting out of it.

To help consumers understand the concepts of notice and choice, the first time a consumer connects to a web site whose privacy practices do not match the default setting in Internet Explorer 6.0, an informational dialog-box appears. This box attempts to educate the consumer about a new "red eye" privacy icon that appears at the bottom of the browser window and what this icon means in light of the user's privacy settings. Then, with Internet Explorer 6.0, as users browse other sites that attempt to set cookies but do not meet their privacy settings, the red-eye will reappear, alerting the consumer to potential privacy issues.

While we have taken care to establish what we believe is a workable default setting, we've provided a sliding-scale feature that allows consumers to easily change their privacy settings. With a single click, consumers can change the default setting to higher privacy settings, which have more stringent requirements for the use of privacy policies, or to lower settings, which are less stringent. For example, the "high" setting requires all web sites, both first and third-party, to obtain explicit (opt-in) consent before the reuse of personal information. We additionally have a feature that allows almost infinite customizability of the privacy settings, and we have an "import" function that allows the consumer to download a third party's privacy settings (which, for example, may have default settings different from IE 6.0) and insert them into the browsing technology.

This is just an overview of our technology's features. We are happy to visit with any congressional office to review the tools in greater detail.

OUR OTHER EFFORTS TO PROMOTE P3P ADOPTION

I also want to mention the fact that, in the run-up to the release of IE 6.0, we are actively encouraging web sites to deploy P3P-compliant privacy policies. Through our ongoing work with the top 100 sites on the web, and with the work that the Internet standards body is doing, by the time that Internet Explorer 6.0 launches this fall, we hope to see significant deployment. We've also developed what we call a "Privacy Statement Wizard," an automated privacy statement generator that can help smaller sites become P3P-compliant by creating policies simply based on the site's answers to a series of questions about its practices (subject, of course, to legal review by the site's lawyer). The statement generator is currently available at http://microsoft.com/privacy/wizard. It also will soon be available at Microsoft's small business web portal, at http://privacy.bcentral.com.

PUTTING IE 6.0 IN PERSPECTIVE

Since P3P is an open standard, not controlled by Microsoft in any way, we believe that other companies will develop additional privacy-enhancing technologies that will also interact in an automated fashion with sites that have posted P3P-compliant privacy policies. In fact, we've already seen the emergence of tools that provide analysis of P3P policies, as well as search engines that only return hits from sites that follow P3P guidelines. Over the long run, we hope to see widespread adoption of P3P by the web community, as well as increasing consumer understanding of the power that P3P tools put in their hands to enhance—and customize—their privacy protection. We believe strongly that P3P is an empowering technology and that it can address in a simpler way the complex questions around consumer preferences and the articulation of sites' privacy policies.

We do not believe that the work we've done in IE 6.0 to enhance consumer privacy is a silver-bullet solution, but we do believe it is a significant positive step—showing that technology can play a critical role in addressing consumers' online privacy concerns. We believe we have done work that consumers want and that will delight them. We also believe that allowing individuals to control their own personal information is an important, enduring mission for Microsoft. It is an ongoing process, and not just a single, all-encompassing step. We take it seriously because our customers do. Finally, we believe that these first steps that we have taken to include serious privacy protection in Internet Explorer will lead to positive cooperation in the industry around this topic and will result in a better Internet and a better economy. In the future, we at Microsoft expect to do additional work in this area, using P3P or other technologies, and we would be happy to keep you abreast of those efforts.

Again, thank you for allowing me to be with you today and I look forward to a continued dialogue.

Mr. STEARNS. I thank you.

Ms. Schlosstein, we will start with you, then.

Ms. SCHLOSSTEIN. Thank you.

Mr. STEARNS. I think we are going to take a few moments here to reestablish the connection, so that the projector can provide the audience a little bit of view of what we are doing here, if that is possible, so that they also would enjoy what we see up here as members.

We are hoping in the near future—I know the Financial Services Committee has retrofitted their committee hearing room to do video teleconferencing. And so in this case, Mr. Austin Hill of Montreal, Canada, could be with us today, if we had had that capability.

And, likewise, we hope to have a projector screen here with us that will all be in place, and we would not have to continually have setups. We just move and plug it in, and we will have that capability, we are assured, that will take place in the near future. So we look forward to that.

Are you ready?

Ms. SCHLOSSTEIN. I am.

Mr. STEARNS. Okay. Go ahead.

**STATEMENT OF FRANCES SCHLOSSTEIN**

Ms. SCHLOSSTEIN. Could I have just a little more light, please?

Mr. STEARNS. Just a little bit more light.

Ms. SCHLOSSTEIN. Chairman Stearns, and members of the committee, Webwasher.com, a leader in internet access management and privacy technology, appears today not as an advocate for or against privacy regulations, but truly as an example of internet filtering technology.

We believe the technology does not and should not establish policy. Technology executes policy. Those who use Webwasher filtering software in a very real sense are already regulating their own internet environment and establishing their own policies of privacy.

What uniquely distinguishes Webwasher is our belief in internet self-determination for the user. There can be no internet privacy without the ability to control one's internet exposure. Webwasher's technology can filter out any hidden data object, oppose the security, privacy, band width, or legal risks.

Today, 4 million individuals and small businesses are using Webwasher worldwide, along with a growing number of enterprise corporations. This morning I would like to take—to provide the subcommittee with a brief look into Webwasher software interface and the types of customizable results possible. And for your convenience, I have included a copy of the presentation slides that I will be discussing in our written testimony.

Let us start now with an example of Webwasher in action, providing privacy protection from unwanted cookies attached to ads. This is Salon.com, a home page with no Webwasher filters activated. And now the same Salon.com home page with Webwasher filters activated for ad and cookie filtering.

As you see, the ads are eliminated at the top and side. To assist the visuals, the same Webwash/Salon.com page with the ads replaced by logo placeholders. This page includes nine ads that represent 38 percent of the page's total band width. What you don't see are the non-permission-based cookies behind the ads which track user behavior. Fortunately, Webwasher does see them.

Webwasher technology protects privacy and the results are measurable. On one average desktop, we conducted a 30-day filtering activity test. The test results—43 percent of band width was saved by filtering out ads. What is more, 79 percent of all cookies entering the network, nearly 5,000 cookies in all, were non-permission-based cookies attached to the filtered ads.

What is behind this technology? Let me show you the Webwasher software interface. Take a look at the tabs across the top—the standard filter, privacy filter, access control, and security filters. You can customize each function. For example, the privacy tab, a user can filter web bugs, cookies, and referrer bugs.

Similarly, the security feature interface can be customized to safeguard a corporate network. Webwasher includes a setting for eliminating bad Java scripts, ActiveX commands, including Trojan Horse-type viruses. This is accomplished through Webwasher's media type and embedded object filters.

Webwasher also approaches privacy through access control. Our access control settings deploy a dynamic, new, URL filter data base to track, classify, and, when appropriate, block changing visual

content on millions of web pages. Webwasher uses intelligent filtering and image recognition to generate the most advanced web block list in the world right now.

Here you can see the filters for pornography and nudity have been activated. To illustrate, here is the Playboy.com page, including a pop-up ad before Webwasher is activated. Now, with Webwasher, a user can block access to the website based on the Playboy.com URL. This is the message generated when a user attempts to visit a blocked site.

However, even if you did not know that Playboy was a site that contained inappropriate images, our technology can filter nudity, breast images, while leaving out content—leaving other content untouched. This is an important achievement in helping users control their privacy.

Webwasher takes a proactive approach to developing new privacy technologies. Here is the next generation technology that enables businesses and media to partner with consumers more effectively. Webwasher is anticipating the day when consumers, businesses, and media cooperate to implement a tight filtering system.

Our seclude-it technology featured here filters advertising according to user-determined interest profiles. For example, this user selected entertainment and lifestyle as just one category of ads they wish to receive. Seclude-it technology will create a new channel from advertiser to consumer that makes ads more targeted, effective, and welcomed.

What we have demonstrated today is the robust privacy protection technology of Webwasher—a technology powerful and flexible enough to execute policy, whether driven by government, corporate, or individual users.

Mr. Chairman, thank you for inviting Webwasher to appear and for assisting consumers, both individuals and corporations, to become more aware of privacy technology options such as Webwasher, already available today on the market and currently being used by 4 million users worldwide.

Thank you.

[The prepared statement of Frances Schlosstein follows:]

PREPARED STATEMENT OF FRANCES SCHLOSSTEIN, VICE PRESIDENT, BUSINESS DEVELOPMENT AND MARKETING USA, WEBWASHER.COM

INTRODUCTION

Chairman Stearns, Ranking Member Towns, and members of the Subcommittee, thank you for the opportunity to participate in this timely hearing and to share webwasher.com's unique perspective on the role of technology in the Congressional information privacy debate.

As your Subcommittee continues to explore these issues in the responsible manner that this series of hearings evidence, we firmly believe that how Congress ultimately defines Internet privacy will affirmatively determine Federal policy direction—as surely as webwasher.com's definition of privacy has shaped our own technological development strategy and core operational focus.

Over the past eighteen months, webwasher.com has directly experienced the consumer demand for privacy—four million Internet users in homes and schools have installed a free version of webwasher.com's intelligent Internet filtering software. This initial track-record, coupled with our emergence in the corporate enterprise marketplace, demonstrates to us that available and currently deployable technologies such as WebWasher already critically shape the privacy policy debate, and thus must also play a role in any related Congressional response to consumer concerns.

ABOUT WEBWASHER AND INTERNET ACCESS MANAGEMENT SOLUTIONS

WebWasher is a state-of-the-art, all-in-one software tool that blocks virus and worm-carrying Internet files, preempts the need for intrusive employee Web monitoring, protects children from pornography, and filters out up to 45% of Internet clutter that typically clogs corporate networks.

How can one program do so many different things in facilitating consumer and corporate privacy protection? Although WebWasher is a single, streamlined piece of software, it has a fully modular menu of independently operating filters that each target a specific category of Internet content. Each filter can be easily toggled on or off and configured for individual preferences, allowing each user—corporate or individual—to execute a highly-customized Internet privacy policy:

- Our privacy filter allows the user to filter out non-permission-based cookies, Web bugs, and the HTTP "referrer string." Almost everyone has heard of "cookies" that allow third parties to track without detection a user's movements on the Web. Even more troublesome to corporations is the "referrer string" usually sent from browser to Website server, potentially allowing an outsider to backtrack to the last browser location, which could be an internal company Web page.
- Our access control setting deploys a dynamic, new URL filter database to track, classify and, when appropriate, block changing visual content on millions of Web pages. This database—"DynaBLocator™"—is being built with the help of an exclusive, new image recognition technology that can keep up with the thousands of porn sites and images that are dynamically generated every day, without stable URL addresses. WebWasher is using image recognition combined with a dozen text-based rating systems to generate the most advanced Web page blocklist in the world.
- Our advertising filter includes a setting for eliminating malicious (ill-intentioned) Java scripts, as well as Java scripts designed to lock advertising into a Web page such that the page will collapse if the advertising is removed. Bad "ActiveX" commands that could allow an intruder to read, delete, or commingle company files can also be filtered.
- Our advertising filter also includes dimension and pop-up settings that remove—at the user's command—unwanted banner and pop-up ads. Internet advertising becomes a serious business issue when 35% to 45% of every page downloaded onto a corporate network is not relevant for immediate core business needs.
- Our "Seclude-It™" technology filters advertising according to a personal interest profile designed and stored on the user's computer, creating a whole new channel from advertiser to consumer that makes ads more valuable and sticky. Advertisers must partner and meta-tag their content so it can be read by the Seclude-It filter.

DEFINING PRIVACY AND BALANCING THE REGULATORY IMPULSE: USER SELF-DETERMINATION AND INDIVIDUALIZED CONTROL

What distinguishes WebWasher—and what is truly unique about our company—is that we equate Internet privacy with nothing less than Internet user self-determination. This commitment to self-determination for all Internet users—individual and corporate, public and private—has from day one driven how we run our company and how we build our tools.

Individualized user control is the reason why we developed, as our technology platform, an Internet filtering software solution. If you want to put the Internet's "controls" into the hands of its users—if you want to establish choice as a primary value in the Internet data transaction—then, we believe, you must create a broad technology for filtering many categories of Internet data that is customizable to the varying needs of users. Acting accordingly, we created and deployed WebWasher.

Fundamentally, webwasher.com believes there can be no Internet *privacy* without the ability to control one's Internet *exposure.* This exposure is two-way because data simultaneously enters and exits a user's computer. Only Webwasher, in a single software tool, addresses the two-way need for consumers to control both *what information is distributed about them over the Web* as well as *what information enters from the Web* into the private realm of the workplace, home, or school.

The benefits of webwasher.com's two-way, intelligent filtering solution are particularly obvious when compared to unidirectional privacy technologies like encryption and hosted (anonymous) surfing that are stuck in the one-way mode. WebWasher is the only leading Internet filtering software that does not compromise its own users' privacy by routing their Internet transmissions back through our own company's server.

Privacy is the security of being able to set one's own course, and most fundamentally, to protect oneself from perceived costs and risks. Whether you are a home Web surfer, an education professional, or a corporate IT manager for a Fortune 100 company, webwasher.com provides a technology that empowers users to operate in a zone of privacy, safety, and choice.

WEBWASHER IN THE ENTERPRISE: MEETING BUSINESS PRIVACY NEEDS

In many respects, the negatives of raw and unfiltered Internet exposure are nowhere so great as in corporations, where thousands of employees have unlimited desktop Internet access for many hours each day. Many companies—whether they are global financial leaders or multinational manufacturers—provide unlimited Internet access to their employees.

IDC has estimated that each employee with unlimited Internet access spends approximately one hour per day viewing non-work-related Internet content, at an annual cost in productivity of $9,600 per employee. Beyond this downtime, it only takes a few employees downloading music or streaming video to bog down an entire network, just as it takes only one employee viewing porn or hate content or downloading viral files in the workplace to put the organization at serious technological or legal risk.

As a spin-off of Siemens Corporation and as a leading global developer of Internet access management software, webwasher.com has worked very hard to understand and be responsive toward the many categories of Internet data that pose security, privacy, or legal risks for the enterprise user, and to assist in meeting their corporate risk management needs through deployment of WebWasher.

Corporations are only now beginning to pre-emptively address the privacy, security and cost implications of employee Internet access through a new category of software exemplified by WebWasher Enterprise Edition. According to a recent study by market analysts Frost & Sullivan, the Internet access control and filtering software market segment, while only a $68 million sector in 1999, is expected to approach $1 billion in revenue potential by 2007."

As a direct result of our own origin and development in the Siemens corporate environment, WebWasher is especially suited for large business users and particularly suited to respond to corporate demands that mirror what our 4 million consumer users have already told us.

The corporate user's WebWasher software application has a full menu of independently operating filters that each target a specific category of Internet content: one filter uses a database to block long lists of objectionable Websites and Web pages; other individual filters reach deep into the Web page to remove invisible data "objects" like Web bugs; and still another filter enables a block list for media-type files such as ".exe" that often carry worms and viruses.

WebWasher's access control filter, powered by dynamic image recognition technology, may prove so effective at *managing* employee Internet use that it removes the need to *monitor* employee Internet use. It promises a solution that is every bit as powerful as employee Web monitoring, but much better at balancing the corporation's need to be an Internet gatekeeper with demands for employee privacy. This same tool could save corporations the cost of collecting and storing voluminous amounts of data on employee Web surfing habits by allowing companies to preemptively manage employee access to all relevant categories of Internet content.

INTERNET ACCESS MANAGEMENT SOLUTIONS AND NEXT STEPS IN THE PRIVACY DEBATE

While today's Internet is an amazing instrument of the Information Economy, there is a toll for travelers on this information superhighway and marketplace. With each click of a mouse, along with the information a user has requested, kilobytes of data are transmitted automatically without either the user's knowledge or consent. Most unseen data is enabling to the information transaction. However, a limitless array of behind-the-scenes channels open wide avenues for data operations designed and controlled by third parties of which the user may never be aware. In other cases, a user's self-determination and individualized control may be compromised by the persistence, copiousness, or mere offensiveness of unmanaged Internet content.

For all these reasons, an intelligent Internet access management tool that can be easily customized and upgraded by the user seems the obvious technological solution— though not a simple one—as the Internet dynamically expands and continually evolves new categories of invasive content. Webwasher.com is committed to keeping its filtering tool updated to address all new genres of Internet content that significant numbers of users, for any reason, may want to filter.

Successful technologies like ours do not establish policy. In fact, we pride ourselves on having developed and introduced an apositional product that meets various users' needs. Again our definition of privacy—user self-determination—has guided our product development. Rather than be reactive to policy dialogue, our focus has been on—merely providing real solutions responsive to growing demand. By bringing privacy-enhancing technologies quickly to market, webwasher.com has changed the privacy landscape and already has impacted the conditions policymakers seek to address.

Yet, technology alone may not solve the Internet privacy dilemma. Business and consumer users must first know what their privacy problems are before they may act to adopt technical solutions to meet these concerns. Achieving such awareness often proves problematic in the Internet privacy arena since most privacy-violating data transfers over the Internet are not "visible" to the consumer. We respectfully recommend that removing this cloak of invisibility and assisting consumers to become aware of the technological options already available to them should be a primary focus of this Subcommittee's agenda.

High privacy standards are often challenged as costly and limiting to the growth and development of Web-based business. However, as an Internet technology company that voluntarily adheres to very strict privacy rules, webwasher.com can only report positive results in the form of high customer retention and a sterling corporate image.

Although we do not testify today as advocates for or against Federal privacy policy, we do see enhanced online privacy as an essential pre-condition for the Internet's next level of development, which will require winning the trust of those who have so far remained skeptical of this new medium.

Mr. Chairman, allow me to thank you for the opportunity to appear before the Subcommittee, and to close with a pledge: webwasher.com intends to stay at the forefront of Internet technology in our continuing mission to put the tools of Internet self-determination in the hands of Internet users.

Webwasher.com greatly appreciates the opportunity to be of assistance to the Subcommittee in this important review and is available to serve as a further resource as required.

Mr. STEARNS. I thank you.

Mr. Schwarz? Oh, we are going to go to Mr. Hsu. Be sure to get that microphone right up close to you, so we can hear you.

**STATEMENT OF STEPHEN HSU**

Mr. HSU. Mr. Chairman, and members of the subcommittee, thank you for this opportunity to share my views on this important subject. My company, SafeWeb, develops internet privacy and security technologies for businesses and consumers.

Our core consumer product, SafeWeb.com, lets internet users surf the web anonymously and securely. SafeWeb's technology lets users access the entire web through a layer of encryption. All of the information coming in and out of their computer is fully encrypted, and dangerous codes such as cookies and web bugs ares filtered.

Our servers act as a virtual intermediary and communicate directly with the SSL, or secure socket layer, engine present in every browser, so that no software download or installation on the part of a user is necessary.

Because our solution is free, effective, and easy to use, it has quickly grown to become one of the most widely used online privacy services in the world. We currently secure 100 million web pages each month. We are currently licensing this technology to businesses and governmental agencies that place the utmost importance on security.

The United States Central Intelligence Agency is one of our investors and has licensed our technology for internal use. The ideas for our technology originated when I was an assistant professor of

physics at Yale University and was forced to deal with numerous hacker intrusions on our department network.

A key insight that I had was that the Clinton administration's relaxation of export controls on encryption, combined with the requirements of secure e-commerce, would guarantee a nearly 100 percent installed base of strong encryption capability in every browser on every desktop.

Although you might not be aware of it, the web browser on your computer has the capability of performing encryption that is believed to be unbreakable even by the National Security Agency or the Central Intelligence Agency. We set out to write software that would make use of this widespread encryption capability.

On a global level, SafeWeb is committed to fighting against censorship and for freedom of information. Each day tens of thousands of individuals in closed societies like China and Iran use SafeWeb to access otherwise blocked contents, such as the BBC, New York Times, and Voice of America websites.

They also use SafeWeb to anonymously express possibly forbidden political views in chat rooms and on discussion boards. Our foreign users can be confident that their activities can neither be tracked, nor monitored, during a SafeWeb session. We at SafeWeb share a strong belief in the power of technology to transform closed societies.

It would be convenient to claim that technology alone can solve the problem of digital privacy. However, I think this is terribly optimistic. Tools such as ours tend to be adopted by sophisticated technologically literate people and less so by the average internet user. According to one survey, only 9 percent of online users have used encryption to scramble their e-mail, and a mere 5 percent have taken advantage of anonymous browsing.

Americans should not have to become experts on cookies, web bugs, and relationship data bases in order to preserve their privacy. It is my opinion that the protection of consumer privacy requires both legal and technological action. I hope that legislators will recognize the current trends and pass laws that will protect the rights of individuals in this burgeoning information age.

And now I would actually like to attempt something which is a little bit tricky, which is a live demonstration. So this laptop is the property of the U.S. Government, and I have not installed any software on it. I am running Mr. Wallent's IE, probably version 5, browser here.

And what you see here is what you would see if you just typed in SafeWeb.com into the browser. It would connect to our servers which are located on the internet, and they would allow you to visit any website that you choose to view. For example, here I think I have Yahoo's site. If you choose to go to another site, you can type in—here I have typed in AltaVista.com.

And what is actually happening now is that this computer is contacting our servers and requesting that page, so you are actually receiving AltaVista.com not through the normal means but through our servers. And if you look carefully, you can see this little lock icon, which means that you are viewing all of this information through a layer of encryption.

Normally, you will only see that lock icon when you are about to give your credit card number to an e-commerce site. But if you use SafeWeb, all of the traffic coming in and out of your computer is encrypted with 128-bit encryption—encryption powerful enough that even intelligence agencies can't break it.

Here I have an icon of a cookie, which when clicked will show you—this cookie will appear on the interface when a third party tries to place a tracking cookie on you. And so here it has intercepted one that would have come from AltaVista had it not been blocked. So if I click on that, you can see that the origin of the cookie was a server called ad.doubleclick.net.

Once that cookie is on your computer, Doubleclick can track you from site to site and track all of your viewing habits. But we have actually blocked that cookie as it passed through our server.

We also offer various levels of configuration similar to what Mr. Wallent talked about for his IE version 6, but currently available already from SafeWeb, which allow you to choose your level of sanitation of Java applets, plug-ins, and different levels of cookie settings.

So I would like to thank the committee for this opportunity to say a few things about SafeWeb. Thanks.

[The prepared statement of Stephen Hsu follows:]

PREPARED STATEMENT OF STEPHEN D.H. HSU, CEO AND CO-FOUNDER, SAFEWEB, INC.

Mr. Chairman and members of the Subcommittee: Thank you for this opportunity to share my views on this important subject. SafeWeb develops Internet privacy and security technologies for businesses and consumers. Our core consumer product, www.safeweb.com, lets Internet users surf the Web anonymously so that no one can pry into their online communications.

SafeWeb's technology lets users access the entire Web through a layer of encryption. All of the information coming in and out of their computers is fully encrypted, and dangerous code such as cookies and Web bugs is filtered. Our servers communicate directly with the SSL (Secure Socket Layer) engine present in every browser so that no software download or installation is necessary.

Because our solution is free, effective and easy to use, it has quickly grown to become the most widely used online privacy service in the world. We currently secure over 100 million Web pages each month through www.safeweb.com. We are also licensing this technology to businesses and governmental agencies that place the utmost importance on security and require the strongest technology available to meet their stringent requirements.

Before discussing the topic of privacy, let's begin with a broad view of what is happening in information technology. You may be familiar with Moore's Law, originally formulated by Gordon Moore, one of the co-founders of Intel. Moore observed that the computing power of microchips doubles roughly every 1.5 years. It is no surprise that today's laptop is far superior to the supercomputer of 10 years ago. A similar trend is occurring in the areas of data storage and data transmission: the cost of storing data is cut in half each year and the capacity to transmit data is doubling each year. With these factors in play, the end result is exponential growth in our ability to store, transmit and analyze information.

What does this mean for privacy? It means that technology will inevitably make it easier for governments and corporations to invade the privacy of individual citizens.

Consider the following example. Currently, someone with access to my credit card records could gain a fairly accurate picture of my eating, shopping and leisure habits. Perhaps two-thirds of all of my personal purchases are made on this credit card. Imagine the situation five years from now, when digital cash and smart cards are ubiquitous and nearly 100 percent of all purchases are executed digitally. Eventually, databases will be able to record not just how much money I spend, but exactly what I purchased, as well as where and when I made this purchase. This will apply to purchases of entertainment and food, as well as other items. It will not be long before databases will be capable of recording all of the phone and e-mail traffic of

ordinary individuals—not just basic data (e.g., identities of sender/caller/recipient, time and length of communication), but the actual content of the communications.

Why would someone be motivated to assemble such data? The answer is simple. Most businesses, from banks to shoe stores, spend significant amounts of money on customer acquisition. As businesses, they are highly motivated to make this process as efficient and economical as possible, and technology can oblige in astounding ways. Government and law enforcement have different, but equally strong, motivations to know more about what people are doing.

Is this a bad thing? Not necessarily. It would be foolish not to acknowledge the advantages this future will bring both to individuals as well as to corporations and governments. However, it is easy to see that these massive databases, once created, will be subject to myriad forms of abuse.

Survey after survey indicates that the overwhelming majority of Americans is already concerned about their online privacy and desire greater protections when they surf the Web. According to one recent survey, Americans are more concerned about loss of privacy than health care, crime, or taxes.[1]

On a global level, the need for online privacy and freedom of speech is even more urgent. Despite different countries' differing laws, we at SafeWeb believe that the right to privacy and the right of free speech are not just rights granted to American citizens by the United States Constitution; these are human rights that every country, democratic or not, ought to accord their citizens. Approximately 327 million people worldwide use the Internet today, and an estimated 502 million people will be online by 2003.

As the number of Internet users steadily grows, we can expect privacy concerns to escalate and grow increasingly volatile. The general public has only just begun to realize the extent of the privacy problem, and has only just begun to explore the possible privacy solutions.

While it would be convenient to claim that technology alone can solve these problems, to do so would be to pronounce a fallacy. There are several companies like SafeWeb that create technologies to help consumers protect their online privacy. However, these technological tools tend to be used by sophisticated, technologically savvy people, and less so by the average Internet user. According to one survey, only nine percent of online users have used encryption to scramble their e-mail, and a mere five percent have taken advantage of anonymous Web browsing services.[2] Americans should not have to become experts on cookies, Web bugs or relational databases in order to preserve their privacy.

It is my opinion that the protection of consumer privacy requires both legal and technological action. I hope that legislators will recognize the current trends and pass laws that will protect the rights of individuals in this burgeoning information age.

Thank you.

Mr. STEARNS. Thank you.

Mr. Schwarz, I guess we will offer you a little bit of time for you to set up.

Mr. SCHWARZ. Actually, I can fly——

Mr. STEARNS. You can fly?

Mr. SCHWARZ. [continuing] directly.

Mr. STEARNS. Wait a second. I think he has to—our staff has to connect something here.

## STATEMENT OF JOHN SCHWARZ

Mr. SCHWARZ. I decided that a presentation without the slides may be more appropriate.

Mr. Chairman, Mr. Stearns, Congressman Towns, members of the subcommittee, my name is John Schwarz. I am the President and CEO of Reciprocal, Incorporated. I would like to thank you for the opportunity to speak or testify before the panel.

I would like to start by saying that your committee is focusing on issues which are extremely important not just to my company

[1] Harris Interactive survey (National Consumers League), October 2000

[2] The Pew Internet & American Life Report; Trust and privacy online: Why Americans want to rewrite the rules (August 2000)

but to our economy, to our citizens' privacy, and I would argue to our citizens' security, and, obviously, ultimately to my company's business.

In our view, privacy, intellectual property, and copyright protection are all critical aspects of the same common issue. We live in an age where the physical world such as we knew it and continue to know it is being displaced by a digital one. In other words, virtually everything that we know today can be described in information and data. And once that knowledge is available, recreating the physical is pretty easy.

Products are being converted to services. In other words, what we used to buy as a "one of" thing we now today buy as a service, as an access to something, as a way to use something. And I would argue that national boundaries are becoming more transparent each day as this data is being shipped across the internet and other networks, literally without any barriers at all.

And so in this environment I think we can argue that securing digital assets and preventing unwanted digital intrusion is equivalent to defending personal and potentially national integrity. So we are talking about very important issues.

My company, Reciprocal, provides customized business infrastructure for the secure online delivery of digital assets, such things as audio, video, books, documents, games, or software. Our solution includes a defined set of features and tools, access to prepaid transaction processing, and the implementation resources needed to integrate the solution into the customer's existing systems.

So we are not a producer of technology. We are a services company that makes technology work for other people. And those other people could be other businesses. Those people could be the government. Those people could be private citizens.

We also offer consulting services to clients that need help with the definition of business models or technology choices in this digital distribution world. We run a secure online delivery solution using our computer infrastructure.

Simply stated, our clients only need to identify the digital assets that they wish to distribute and the channel through which these products are to be delivered, and we do the rest. We are arguing for a proactive management of digital assets. These can be personal, corporate, governmental or educational assets. But the proactive protection of those is very important.

Just as an example, the global media market is approaching $200 billion annually. Many of the properties are extremely valuable. You have all seen first-run movies generating $75 million of sales in a single weekend or a best-selling book selling 500,000 copies in a month.

In other industries, pharmaceutical clinical trials are distributed to thousands of subjects and their doctors. Contracts and other legal documents need to be verifiably delivered and secured. And the access to these documents and these media assets needs to be appropriately managed.

Virtually all media information today is produced in a digital format. In fact, it is almost a definitive statement. This means that it is copyable with perfect fidelity. Software and hardware that en-

able the reproduction of digital assets is now a standard feature on most computers.

Vast amounts of digital assets are, thus, illegally copied and redistributed, and these digital assets include the personal information which was described by my colleagues that is gathered from the analysis of personal behavior as people browse through the internet.

The market or the industry, our industry, has responded with a large and all-too-often confusing array of solutions developed to assist digital owners to keep what is theirs—from a simple user ID and password, to certificates of authenticity, to cookie management, to digital watermarking, to fingerprinting, to encryption, and digital rights management.

The simple truth is none of these are infallible, and that all are currently difficult to implement within what I would call a comprehensive solution. All of these tools require fairly substantial knowledge on the part of the people that will be using them.

The Reciprocal role, or the role of my company, is to take the complexity out of the decision processes and the implementation and to provide the best flexible solution for the problem at hand.

I would argue that our effectiveness and competitiveness as individuals, as companies, and as a Nation is enhanced in an environment where standards prevail, where systems can be open because there is intellectual property protection for the developer, where the invasion of privacy is treated as an illegal activity, and where the authors can be assured that their copyright has an enforceable contractual value.

And I think, by extension, we can argue that our individual rights to privacy surpass the corporate rights to copyright and to intellectual property.

The role of Reciprocal is to take it from there and make sure that these solutions are available in an easy, comprehensible, cheap, and effective way.

Thank you for listening, and I am happy to take questions.

[The prepared statement of John Schwarz follows:]

PREPARED STATEMENT OF JOHN SCHWARZ, PRESIDENT AND CEO, RECIPROCAL INC.

Dear Chairman Stearns, Congressman Towns, members of the sub-committee: My name is John Schwarz. I am the President and CEO of Reciprocal, Inc. Thank you for the opportunity to speak to you today. Your committee is focusing on issues that are very important to our economy, to our citizens' privacy and security, and to my company's business. In our view, privacy, intellectual property and copyright protection are all critical aspects of a common issue. We live in the age where the physical world is being displaced by a digital one, where products are being converted to services and where national boundaries become more transparent each day. Consequently, being able to secure digital assets and prevent unwanted digital intrusion is equivalent to defending personal and national integrity.

Reciprocal provides customized business infrastructure for the secure online delivery of digital assets (audio, video, books and documents, games or software). Our solution includes a defined set of features and tools, access to pre-paid transaction processing, and the implementation resources needed to integrate the solution into the customer's existing systems. In addition, we offer consulting services to clients who need help with the definition of business models or technology choices in the digital distribution world.

We run a secure online delivery solution using our own computer infrastructure. Simply stated, our clients only need to identify the digital assets they wish to distribute and the channel through which these products are to be delivered and we do the rest.

The global media market is approaching $250B annually. Many of the properties are extremely valuable—you have all seen a first run movie generate $75M in sales in a single weekend, or a best selling book sell 500,000 copies in a month. In other industries, pharmaceutical clinical trials are distributed to thousands of subjects and their doctors, contracts and other legal documents need to be verifiably delivered and secured.

Virtually all media today is produced in a digital format. This means that it is copyable with perfect fidelity. Software and hardware that enable the reproduction of digital assets is now a standard feature on most computers. Vast amounts of digital assets are thus illegally copied and redistributed.

The market has responded with a large and all too often confusing array of solutions developed that assist digital asset owners to keep what's theirs. From simple user id and password, to certificates of authenticity, digital watermarking and fingerprinting, encryption and digital rights management, the simple truth is that none are infallible and all are currently difficult to implement within a comprehensive solution.Reciprocal's role is to take the complexity out of the decision process and implementation and to provide the best flexible solution for the problem at hand.

Our effectiveness in enhanced in an environment where standards prevail, where systems can be open because there is intellectual property protection for the developer, where the invasion of privacy is treated as an illegal activity, and where the authors can be assured that their copyright has an enforceable contractual value.

Reciprocal can take it from there.

Once again, thank you for the opportunity to testify today and I look forward to answering any questions members of the panel may have.

Mr. STEARNS. Thank you. I will start with the questions.

Mr. Schwarz, as I understand it, you were the general manager of the IBM plant down in Boca Raton before you started your business.

Mr. SCHWARZ. That is correct.

Mr. STEARNS. And so you have seen it from a more—a longer perspective perhaps than most. In a nutshell, do you think the U.S. Government, we as legislators, should set a standard for internet privacy? Just yes or no, and then tell me why.

Mr. SCHWARZ. I would say eventually yes. Now may not be the right time.

Mr. STEARNS. So right now you, in your personal opinion, with all of your experience at IBM, and your new company, you do not think that we need to establish internet privacy as a legislative body right at the moment.

Mr. SCHWARZ. I think as Congressman Markey had said earlier, there has to be some sort of a minimum floor.

Mr. STEARNS. Minimum floor. Okay.

Mr. SCHWARZ. What that is is going to be difficult to define, and I don't think we know enough today to set that standard.

Mr. STEARNS. Well, Microsoft has worked with their new P3P, when it is fully integrated I guess with Explorer 6—when is that going to be released, Mr. Wallent?

Mr. WALLENT. We actually have next Monday publicly available data that has all of the functionality that I showed you here today——

Mr. STEARNS. Okay.

Mr. WALLENT. [continuing] that anyone can download onto Windows machines from Windows 98 forward. We expect to have a final release of Internet Explorer 6 by October 25 of this year, when we plan to launch Microsoft Windows XP.

Mr. STEARNS. How many people will eventually be using this new P3P technology?

Mr. WALLENT. Well, if past history is any guide, we expect that probably within the first 6 months of release of Internet Explorer 6 approximately 30 percent of the people who use Internet Explorer will be updated to the latest version. What that means in real numbers is that we expect by mid-2002 to have somewhere between 30 and 50 million people using Internet Explorer 6.

Mr. STEARNS. Worldwide.

Mr. WALLENT. Worldwide, yes, sir.

Mr. STEARNS. Okay. You noted your work with the World Wide Web Consortium privacy working group on P3P. How important are standards and standard-setting organizations when addressing privacy concerns with technological solutions? And I guess the question, like I talked to Mr. Schwarz, what role, if any, should the government have in setting these standards?

Mr. WALLENT. Certainly. With respect to the issue on standards, the work we did with the World Wide Web Consortium was critical, I believe, to creating a useable, worldwide solution that will help control users' privacy. As we saw last summer when Microsoft tried to do something that was not a standard, but what we did only in our browsing software, it wasn't very successful.

But yet when we pulled together the resources of the overall internet economy and the internet community, I think we worked to create something that will be very powerful for consumers.

Mr. STEARNS. Mr. Hsu, when you talk about SafeWeb, as I understand it is a free service.

Mr. HSU. Right.

Mr. STEARNS. That you can go—the consumer can go on the internet and download it and interface. How do you make money with it?

Mr. HSU. Actually, one correction. It doesn't require any download.

Mr. STEARNS. Okay.

Mr. HSU. It interfaces directly with Internet Explorer or any browser.

Mr. STEARNS. So it is a seamless interface.

Mr. HSU. Yes. The consumer service that we offer, which is free to the consumer, actually pays for itself based on the advertising that we run on the actual toolbar that you saw.

Mr. STEARNS. What happens if somebody eliminates that advertising that you are hoping to use to make sufficient funds so that you can operate?

Mr. HSU. Well, then, I think we would be in trouble. Let me comment that I think most privacy startups are in trouble right now. It is very difficult to monetize privacy, although there is a widespread—if you look at opinion polls, a widespread demand for it. It is very hard to monetize.

My company, like Austin Hill's company and all of the other privacy companies, are probably going to get most of our revenues from corporate clients, from security consulting, from developing BPN-like products. And so it would be a mistake to think that the privacy industry, technology industry, is in good shape right now.

Mr. STEARNS. Let me ask you the question I have asked Mr. Wallent and Mr. Schwarz. Do you think at this point the U.S. Government should set a standard in internet privacy?

Mr. HSU. I have to agree with Mr. Schwarz that in the long run I think it is absolutely necessary, because technologies can only protect you to a certain extent. And in the end, your data will be stored in data bases that you have no control over.

Right now, I don't think it is a completely critical time. I think that we could wait a few years and see how things develop before we actually have to——

Mr. STEARNS. Even so, the European Union has already developed a pretty comprehensive internet privacy program. And they argue that the opt-in or opt-out, depending upon the type of information, whether it is medical or financial, is very acute, and that this information should not be collected without the person's approval.

So you don't think the citizen does have that right in the United States to either opt-in or opt-out?

Mr. HSU. I think that in the long run people should have that option. However, if we delay a year or 2, it is not going to kill anybody, because right now I think the data that is in those data bases is not nearly as dangerous as what we are going to see in 5 years.

Mr. STEARNS. Okay. And my last question to Ms. Schlosstein. Yours is also free to individuals but not to businesses, is that correct?

Ms. SCHLOSSTEIN. That is correct.

Mr. STEARNS. And how many Americans I think have downloaded your software?

Ms. SCHLOSSTEIN. We estimate it is—approximately 50 percent of our downloads are from the United States and from Americans, and that is 2 million of the consumers.

Mr. STEARNS. And what would be your answer to the question I have given to the other three. Should the Federal Government set standards for internet privacy now or in the future?

Ms. SCHLOSSTEIN. Well, we believe that it is inevitable. What we stand for at Webwasher is user self-determination, that individuals need and have the right to protect their privacy, whether—both through the regulations and through the technology that offers them a way to block and control their own settings and filtering.

Mr. STEARNS. All right. Thank you.

And now the ranking member, Mr. Towns?

Mr. TOWNS. Let me just sort of follow up along the same line. It is said that most companies do not take privacy seriously. Now, if most companies do not take privacy seriously, then should we still continue to wait? Let me sort of get a response as we move down the line, starting with you, Mr. Hsu.

Mr. HSU. I think companies are starting to take things more seriously. But the problem is that once data is collected it is very hard to tell how it will be used in the future. So that as a company, a very well-intentioned company may collect a tremendous amount of data, and there is no telling who will have access to that data base in the future. So there is an issue even though companies are taking privacy seriously.

Mr. WALLENT. I believe, and I think Microsoft believes, that given the work that we have done now in Internet Explorer going forward, because of the position that we have in the market, which we admit kind of carries much responsibility with it, it also means

that at times choices that we make impact others, and I think that the choices that we have made around Internet Explorer 6 in requiring P3P policies—if those sites want to do user tracking.

Websites still work just fine without privacy policies, but yet they don't get to track the users, and that user tracking is something that really aids the economics of those sites very greatly.

So we think that this economic incentive of the consumer choosing a product like Internet Explorer, the sites wanting to have information from the consumer, but the consumer being in the driver's seat. Richard Purcell, our chief privacy officer at Microsoft, often says that consumers tell him that they want to use the web, not be used by the web. And I think the work we have done in Internet Explorer starts to deliver on that vision.

Mr. TOWNS. All right. Thank you very much.

Mr. Schwarz?

Mr. SCHWARZ. Congressman Towns, I am not sure that I would argue that companies don't care about privacy. I think companies care about privacy, certainly privacy related to their own data.

They also care about privacy relative to their customers' data. It is not clear whether companies care about data that isn't theirs or isn't their customers', but that, in fact, provides access to other people through that data.

I also would argue that individuals have often an interest in transgressing privacy of other individuals' privacy. And this is where the real crux of the matter is, because it is not necessarily the willful behavior of companies disregarding privacy laws or privacy rules.

It is the willful behavior of individuals that are disregarding those rules, and that is I think where the government needs to focus on is, how do we make sure that we manage the intrusion into people's privacy by people with ill intent?

Ms. SCHLOSSTEIN. Webwasher responds to—believes very strongly in the need for privacy protection and in the hands of the user, whether it be defined as the individual, the corporate user, or the school or government, whoever is controlling the entrance to the network.

We believe right now we have technology—Webwasher has technology, and we are finding that corporate infrastructures are adopting this kind of technology for privacy and security. And what we believe is that, with policy or without, products such as Webwasher can, at the gateway or at the individual desktop, be used by individuals to determine what comes in and what comes out of their box now, and as a complement with future policy.

Mr. TOWNS. All right. Thank you very much, Mr. Chairman. I yield.

Mr. STEARNS. I thank my colleague.

The gentleman from New Hampshire, Mr. Bass, is recognized.

Mr. BASS. Thank you very much, Mr. Chairman.

Ms. Schlosstein, the Webmaster filtering software——

Ms. SCHLOSSTEIN. Webwasher.

Mr. BASS. I am sorry, Webwasher.

Ms. SCHLOSSTEIN. I would like to, for the record, make that correction. It is Webwasher.com.

Mr. BASS. Webwasher.com.

Ms. SCHLOSSTEIN. Thank you.

Mr. BASS. Filters out all of these ads. How are the people that are putting up these websites going to make money if everybody starts washing out their ads?

Ms. SCHLOSSTEIN. Well, one way to approach that is if you saw the last slide that we presented, which was Webwasher's secluded product, Webwasher takes really a pro-consumer stance in that we have a right to decide what comes in or doesn't come in to our networks.

And, therefore, it is not anti-advertising, but only that we believe as the paradigm is shifting that the old paradigm of advertising in—traditional advertising is not working on the web, and that the future of advertising on the web is going to be a cooperative activity between the consumer, the media, and the businesses in the kind of activity that I demonstrated as seclude-it, where one can select what kind of advertising people want, when they want it, and making it really a more profitable and more convenient and welcomed activity than it currently is in the intrusive way.

Mr. BASS. Are there different types of advertising, though? Is it a kind of advertising where it is just—is there any such thing as an ad on a website that just is the ad and it doesn't leave any information in your computer? Does that exist?

Ms. SCHLOSSTEIN. Well, most ads, you know, are multi-layered, so to speak, in that they—you will see the visual ad, or whatever. But behind that ad it was—of the ads that we have stripped out in that example that I gave you of Salon.com, there were nine ads on that page. One component is it invaded privacy. You could imply from the amount of band width or time or space it took of the consumer's actual space.

But the other part that we didn't see were the cookies behind that. Thirty-eight percent—I mean, 38 percent of the band width, but 79 percent of all of the cookies that were coming into that particular box were attached—were non-permission-based. And so each ad that is coming in has attached to it other—could have malicious code, could have—the pop-ups could have cookies, could have other privacy-imposing activities going on at the same time. And many do.

Mr. BASS. Does your service eliminate or filter out things other than ads?

Ms. SCHLOSSTEIN. Yes. The Webwasher technology takes a very broad look at privacy, in that we look at not only advertising or content filtering, we look at the access control. We view an invasion of privacy, having children, for example, being exposed to pornography inappropriately. We view privacy as another approach or a front on privacy in a corporate environment with malicious code, ActiveX, Trojan Horses, those kinds of things, that could invade a corporate network and scramble the files or whatever as another imposition on corporate privacy and individual privacy.

And Webwasher's settings are such that you can customize them to really address any one of those privacy concerns.

Mr. BASS. Do you or Mr.—is it Sue?

Mr. HSU. Shoe as in tennis shoe.

Mr. BASS. You know who has your software, so you must have a data base of users. Is that right?

Mr. HSU. No. Actually, our product doesn't require you to install any software on your computer. You just connect—you point your browser at our servers. You set up that connection. It is all encrypted, and then you just go.

Mr. BASS. Do you know that I have contacted you?

Mr. HSU. No.

Mr. BASS. Really. How about you, Ms. Schlosstein? In other words, do you have—if I sign up for Webwasher.com, do you know I did?

Ms. SCHLOSSTEIN. Webwasher practices what it preaches, in that, no, we do not keep records of who downloads our——

Mr. BASS. So you can't use the information that I am using your server——

Ms. SCHLOSSTEIN. Absolutely not.

Mr. BASS. [continuing] and sell it to somebody else. It is sort of like two mirrors. It goes——

Ms. SCHLOSSTEIN. Right. Let me make a distinction here, because I think it is very important between the two technologies. And I think they are both valid and they are both very important in terms of what Webwasher does and what Webwasher is is completely controlled by the user as determined whether it be the corporate, the individual, or whatever.

There is no outside governing body. We do not take or keep or control any of that information, so there isn't any possibility of a leakage of that information or a misuse of that information, because it never leaves the control of who that self-determined user is.

Mr. BASS. Can I interrupt you, because I am going to run out of time.

Mr. Hsu, you made a comment at the very end of an answer to the Chairman's question that this is nothing—I am going to murder the quote here—that this is nothing compared to what it is going to be like 5 years from now.

Mr. HSU. That is absolutely true. I think——

Mr. BASS. Tell me about that. What is going to——

Mr. HSU. Well, I think people might be familiar with Moore's Law, which is that the power of CPUs doubles every year and a half. Well, also the power of the band width we use to transmit information and the cost of storing it, those things increase by factors of two every year.

So we are on an exponential growth path. And all of those abilities—to store data, transmit data, and analyze data—are all useful in invading people's privacy. So we are just at the very beginning right now. A few web entities have taken aggressive advantage of the way browsers are written to put these cookies on you and track you, but I think that is a very minor thing compared to what you will see 5 years from now.

Mr. BASS. Thank you, Mr. Chairman.

Mr. STEARNS. I thank you.

The gentlelady from California, Ms. Eshoo, is recognized for——

Ms. ESHOO. I am going to pass, sir.

Mr. STEARNS. All right. The gentleman from Nebraska, Mr. Terry? Sorry, sorry, sorry. Mr. Markey from Massachusetts? Sorry.

Mr. MARKEY. Thank you, Mr. Chairman.

Mr. STEARNS. No problem.

Mr. MARKEY. First of all, let me say that I think there is a false security privacy dichotomy which is made. In other words, industries say that we have top-notch security, meaning the information as it comes from your home to our company is very secure. Once we get it, now it is a privacy policy. That is a different thing altogether.

And now we have a right to modify the privacy. Okay? But don't worry, it is secure. No purple-haired kid living next door to you will be able to crack through our very top-notch encryption.

Now, from a consumer's perspective, they see the whole thing as privacy. They don't make this distinction. The reason corporate America makes the distinction is they want to give you confidence to let it go from your home to the bank or to the hospital or to the company, but then it is a different set of standards once it hits our company.

Now, we reserve the right to do certain things with it, and you have got to check with us on an ongoing basis to see whether or not your privacy is protected. Of course, the individual doesn't quite see it that way. It is all security or all privacy—whichever word you want to use, but it should be the same the whole way.

So WebTV is a good example. That is a Microsoft product. So I just pulled down here privacy policy for WebTV. So WebTV says that when you register as a primary user of the WebTV network service, WNI will request information that personally identifies you or allows us to contact you. On the WebTV network services information is your name, home address, phone number, e-mail address, and credit card number—my credit card number.

Now, you say back here that I have the right to opt out of having this ever shared with anyone else. But I personally believe you should have to get my permission. I mean, I gave you my credit card number, but I want you to have to come to me if you want to give it to somebody else.

Now, do you think that is unreasonable, Mr. Wallent, that that should be a national standard? That if you are going to take my very, very, very private credit card number, and I am going to use it to do business with you, that you should have to get permission from me if you are going to use it for any other purpose. Do you think that would be an unreasonable standard for the Congress to legislate?

Mr. WALLENT. Well, just to be clear, Microsoft doesn't oppose either privacy legislation or a specific standard per se. But with all of this——

Mr. MARKEY. So you would not oppose—so Microsoft would not oppose us applying an opt-in standard for credit card numbers. Is that what you are saying?

Mr. WALLENT. No, that is not what I am saying, sir.

Mr. MARKEY. Oh, I——

Mr. WALLENT. What I am saying is we are not opposed to legislation per se.

Mr. MARKEY. No, I understand that. But would you oppose us applying an opt-in standard for credit card numbers that are obtained by private sector corporate or individuals, and, then, that they can't

be retransferred for other purposes without the explicit permission of individuals in America?

Mr. WALLENT. I am certainly not a lawyer. I am a software developer, which gives me some benefit sitting here with you.

Mr. MARKEY. Well, but you are American, you are a human being. Okay. Do you think that—would you want someone taking your credit card number and just selling it as information, or would you want to have them have to get permission from you if you had entrusted them with your credit card number?

Mr. WALLENT. Well, I believe, sir, that information like your credit card, there are laws today that prevent credit card fraud. If I give Amazon.com my credit card number to buy a book, that doesn't give them permission to charge pornography on that credit card or some—you know, 10 other books that they think I might like.

So I am not sure I quite understand your question, sir, because I believe——

Mr. MARKEY. Right. There is a difference, though. We are talking about a difference here. There is misuse of it, in terms of creating credit card fraud, and then there is just my desire to be private. I am giving it to you. I don't want you to give it to somebody else, even if that other person isn't going to potentially engage in fraud.

I just don't want the whole world to have my credit card number. Do you think that that is—would that be an unreasonable thing for us to legislate here?

Mr. WALLENT. Well, sir, I think there is two separate issues. One is Microsoft firmly believes in the concept of notice and choice.

Mr. MARKEY. Well, that is what I am saying to you. So it is no—who has the choice? Do you have to come to us and say, "Here is your choice. If you don't give us permission, then we can't use it. Please give us your permission." Or should it be the other way around where we are going to use it, unless you actively try to stop us.

Do you think it would be unreasonable for us to say that you have to come to each of us and ask for our permission to use the credit card information which you have gathered from us for any purpose other than that which you originally contracted from a corporation perspective to gain access to that number?

Mr. WALLENT. As I said, we do fundamentally believe in the concept of notice and choice. And I think——

Mr. MARKEY. But you are not answering my question. The question is: what is the choice? Okay? Where is the burden here? I know you are not going to answer it.

Here is why—I know you are not going to answer it, and I know this is the answer that you had. But here is the problem—at the back end of this thing, changes to the WebTV network service statement of privacy. WNI may make changes to the statement from time to time.

They will post changes to our privacy statement here, right at the very bottom of this six-page privacy—we will post changes here, so be sure to check that periodically to find out if you have any more privacy that might have been changed here tomorrow morning, even though today we gave you this. We may also notify

you of significant changes by e-mail. We may also notify you. But we may not notify you, huh?

Well, that doesn't sound like a very strong commitment. When I sign up, I want it to be my deal now and forever. Amen. So, you know, it is a little bit troubling to be honest with you. There is also another part in here that deals with video and other information that you might gain from me. But, you know, in the cable industry——

Mr. STEARNS. The gentleman's time has expired.

Mr. MARKEY. Could I just—30 seconds, Mr. Chairman, and I won't——

Mr. STEARNS. By unanimous consent, so ordered.

Mr. MARKEY. I thank you.

In 1984, we passed the Cable Act, and in the Cable Act every American out here, as they are flipping from station to station, the cable industry cannot sell that information. They can't tell anyone that you flip to that particular station at 11 at night. You know? That no one else in the family knows you are watching at 11 at night, anyone else in the neighborhood, or your boss. That is yours. And they have to get your explicit permission to give out that information.

Well, a lot of the information that now, as we move 5 years down the line, it is going to be online is the same kind of very sensitive information. And I would like to think that Microsoft would understand that, just as Americans, as human beings. That the very same laws from the analog world must make some sense, because each of us might not want everyone else knowing that we were watching—gaining access to that information.

And a credit card number is a good example, and the fact that you won't give us a specific commitment here that we have a right to protect our credit card number. Your coming to us is a good indication of how far we have to go in this debate.

Mr. STEARNS. I thank the gentleman. His time has expired.

The gentleman from Nebraska, Mr. Terry?

Mr. TERRY. Thank you, Mr. Chairman.

I will actually allow you guys to talk a little bit here, but let us follow up on the comments by Mr. Markey, because there is different philosophies on how to help consumers with privacy. You have all developed different types of technologies that work.

Some of us feel that each consumer should be in control of their own destiny here, they get to make their own decisions instead of Congress making the decisions for them, personal empowerment and allowing—and it seems like your technologies allow that.

My question, though, is: what Mr. Markey is leading to, and what begs the question from my standpoint, is these technologies are great, they empower the consumer, but unless you are watching a congressional hearing, which amazingly very few people do, how do we get the word out? How do we actually let consumers know about this? How do we educate consumers about what is out there?

Because I would guarantee you, if you just pull 10 people from my neighborhood together, and maybe one of them will even know what a cookie is. So if I believe in personal empowerment and letting consumers make their own decisions on their sliding scale like

you have developed, how do we let them do that? They have to be educated to be able to make those type of decisions.

So where do you fit into the process? And what do you believe should be done to educate consumers? I will let anybody start with it. Go down the panel.

Mr. HSU. Well, I think education is the main issue, because I think most people don't understand what cookies are, and most people don't understand that when they send an e-mail it is like sending a postcard, that anyone in the middle between you and the recipient can read it.

I deal with venture capitalists and tech reporters every day who don't understand the privacy issues, and I don't think the average person understands them either. So for industry to say that people make these informed choices and punish companies that have bad privacy policies I think is a little optimistic, considering the privacy policy that Mr. Markey read is very complex and most people can't understand it.

So I think that education is extremely important, but I am not optimistic at the rate at which people will understand these complex technologies.

Mr. WALLENT. This raises the interesting issue that I tried to bring up in my testimony, which is it comes to a question of defaults. It is all well and fine to have controls in a product like Internet Explorer that let people control their privacy after the fact once they discover that that can be done.

We have tried to take a higher standard with Internet Explorer 6 and provide good privacy defaults, requiring privacy policies, and for reuse of personal information requiring that consumers have the ability to opt out and providing easy ways to let consumers dial up the bar, so it has to go to an opt-in model.

Furthermore, besides just building our technology, I have a team of about 15 people who spend full-time now evangelizing P3P. Even though it is not a Microsoft technology, we evangelize it to the top 100 websites, and also to all of the online advertisers, to try to get them to use that technology because we think it is the right thing for consumers.

Mr. SCHWARZ. I would just like to point out, in addition to Congressman Markey's point about the cable TV law of 1984, I would suspect that not one in a hundred people in this country would know that, in fact, passing that information back and forth is not allowed.

And so we are now some 16 or 17 years past that point, and we still don't have that education in place. I am not even sure that that education is necessary.

And so I think without some minimum floor that is, in fact, legislated or somehow provided as a standard by the government or by the industry, we will not make much progress in this regard. So I would argue that—to your point on education, education is important, but I think a minimum floor is going to be required.

The question is going to be: what do we define as sensitive data or data that must be protected? And how do we make that standard happen? And I don't think we have the answer today.

Ms. SCHLOSSTEIN. I agree that when Webwasher first started out we allowed for—we actually didn't have settings, and we requested

that people actually set the settings themselves. And the feedback that we got from our users was that they did actually want to have default settings set, so that they wouldn't have to deal with it on a microscopic basis. And I think that is one of the dangers that we have with the P3P platform and other very complex dialogs that occur.

So what Webwasher has done is we have actually just listened to the consumer and what they want, and our default settings are such that we have cookies—non-permission-based advertising cookies are part of the default settings now as per request by the consumers that have been using the product, and then they can go in and customize it at will, whichever way they want, if they have the knowledge and the desire to go it a further—a higher level. So that is one way that we have resolved that privacy initiative.

Mr. TERRY. Thank you.

Mr. STEARNS. The gentleman's time has expired.

The gentlelady from Colorado, Ms. DeGette, is recognized.

Ms. DEGETTE. Thank you, Mr. Chairman.

One thing that we are grappling with as policymakers is the fact that increasingly states are beginning to look at privacy issues, as well as Congress. And then you have an issue—an international issue, of course, which many of you are dealing with.

And so what I am wondering is how difficult it is for companies to navigate between the divergent privacy policies of different countries. Perhaps, Mr. Wallent, you could speak to that for a moment.

Mr. WALLENT. Certainly. So, obviously, not having a single worldwide standard is obviously additional hurdles that companies need to jump over. At Microsoft we are blessed with a large number of people and good resources to help us solve those problems.

So if you look at the work we have done on MSN, for example, and the affiliated products there, they are able to jump through the appropriate legislative and regulatory hoops across the world.

Ms. DEGETTE. But I think you would probably agree that you are unique in that capability.

Mr. WALLENT. I absolutely would. And what I was going to comment was is that it becomes excessively hard for smaller companies who are just starting up or startups to kind of follow all the right rules and understand what the laws are in all of the different places. That is why, to some extent, I think that technology standards such as P3P—everyone is concerned about privacy regulation and defining the privacy standards on a site.

P3P provides a common mechanism for a site to define their privacy policy. Now, whether or not——

Ms. DEGETTE. Well, let me stop you. We only get 5 minutes——

Mr. WALLENT. I am sorry.

Ms. DEGETTE. [continuing] so that is the problem. And so I guess what I am positing, almost as a devil's advocate position, except for I think there is some issue here, is wouldn't there be a benefit to trying to craft one uniform Federal law, so that at least we would have a consistent U.S. standard? And I don't know what that standard would look like. That is what we are grappling with.

But, you know, what we are looking at here is not just all of the international issues, but now 50 divergent State laws.

Mr. WALLENT. Right. So, as I was trying to answer for Mr. Markey, Microsoft is not opposed to privacy legislation per se. We believe in the concepts of notice and choice. But the devil is in the details. What data——

Ms. DEGETTE. I understand that. But you think it would be a good idea to try to craft something working on the details.

Mr. WALLENT. I think that it is a challenge to decide what data should be opt-in and what data should be opt-out, what practices——

Ms. DEGETTE. I understand it is a challenge. But you think it is a goal we should try to work together on? Yes or no.

Mr. WALLENT. I think it is certainly a goal to protect consumers' privacy. Absolutely.

Ms. DEGETTE. Right. Mr. Schwarz, I saw you nodding. Perhaps you would like to comment on that.

Mr. SCHWARZ. I am in agreement. There is a requirement to set a standard, to set a base, to set a minimum, but the difficulty is going to be what data, to what extent, and I don't know.

Ms. DEGETTE. Mr. Hsu, what is your view on this?

Mr. HSU. Well, I think a uniform standard is always preferable to a patchwork. A small company would have to do a lot of work to try and comply with every state's varying legislation.

Ms. DEGETTE. Ms. Schlosstein?

Ms. SCHLOSSTEIN. I think that there is a need for a baseline standard. But I think that beyond—above and beyond that that the diversity in our country really demands a diversity in policy and allows—that will allow for a diversity in policy, and that the technology must be flexible enough in order to reflect that diversity in policy.

Ms. DEGETTE. Thank you.

Something else that I am wondering about. We sit here and we have these hearings, and we hear testimony about the cookies and the different levels, and so on. And I must say, mainly due to the fact that I have two young children, I feel like I am pretty up on computer stuff. And also, I have a husband who is active in high tech issues.

But I don't think I represent the average American consumer, and I would bet that the average American consumer doesn't even know about what a cookie is or that it is happening on their computer when they order something from Amazon.com. And all of you are shaking your heads in agreement.

I am wondering if any of you know what the level of knowledge of consumers is of these issues, and what the industry is doing to educate consumers about what they can do. Perhaps we should start with you, Ms. Schlosstein.

Ms. SCHLOSSTEIN. Well, I know—I would have to agree that the knowledge level is low, and it is increasing very, very quickly as these debates contribute to that, as conversations in the public press about advertising cookies, and that I believe in the last few weeks every single national and international paper has had some sort of public article on that.

So I believe the issue is escalating. We have found that there is a completely growing demand for it, actually.

Ms. DEGETTE. Mr. Chairman, if I can ask unanimous consent just for another additional time to allow the rest to answer perhaps as to what efforts the industry is making for consumer education.

Mr. STEARNS. By unanimous consent, so ordered.

Ms. DEGETTE. Thank you.

Mr. STEARNS. Go ahead. If the rest of you will answer her question.

Mr. SCHWARZ. My answer would be that the level of knowledge depends on the age of the person that you are talking to. I would argue that kids that are in grade school, high school, have no difficulty with most of what we talked about today.

When you get to people of our age, it is a different story. And I don't think that we are going to change that. I think we will have to wait for this new generation of people that are growing up with computers as a toy to become consumers and adults, to have the level of knowledge that is necessary to make these informed decisions.

And so in the meanwhile, while we are dealing with consumers that are not that educated, there is some level of base that is necessary to protect them.

Mr. WALLENT. To somewhat echo what Mr. Schwarz has said, I think there was an interesting issue, though, where I don't think in the technology industry it is our goal to try to educate consumers about all of the little nitty details about technology, about what a cookie is and what it does, and first party and third party.

You have to have good consumer privacy and good solutions for consumers that don't require them to understand what my job is. It just has to work. It has to make sense for consumers and have understandable choices for them to make. And that is really something that we have tried to work very hard on.

Mr. HSU. I agree with Mr. Wallent. I don't have any hope that at any point in time 90 percent of the population will understand what a cookie is or what a profiling data base is. Even a kid who is very good at playing Doom may not understand what Doubleclick is doing with their data. So I think that we have to simply it in some way and inspire confidence in the individual that things are being done, even though they don't understand the technical nitty-gritty.

Ms. DEGETTE. Well, I guess I would just say that if people don't know what is going on, they don't realize the need for privacy policy. And so I think consumer education needs to happen.

And, Mr. Chairman, I would ask if all of these witnesses could perhaps supplement the record in writing by telling us what their consumer education efforts are. They are never going to understand the need to have a privacy policy if they don't know what their risk is.

And I thank the Chair for its indulgence.

Mr. STEARNS. I think what the gentlelady is alluding to the panel is that we, as legislators, would like your input on what we could do to educate, and what can be done on a national scale to educate users of computers who will be let into this camouflaged area where they think they are safe, where, in fact, they could be detected and a lot of their privacy revealed. So if you would do that, it would be appreciated.

The gentlelady's time is up, and the next person—there is no one on this side. We will move to Mr. Doyle of Pennsylvania.

Mr. DOYLE. Thank you, Mr. Chairman.

It has been very interesting. Mr. Markey and I were just talking. I mean, when you think about the web and the computers, so many of us are in kindergarten in terms of understanding the applications. Those of us that started dabbling in these things at a later stage of our lives, we understand the implications of that information, but not the applications.

Our children seem to understand the applications but don't think about the implications of what they are doing on the web. And how to bring everyone up to speed—I don't think we are ever going to be able to do that. I don't think there is going to be a way to effectively educate everybody on how to use these tools.

I mean, most people just don't have a clue how to do any of this, and I don't think they are aware of how the information is being used. I think that is what is going to change this down the road. I mean, the idea that somebody would be able to sell a list of all of the telephone numbers you dialed in the last month—you know, people would—they grasp that, and they would never permit that.

What they don't grasp is how this data is floating around the web and how people are able to track it and access it and use it. People really don't understand that is what is going on.

I remember a lot of us, the first time we discovered that when you send an e-mail, and you erased it, everybody thought it was erased. Then you found out it is still on the hard drive, and I can bet you a lot less e-mails went out of this place once that was discovered a few years back.

So I think, you know, as people come to understand, you know, how this works, and as we start to progress as a Nation in our education of the computer age, that it is inevitable that there is going to be standards.

So maybe we are not ready just yet to figure out maybe what that standard should be today, but we are going to figure it out I think fairly quickly, because, as Mr. Hsu said, 3, 4, 5 years down the road, I mean, people are going to demand it once they come to more fully understand how this information is being used.

But I find it—the discussion fascinating. Mr. Wallent, I am just curious. Now, you say there is sort of an incentive for people to join into the privacy policies—you know, adopt the privacy policies and code them in this P3P language because otherwise the browser won't accept their cookies. Right?

Mr. WALLENT. Yes, sir.

Mr. DOYLE. And I am just wondering, do you see future applications for this technology and the P3P standard, like to extend it into other areas such as minimum encryption standards?

Mr. WALLENT. Sir, to answer your first question, sir, yes, I do believe the P3P will be used—will be deployed onsites, because if sites do not deploy it their advertising revenue and some of their functionality will be blocked. With respect to the application of P3P to other technologies like encryption, P3P is a good generic technology to describe the data practices of a site.

It is not exactly clear to me how that would be applied to encryption, other than for the consumer to decide what level of encryption that is required based on the data practices of that site.

I just—if I could have just a moment, sir. I just wanted to make it clear that I don't actually work for WebTV. I have not worked on their privacy policy. Mr. Markey raises a very legitimate concern about the credit card issue that we absolutely will follow up with him after this to make sure that that is addressed. We take private information very seriously and want to make sure we address any concerns that exist on the panel.

Mr. DOYLE. I am just curious, too. What assurances are really in place to make sure that, you know, when a website agrees to Internet Explorer's privacy standards that they will actually adhere to the privacy policy? I mean, in other words, I may be secure on my side, but what stops a third party from saying they are going to follow your internet privacy but then just goes ahead and shares the information with someone else anyway?

Mr. WALLENT. Our analysis of that, sir, and from our conversations with many of the State attorneys general on this topic, is that existing consumer protection law about deceptive trade practices would be covered. Essentially, the company is making a legal representation as to what their business practices are. If they say, "No, we don't keep any of your information," but yet go ahead and do it, then clearly they are in violation of that. And the great thing is that we have it on record as to what they said their practice was in an unambiguous fashion.

Mr. DOYLE. Yes?

Ms. SCHLOSSTEIN. Could I just add to that? And I think that is one of the issues that we are going to have to deal with with P3P and other privacy protections that exist outside of the user's immediate control.

And one of the things that—I mean, it could be a complimentary function such as Webwasher or other technologies that allow both that preference selection, but at the same time, complimentary-wise, to be able to block or control anything that is going out or that information that you do not want circulated or you don't want, so that technology is available.

Mr. DOYLE. Great. Anyone else? Yes?

Mr. SCHWARZ. I would just like to also add that one of the techniques that might be deployed is to work with companies that, in fact, produce information which is sensitive information, such as credit card, such as health data, and work with them to make sure that the data that they produce or the data that they control is never dealt with in an inappropriate way.

Technology exists to protect that type of content, whether through encryption or whether through hardware implementation. And there may be another channel to get to the problem rather than looking at it bottoms up through the grass-roots effort.

Mr. DOYLE. Thank you.

Thank you, Mr. Chairman.

Mr. STEARNS. I thank the gentleman.

The gentlelady from California, Ms. Eshoo?

Ms. ESHOO. Thank you, Mr. Chairman.

Let me ask the panel if—first of all, if any of you advertise your technologies online.

Mr. HSU. We have in the past.

Ms. ESHOO. You have in the past. You don't today?

Mr. HSU. Well, actually, I can't—it is possible that we may actually have some banners running on other people's sites right now. So——

Ms. ESHOO. It doesn't sound like it is a full-fledged program, though.

Mr. HSU. No, it is not a big effort.

Mr. WALLENT. Microsoft, in our advertising for Windows XP, privacy is one of the key messages around that. We plan to spend as much money, if not more, on Windows XP than we did on Windows 95 for the marketing efforts and launch. So we expect that we will be touting our privacy efforts very, very heavily, both online and through other media.

Mr. SCHWARZ. Our entire business is built around protecting assets, and so we advertise by default.

Ms. SCHLOSSTEIN. Though we protect privacy, we don't advertise our product, but we do get—we have 4 million users just by the identified need from it. People find out about it through——

Ms. ESHOO. It really is a curiosity question more than anything else, because we are talking about how best to have the consumer understand that these technologies—first of all, that they are available, how did they find out about them, and I think there have been several questions kind of in and around that.

But I was curious to know how, you know, the masses find out about this. Or is it kind of, as we say inside the Beltway here, is it within the—kind of the geek community that we know that this is available. So it was a curiosity question.

Do any of your technologies—the P3P, Webwasher, SafeWeb—do they slow down the browsing speeds of the online user?

Ms. SCHLOSSTEIN. I can speak for Webwasher—does not.

Ms. ESHOO. Does not.

Ms. SCHLOSSTEIN. It actually speeds it up because it blocks—it actually filters out unwanted content and makes the actual browsing experience faster and more accessible for the user.

Ms. ESHOO. I mean, it is obvious why I am asking the question. If it does slow down, then people will not be so apt to move to the technology if, in fact——

Ms. SCHLOSSTEIN. Yes. I think that is one of the benefits of having it on your box or on your server is that you actually can control it. Whereas, if it is—if it does, you are at the mercy of another server.

Mr. WALLENT. The performance issue around P3P was one of the critical things that Microsoft participated on the committee to try to resolve. And, in fact——

Ms. ESHOO. We have got to get you over to the State Department. You know, you give these answers that are—there is an answer buried in the answer, but it is not like upfront. It is kind of diplomatic talk.

But at any rate, I congratulate you for having refined that.

Mr. WALLENT. No, there is no performance problem with Internet Explorer.

Ms. ESHOO. Okay.

Mr. HSU. In our case, because we are routing your data through an intermediary server before we encrypt it, there is a small performance hit.

Ms. ESHOO. What kind of feedback have you gotten from consumers and businesses about what you have? And how do you assess that?

Ms. SCHLOSSTEIN. Webwasher has a support line where we get 500 to 600 e-mails a day, and 60 percent of them are positive. So we are getting—I mean, we are getting rave reviews, thank yous, all the time—not only for the privacy that we are protecting but for the convenience that we are offering and giving them user control and self-determination online.

Ms. ESHOO. So for the time that you have had the product, give us just a little bit more. Put a little different——

Ms. SCHLOSSTEIN. Okay. Well, we have 4 million users worldwide. We have been—Webwasher has been around for about 18 months, almost 2 years, from when it was deployed. And in that time, we find that as—ironically, it is a public education issue.

And as this issue becomes more—every time there is an article in the paper, we have an enormous spike in terms of downloads onto our site. We can't tell you who they are because we don't know exactly. But we have an enormous spike, and we have an—we know that as the education and interest and awareness level rises, the demand for more privacy is going to really be enormous.

Ms. ESHOO. So you said, what, 500——

Ms. SCHLOSSTEIN. We get 500 to 600 e-mails a day.

Ms. ESHOO. A day.

Ms. SCHLOSSTEIN. A day. And I——

Ms. ESHOO. And they all say, "This is terrific"? Or do they give you——

Ms. SCHLOSSTEIN. You know, unless it is a download blip or something like that, in terms of the technological issue, or they are saying it doesn't—they find the new advertising size that we need to add to our new filters, or whatever. Most of it is around, "You are my hero," the convenience, "I am not bothered by the downloads anymore," the privacy is protected.

Ms. ESHOO. So it is positive.

Ms. SCHLOSSTEIN. And it is very positive.

Ms. ESHOO. I love the name of your company. I think it is just terrific.

Ms. SCHLOSSTEIN. Thank you.

Ms. ESHOO. Did you come up with it?

Ms. SCHLOSSTEIN. No, I would like to take credit.

Ms. ESHOO. Yes, good. Good.

Mr. SCHWARZ. Since our business, in fact, is making sure that people only get access to what they have paid for, or should have access to, this behavior is a fundamental component of the relationship we have with our clients.

What we find is that if the service that we provide does not make the experience that they have with the product that they are trying to acquire any more difficult than it had been prior to the introduction of the service, then they are reasonably happy. Of course, when the service becomes intrusive, it becomes a real problem for

them. So the convenience and the ease of use is a fundamental requirement that cannot be broached.

Ms. ESHOO. But what do they say to you, and how do you——

Mr. SCHWARZ. Well, they simply stop buying.

Ms. ESHOO. Do you hear from a lot of people? They are happy? They——

Mr. SCHWARZ. We have done implementation for about 300 firms that distribute——

Ms. ESHOO. I see.

Mr. SCHWARZ. [continuing] online, and have millions of transactions actually using that service. What we find is when the implementation for a certain client is intrusive in a way that the user deals with the content that they are trying to acquire, they stop buying. It is that simple. And you can track that almost one for one.

What they do like is once——

Ms. ESHOO. I think we are just about—the red light is on. Microsoft is not—can't get that information yet, because you are not out there. Mr.—yes, the next person, because I think—the red light is on, so I don't have any more time.

Mr. HSU. We get tremendously positive feedback, and the most positive feedback we get is typically from people in closed societies like Saudi Arabia or China, who can't see most of the web and are enabled to see it by using our service.

Ms. ESHOO. But do you know what I am looking for more than anything else? Your indulgence, Mr. Chairman, for 30 seconds more. Is it anecdotal, or do you actually—do you collect this, so that there is a building—there is a record-building of the technology and the response from people?

Mr. HSU. We store it.

Ms. ESHOO. You do.

Mr. HSU. We have thousands of e-mails from users that are positive, yes.

Ms. ESHOO. Okay. Thank you.

Thank you, Mr. Chairman.

Mr. STEARNS. I thank the gentlelady.

Mr. Shimkus?

Mr. SHIMKUS. Thank you, Mr. Chairman, and I will be brief. A simple question, kind of tied to my brief opening statement.

From the testimony—and as you can tell, I have been in and out with other meetings. But my perception is that the market has worked, the demand is present for a product to be offered. These are supposedly success stories of the basic supply and demand business model.

Briefly, tell—and, again, I apologize. This may have been answered in some of the statements. But can you briefly just go by—because the real debate is, how much do we intervene? What do we do here in Washington to pass laws to protect privacy but give people options?

Your testimony has made the compelling case that the market is working. There is a demand. If government is to intervene and attempt some standardization, which is—will be the argument that is being made for public safety of personal information—tell me the

benefits and disadvantages of doing that. And if you can just go left to right, starting with Ms. Schlosstein.

Ms. SCHLOSSTEIN. The benefits and disadvantages to policy?

Mr. SHIMKUS. Federal law mandating standards or standard practices. Actually, maybe software requirements. We do that. We do intervene so much sometimes that we actually dictate technology. So is that good or bad?

Ms. SCHLOSSTEIN. Well, the stance that Webwasher takes is that we really support using—that we provide a technology that allows for the execution of policies, whether they be minimal or really excessive.

What we would suggest probably is that in the interest of protecting consumer privacy and the right—the personal right, user rights, that the minimum amount of regulation be imposed by the government, and that you allow people to have the technology to address it on their individual, corporate, or governmental policies, so that they can be customized to reflect the uniqueness that makes this country, which is that we have so many different perspectives.

Mr. SHIMKUS. So that is a disadvantage, but you haven't told me if there is a benefit to government intervention.

Ms. SCHLOSSTEIN. Well, clearly, I mean, if you take the case of child pornography, there is not a person in this room that wouldn't—would say that children should not be protected from pornography.

But at the same time, and this is the dilemma, the conundrum, is you also wouldn't say with the—with the education benefits that are available through the worldwide web, that you wouldn't, at the same time, obstruct a child for getting education through the web that is available to them, because—and I understand there has been some trouble with like the copyrights—that Middlesex College might be blocked from the students doing research in colleges because sexes in Middlesex has been blocked by a blocker.

And the technology is such, and I demonstrated a little bit of that with our Dynablockade, or the block list function, with now the technology that allows for image recognition and contextual identification, so that you can read something within the context.

So you can read skin tones and nudity within a context, identify is it a medical site, is it an educationsite, is it a pornography site, that the technology allows now for these kinds of distinctions that will protect—will play on both sides of the fence.

Mr. SHIMKUS. Let me get to the rest of them. But my question stems to that. Does government intervention in legislative language help corporate America, who is assessing producing a product based upon demand, is our involvement helpful, or is it harmful? Will it impede the ability for you to do the research and development and reap the benefits of an identified demand?

Let me go to the other members. So——

Ms. SCHLOSSTEIN. Just to clarify that Webwasher is apositional in that what we are designed to do is allow for execution of policy that is needed.

Mr. SHIMKUS. Mr. Schwarz?

Mr. SCHWARZ. I think our view would be that you have to set an environment within which behavior can be managed and the mar-

kets can behave in a way that works. The point that I would like to leave with you is that you need to move incrementally.

We don't know enough about these issues to set a standard for all times. So you need to work within what is available and work in a way that allows you to increment your way as the industry has the ability to deliver or as the industry itself learns.

There are almost 20 million people producing this technology around the world each year. And they will be, by definition, ahead of anything that you can think of as a government or as a policy-making body. You need to stay in tune and need to stay with that advancement and not to damage it in some way.

Mr. SHIMKUS. Mr. Wallent?

Mr. WALLENT. There are certainly critical areas that legislation and your body can help with, especially in areas like identity. In fact, we talked earlier about what if sites deceive the public or tell them the wrong thing. I think the challenge, though, is getting the technology right and making sure that any specifications in the technology don't actually retard progress.

Eighteen months ago I couldn't have told you the way the P3P was going to work. It is hard to see into the future that far and define the technology.

Mr. SHIMKUS. It is very hard for politicians who are not working in engineering to make those determinations.

Mr. Hsu?

Mr. HSU. Well, the technologies you have heard about today can do things like protect you from cookie profiling or protect your data by encryption. But I think the key point is that if I make a transaction with Amazon, they know who I am, they know where I live, they have my credit card number. It is stored in their data base.

I cannot develop any technology that protects that data once Amazon has it, and that is the province of legislation.

Mr. SHIMKUS. Thank you, Mr. Chairman. I yield back.

Mr. STEARNS. Thank you.

We have completed our questions. Oh, yes. Sure.

Mr. TOWNS. One quick question.

Mr. STEARNS. Yes, Mr. Towns?

Mr. TOWNS. Mr. Schwarz, you indicated in your testimony that the technology currently used to protect intellectual property could also be used to protect government documents and records. Could you explain how this technology could benefit consumers by protecting medical, financial records, and also just personal information?

Mr. SCHWARZ. Absolutely, Congressman Towns. The fundamental technology which we deploy is based on encryption. We place the document in question into an encrypted envelope, and there is a key assigned to that envelope, and the key is the private property of the person that is designed or destined to be the recipient of that document.

And so the key and the document are always in the hands of that one individual that has been authorized to get access. And that technology can be applied to any document, whether it is medical information, whether it is financial information, whether it is music, or whether it is video.

Mr. STEARNS. And I thank panel No. 1 very much. I know how valuable your time is. And we appreciate your answers, and we look forward to continuing our discussion with you.

And now I will ask panel No. 2 to come forward. While panel No. 2 is coming forward, I would point out to my colleagues and to the audience that what has been alluded to by Webwasher is what I guess they have called contextual content. But this is really the start of artificial intelligence.

And what Mr. Hsu has mentioned, that Moore's Law has been applying to chips, it is also applying to broad band and storage. And so the analyzing, the storage, and all of this is moving so rapidly that these logarithms that are going to be created thereby where they will make decisions based upon millions and millions shades of meaning, you will make a contextual content decision which ultimately will be artificial intelligence, which they will be able to determine whether to block out something or not. And I think that alone is pretty interesting in itself.

Now, panel No. 2 is Mr. Trevor Hughes, Director, Privacy Compliance, Engage, Incorporated; Mr. Jerry Cerasale, Senior Vice President, Government Affairs, Direct Marketing Association, Incorporated; Mr. Steven J. Cole, Senior VP and General Counsel, Corporate Secretary of the Council of Better Business Bureaus, Incorporated; and Mr. Jerry DeVault, National Director, Innovative Assurance Solutions, Ernst & Young. We also have Mr. Marc Rotenberg, Executive Director, Electronic Privacy Information Center, Washington, D.C.

What we have here is a decision as to whether to start here with our opening statements. It is quarter after 12. I always believe in just moving ahead, so we will just start with the first opening statement, and we will just continue on and we will break in about—a little after 7 or 8 minutes, and hopefully then we will come back after lunch and—we have one vote now, and then we have another vote in about 45 minutes to an hour.

So we will start with the opening statements, if you folks are all set up and you are ready with your demonstration. Is that Okay? Okay. I can't see your name tag. Just move it to the left. Yes. Mr. Hughes, why don't you start?

**STATEMENTS OF J. TREVOR HUGHES, DIRECTOR, PRIVACY COMPLIANCE, ENGAGE, INC.; JERRY CERASALE, SENIOR VICE PRESIDENT, GOVERNMENT AFFAIRS, DIRECT MARKETING ASSOCIATION, INC.; STEVEN J. COLE, SENIOR VP AND GENERAL COUNSEL, CORPORATE SECRETARY OF THE COUNCIL OF BETTER BUSINESS BUREAUS, INC.; JERRY R. DEVAULT, NATIONAL DIRECTOR, INNOVATIVE ASSURANCE SOLUTIONS, ERNST & YOUNG; AND MARC ROTENBERG, EXECUTIVE DIRECTOR, ELECTRONIC PRIVACY INFORMATION CENTER**

Mr. HUGHES. By all means. Mr. Chairman, members of the committee, good——

Mr. STEARNS. If you don't mind just moving it as close as possible to you.

Mr. HUGHES. Absolutely. Good afternoon. My name is Trevor Hughes, and I am Director of Privacy at Engage. Engage is an on-

line media company. I am speaking today on behalf of the Network Advertising Initiative. Engage is a member company of the Network Advertising Initiative.

The NAI is comprised of six online advertising companies, such as Doubleclick, Engage, Avenue A, L90, Advanced Logic, and that is it. We, as a group, represent to our belief approximately 90 percent of the third party ad networks online today.

What we do is provide services to both advertisers' and publishers' websites online. We help to get advertisements to websites, and we help websites to monetize the advertising inventory that they have on their sites. One of the things that we do in this process is online preference marketing, otherwise known as profiling.

Profiling is the practice of viewing the click stream habits of a browser as it goes from site to site within any one of our members' networks. We, as a group, recognize that there are significant consumer privacy issues associated with this practice, and, as a result, almost 2 years ago now began a process of developing principles in conjunction with the FTC and the DOC, the Department of Commerce, to provide standard guidelines for our industry in regards to online preference marketing or profiling.

Those principles were released last July, almost a year ago now, and we are very proud of them. We have been working for a year under those principles. The principles, at their heart, require notice and choice. They require that our members provide notice through the thousands of websites that we represent, and also that we provide choice, various different forms of choice depending on the context of the data that we are gathering.

What I would like to talk to you today about is one of our most recent announcements, and that is of a gateway website that we launched just last month. This gateway website provides a number of important things to consumers. First of all, and perhaps most important, it provides a global opt out, a single opt-out source, where you can go and opt out of the online preference marketing practices of all six members.

You can see here the home page of the NAI, the Network Advertising Initiative. And in the bottom left corner of the screen is the opt out. That button will take you to a page that describes the process of anonymous profiling. Anonymous profiling is one of the categories of online preference marketing discussed under the NAI principles. Anonymous profiling, or non-PII as we call it, does not involve any personally identifiable information. In other words, we don't know who you are. We don't have your name or your address or your phone number or your credit card number. We don't have any identifiable information.

Rather, what we have is information about your visit to a certain site. Now, consumers may not want to have that information gathered. For that reason, we provide an opt out. This opt out is on this page. And as you scroll down, you can see each company has a description of their practices, and then a check box where you can select the opt-out option. You can say that you would like to opt out.

Once you have done that, you have gone through the six companies, I have checked off two in this example here—Engage and L90—you get a confirmation page. The confirmation page tells you,

indeed, that you have opted out. You can see green checkmarks indicating that the opt out was successful for both Engage and L90.

We found that this is a very powerful tool for consumers. And in the 1 month that the NAI gateway has been up, we have had 30,000 visits to the website, and approximately 17,000 unique opt-outs at the website.

Not only do we provide a confirmation at the time that you opt out, but you can also come to the site at any time to verify what types of cookies you have on your browser from NAI member companies. The verify function on the site is very powerful. You can see I ran it here just the other day. And what it does is it looks at your browser and tells you what types of cookies you have on your browser.

You can see for most of the members there is no cookie on this browser. Doubleclick has an active cookie. And because we have just opted out of Engage and L90, we have opt-out cookies from both Engage and L90. The combination of the opt out, the confirmation, and the verify functions we feel provide really significant—really significant consumer protection around notice and choice.

The other thing that I would like to speak to you about just briefly is the third party enforcement program that we have announced and also released. We have an independent audit firm, Arthur Andersen, now known as Andersen, and Andersen actually audits every member, or actually every member is responsible for obtaining an audit, whether through Andersen or another audit firm.

Andersen also manages a compliance program for us, where consumers can go to this site, which is accessible through the NAI site, and actually file a complaint. There is a fairly simple process that they can go through by entering some information about what their complaint is, the member that is involved, and Andersen will investigate those complaints. Andersen also fully describes the complaint process.

After an investigation, if Andersen feels that action is warranted it has a number of options available to it. It can expel a member from the compliance program and remove the compliance seal that Andersen offers. It can also notify the FTC. And through the Andersen website that we see here, it can also provide notice that the member has been expelled from the program.

In summary, we feel that the NAI has truly worked diligently over the past 18 months or so to develop a series of protections and self-regulatory standards that are meaningful and substantive. And the combination of our global opt-out and the enforcement program offered through Andersen we feel really do offer significant protections for consumers online today.

[The prepared statement of J. Trevor Hughes follows:]

PREPARED STATEMENT OF J. TREVOR HUGHES, DIRECTOR OF PRIVACY, ENGAGE, INC.

Mr. Chairman and Members of the Committee, I want to thank you for inviting me to testify. My name is Trevor Hughes, and I am the Director of Privacy for Engage. Engage is an Internet marketing and advertising services company that provides strategic marketing solutions to companies both online and offline. We were founded in 1995 and currently operate as a majority-owned operating company of CMGI.

I'm here today representing the Network Advertising Initiative, an industry group comprised of the leading Internet advertising companies formed to address con-

sumer privacy concerns. The NAI companies represent more than 90 percent of the third-party Internet advertising industry in terms of revenue and numbers of ads served. At the request of the Federal Trade Commission and the Department of Commerce, we formed the NAI to develop self-regulatory principles that would govern the practice of online preference marketing, or so-called "profiling" practices.

Mr. Chairman, as you know, the NAI announced its self-regulatory principles in July of last year after months of intensive consultations with the Federal Trade Commission and Commerce Department. The Internet advertising industry, and more specifically, the online preference marketing industry, needed to adopt "rules of the road" for its information practices to satisfy legitimate user concerns about privacy. For the industry to write these rules in a manner that would gain public confidence, the NAI needed the guiding hand of public officials. The talks between the NAI and the federal government were tough but fair, in that the industry had to make a number of important concessions. Ultimately, we were pleased that the NAI could develop industry self-regulatory guidelines that are meaningful and real and which the FTC and Clinton Administration could and did unanimously applaud.

The NAI principles deal with the practice of Online Preference Marketing. We define this as "data collected over time and across web-sites, which is used to determine or predict consumer characteristics or preferences for use in ad delivery on the Web." In other words, we try to figure out that which is the best ad to play to a consumer at a given point in time. This benefits the consumer, because they receive banner ads more relevant than would otherwise be the case. It also benefits the advertiser, because their advertising dollars are spent more effectively. Perhaps most important, this presentation of relevant advertisements allows many Web sites to gain a better return on their advertising space than they would in an untargeted environment. Collectively, our job is to make the Internet a more efficient and competitive advertising medium that will further stimulate the growth and viability of the Internet as a source for free or reduced-price content and services. Many web sites depend on our services to be competitive today.

Although OPM can be, and often stays, strictly anonymous, there are valuable consumer services that can be offered by linking OPM data to PII in an environment where consumers are given the option to choose whether the combination of that data takes place. The NAI principles lay out the ground rules and safeguards for the collection and use of Non-PII, the collection and use of PII, and the merger of PII with Non-PII.

In summary, here are the guidelines:

For Non-PII, we require notice and choice. NAI members must disclose their OPM practices through their web sites and through the NAI gateway web site, and in addition, where possible, they must contractually require their web-sites partners to disclose the collection of Non-PII for OPM. NAI members provide mechanisms for consumers to opt-out from the use of Non-PII for OPM through their respective web-sites and through the NAI gateway web-site.

For PII, we require that NAI members follow the Online Privacy Alliance (OPA) guidelines for Online Privacy Policies. These policies require the adoption and implementation of a privacy policy, and that notice and choice be afforded. In addition to and above the requirements of the OPA guidelines, NAI members will not use any sensitive personally identifiable data for OPM, that is, we have banned the use of any personally identifiable information about sensitive medical or financial data, sexual behavior or sexual orientation, or social security numbers for OPM.

For the merger of non-PII with PII, we have two scenarios. The first case is where PII is linked with previously collected Non-PII. In this case NAI members will not, without prior affirmative consent ("opt-in") merge PII with previously collected Non-PII. The second case is where PII will be merged with Non-PII for OPM purposes on a going forward basis. In this case NAI members will provide consumers with robust notice and choice.

The NAI principles include several examples of what would be considered robust notice for each of these scenarios.

The NAI principles commit NAI to develop a web site where consumers can go to "opt-out". We have done so and launched the site in May. Any consumer can today visit www.networkadvertising.org and opt-out for any or all of the NAI member ad networks. We think this is a very useful tool for consumers, and more than 30,000 consumers visited the site during its first week of operation.

The NAI members also have agreed to establish a third-party enforcement program, and we have retained Arthur Andersen and have completed that task as well. I have attached a copy of the Andersen Compliance Program document, which describes in detail all the various elements of this independent enforcement mechanism.

Andersen has launched a website—www.andersencompliance.com—where consumers can go to complain about failures to comply with the NAI Principles. If Andersen finds these complaints to be valid, Andersen can launch an investigation of any NAI member. And if Andersen finds that a Member refuses to comply with the Principles, then Andersen will remove the NAI member from the program, which means that the Member may no longer display the NAI seal. Moreover, in such an instance Andersen will notify the Federal Trade Commission with a summary of the complaint, its investigation and the failure of the Member to comply.

Finally, the NAI members strongly believe that industry, government, consumer, and advertiser pressures to set and maintain high standards for privacy will render participation in the NAI all-but-mandatory for all network advertisers.

We believe strongly that these principles represent a reasonable and workable self-regulatory approach that satisfies the needs of Internet commerce and advertising while addressing appropriately user concerns about privacy.

In conclusion and to summarize, the NAI self-regulatory principles are designed primarily to accomplish two things: first, to force advertisers and web-sites where "profiling" occurs to post notices that are strong and clear, and second, to make it easy for users to opt-out. Under these principles, NAI companies agree to afford consumers with important notice disclosures and appropriate methods of choice for participation, while at the same time one of the main engines behind this nation's booming new economy, the Internet, can continue its remarkable growth and improve as a provider of free and reduced-price content.

These agreements attested to by the signatories of the NAI Principles represent unprecedented levels of user privacy protections. Because of the contractual reach of these NAI companies across literally thousands of Web sites, the NAI Principles already have had a broad impact on Web privacy. We are very proud of these two new websites for consumers—the NAI site and the Andersen site—and we encourage you and your staff to visit these sites and give us your feedback, as we continue to refine the NAI program.

Mr. Chairman, on behalf of the NAI, I want to pledge that we will continue to work with the FTC, the Commerce Department and you and members of your staff to ensure that these self-regulatory principles live up to their promise.

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

Mr. STEARNS. I thank Mr. Hughes.

Mr. Cerasale?

**STATEMENT OF JERRY CERASALE**

Mr. CERASALE. Thank you, Mr. Chairman. Jerry Cerasale, the Senior Vice President for Government Affairs for the Direct Marketing Association. It is an association of companies with about 5,000 members who market goods directly to consumers and to businesses.

Basically, that type of marketing requires trust. If you buy something without touching it, you paid for it before you receive it. And in the United States, it is about $1.7 trillion in sales a year. About $1 trillion of it is business to consumers.

The DMA tries to build that trust through education, supporting technology, creating privacy policy generators for online marketers, self-regulatory guidelines, ethics procedures, etcetera. And these are all outlined in my written testimony, which I hope will be included in the record.

I want to focus today on the DMA's privacy promise to American consumers, and I think they are putting up a chart which kind of explains it. Every member marketer of the DMA marketing to consumers must agree to this promise and reconfirm it annually, regardless of the medium, whether it is mail, telephone, or the internet.

What does it require? It requires you to tell people if you are sharing their information, marketing information with others. You have to tell them.

Second, you have to give the consumers a choice to say no, they don't want you to share it, and to honor it.

The third one is if somebody tells you, listen, I am a customer of yours, but I don't want you to send me any more information via phone, telephone, whatever, phone, mail, or e-mail, you have to honor that as well.

And the fourth thing is you have to use the preference service, the suppression list that the DMA has. We have three of them—the mail preference service, which has been in existence since 1972. There are 4 million people on that list. The telephone preference service has been in existence since 1985, 4 million again. By the way, the telephone preference service is the do not call list for the State of Connecticut, will be the do not call list for the State of Wyoming on July 1, and will be the do not call list for the State of Maine on August 1.

And we also have an e-mail preference service, which we started after Y2K, which has 50,000 names on it at the moment. These services have to be used to eliminate the name, address, e-mail address, phone number, whatever, from any marketing campaign that a marketer has going out to try and find new prospects.

So this, in a sense, is a do not contact me list based upon the type of medium you use. It is free to consumers. Marketers do have to pay to subscribe. But it is $460 a year, and it can be subscribed to by a letter shop, which will clean up all of the lists for anyone using that shop. So one subscription can be used for a significant number of marketers. The EMPA—to get on that list, go through E-MPS.org, and you can sign up right online.

Now, what happens here with this? Well, we have staff in Washington that just deal with compliance for the privacy promise. So they are doing checks to make sure people are, in fact, following what they promised.

The mail preference service, telephone preference service, and e-mail preference service also are seated to ensure that someone isn't using that list for marketing as opposed to suppression. And we do get after people there through contract, etcetera.

But we also have a process at the DMA, the Committee on Ethical Business Practices, which reviews all DMA guidelines, not just the privacy promise. We work for correction. It is self-regulatory. We work to correct things to make it better, to stop what they are doing or correct what is happening which we think violates our guidelines, including the privacy promise.

If you refuse to work with the DMA to correct it, we have a couple of things that we can do. We have the potential of public dismissal, and for the privacy promise we have an antitrust exemption from the FTC. Or we can refer the question to the appropriate law enforcement agency, be that the FTC, the Postal Inspection Service, State Attorney General, the FCC if it has to deal with telephone.

That is our promise. That is what we try and do. We have a process already set up. We do a significant amount of education, because we think it is important to provide consumers with choice, with ability to control their information, because you cannot have direct marketing without information.

I have to have your name and address to provide to you the good that you purchased. I have to have a means to collect payment, most likely a credit card, to be able to do it. So direct marketing, unlike going to a mall and paying cash, requires information, and we have to have that consumer trust.

Thank you. I am ready to answer any questions.

[The prepared statement of Jerry Cerasale follows:]

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

I. INTRODUCTION.

Good morning, Mr. Chairman, and thank you for the opportunity to appear before your Subcommittee as it examines industry best practices and technological solutions for information privacy. I am Jerry Cerasale, Senior Vice President of Government Affairs for The Direct Marketing Association, Inc. ("The DMA"), the largest trade association for businesses interested in online and offline direct, database, and interactive marketing and electronic commerce.

The DMA represents nearly 5,000 companies in the United States and 53 foreign nations. Founded in 1917, its members include direct marketers from every business segment, as well as the non-profit and electronic marketing sectors. Included are catalogers, Internet retailers and service providers, financial services providers, book and magazine publishers, book and music clubs, retail stores, industrial manufacturers, and a host of other vertical segments including the service industries that support them.

The DMA's leadership also extends into the Internet and electronic commerce areas through the companies that are members of The DMA's Internet Alliance and the Association for Interactive Media. Members of The DMA include L.L. Bean, Time Inc., Dell Computer, Gateway 2000, DoubleClick, autobytel.com, BMG Direct, Charles Schwab & Co., Lucent Technologies, eBay, Acxiom, AT&T, AOL TimeWarner, IBM, MCI WorldCom, and others.

The DMA is a long-time leader in self-regulation and peer regulation. DMA member companies, given their track record in delivering high quality goods and services to consumers, have a major stake in the success of both online and offline commerce. The healthy, continued development of brick and mortar, catalog, and electronic commerce depends on consumer trust. It is important that these online and offline communications mediums engage in transparent marketing practices to earn that trust.

Members of The DMA are held to effective industry standards. It is these practices that I wish to focus on in my testimony today, which will place into clearer focus the state of the direct marketing industry's best privacy practices. The DMA's best practices include:

- Several DMA programs which are essential to protecting privacy online that, when created, were ahead of their time, and are now industry tools and common best practices;
- The DMA's self-regulatory Ethical Business Practice Guidelines which protect consumers privacy by addressing complaints concerning practices contrary to the Guidelines;
- A new DMA program that will satisfy the enforcement requirement of the U.S.-E.U. Safe Harbor to the European Data Directive;
- Several technology solutions supported by The DMA which will help consumers to choose and enforce how their personal data is collected and used by businesses; and
- Important DMA public education initiatives which help the government, businesses, and, most importantly, consumers to better understand the information collection process.

II. THE DMA'S BASIC ONLINE AND OFFLINE PROGRAMS.

The DMA's members understand and respect the privacy needs of consumers, can react much faster than the government to new conditions in the marketplace, and therefore has developed a self-regulatory response to privacy. For decades, The DMA and its members have worked to develop effective consumer notice and choice practices as a fundamental element of self-regulation.

Below is a brief description of The DMA's business practice tools created to incorporate both notice and choice elements and to bolster a responsible exchange of consumer information.

*A. The DMA's Privacy Promise.*

The DMA is providing leadership in the offline and online worlds through the "Privacy Promise to American Consumers," ("Privacy Promise"), which became effective July 1, 1999. The Privacy Promise requires, as a condition of membership in The DMA, that companies, including online businesses, follow a set of privacy protection practices:

- Providing customers with notice of their ability to opt out of information exchanges for marketing purposes;
- Honoring promptly individual requests to opt out of the sale, rental, or exchange of their contact information to third parties for marketing purposes;
- Accepting and maintaining consumer requests to be on an in-house suppress file to stop receiving unwanted commercial solicitations; and
- Using The DMA Preference Service suppression files, which exist for mail, telephone, and e-mail lists.

Members are permitted to display a recognizable "seal" that assures consumers of a company's commitment to privacy protection.

*B. The DMA's Privacy Principles and Guidance for Marketing Online.*

The DMA is also providing leadership in the online world. The DMA's *Privacy Principles and Guidance for Marketing Online* ("Online Guidelines") explain and highlight issues unique to online and Internet marketing. When marketing online, companies are advised that the notice they provide to consumers regarding their information practices be placed in a prominent place. The notice should state whether the marketer collects personal information online from individuals, provide certain disclosures, identify the marketer and provide an e-mail, postal address, and telephone number at which the marketer can be contacted. Marketers sharing personal information collected online are also required to provide consumers with an opportunity to opt out from the rental, exchange, or sale of this information for commercial purposes.

For online e-mail solicitations, The DMA Online Guidelines state that member solicitations should be clearly identified as such and disclose the marketer's identity. Marketers using e-mail are required to furnish consumers, with whom they do not have an established business relationship, with notice and a mechanism through which consumers can notify the marketer that they do not wish to receive future online solicitations.

*C. The DMA's Preference Services.*

The DMA has developed services to assist our members in adhering to our primary values of notice and consent. The DMA offers three different preference services for various mediums that empower consumers with effective choice: (1) the Mail Preference Service ("MPS"); (2) the Telephone Preference Service ("TPS"); and (3) the e-Mail Preference Service ("e-MPS"). Use of these services by member companies that market to consumers is required as a part of the Privacy Promise. To protect against abuse of these Preference Services, The DMA seeds and constantly monitors these lists.

*1. Mail Preference Service.*—In 1971, The DMA launched the MPS. The MPS gives consumers the power to choose whether to receive promotional mail at home. Those who wish not to receive promotional mail at home can register with The DMA's MPS by providing a name, home address, and signature by mail, at no cost, or online via the DMA Consumer Help Web site. Once a consumer's name and home address is added to the list, it remains on the list for five years. Consumers are informed about the availability of this service through state and local consumer agencies and print and broadcast advertising.

*2. Telephone Preference Service.*—Similar to the MPS, The DMA created the TPS in 1985 to honor consumer choice in telemarketing. TPS is a consumer service that is easy to use and offered at no cost. To register with TPS, individuals need only provide a name, home address, home telephone number, and signature, by either mail or via The DMA Consumer Help Web site. Afterwards, individuals' names will remain on the TPS list for five years.

The DMA is also the official distributor of the do-not-call list of the States of Connecticut, Maine, and Wyoming. All of the names found on these three States' do-not-call lists have been incorporated into The DMA's TPS file.

*3. e-Mail Preference Service.*—In further developing responsible marketing practices for the Internet age, we adapted the fundamental principles of the MPS and

TPS to create the e-MPS. The DMA's e-MPS similarly empowers consumers with notice and choice concerning the receipt of unsolicited commercial e-mail ("UCE"). Launched last year, the e-MPS allows individuals to remove their e-mail addresses from Internet marketing lists. This ambitious undertaking is aimed at empowering consumers to exercise choice regarding receipt of UCE, while creating opportunity for the many exciting new benefits of legitimate marketing in the interactive economy.

Since January 2000, consumers have been able to register for the e-MPS at a special DMA Web site. Consumers can use this service, at no cost, to place their e-mail addresses on a list indicating that they do not wish to receive UCE. This service affords consumers the flexibility to determine the types of solicitations they receive. Through this service, individuals can opt out of business-to-consumer UCE, business-to-business UCE, or all UCE.

Consumers on the e-MPS list will receive no e-mail from DMA members unless they have an established online business relationship with that company. This service also is available to companies that are not members of The DMA so that they too may take advantage of this innovative service and respect the choice of consumers who choose not to receive UCE.

*D. The DMA's Privacy Policy Generator.*

Another effective DMA program developed to help members provide effective notice and choice to consumers is The DMA's Privacy Policy Generator. This tool, available at The DMA's Web site, allows companies to create and post effective privacy policies.

The DMA's Privacy Policy Generator (http://www.the-dma.org/policy.html) enables companies, through a series of questions, to develop customized privacy policies for posting on their Web sites based on the companies' policies regarding the collection, use, and sharing of personal information. The utility of this tool, and the ease with which it is used, is demonstrated by the hundreds of companies that have used it and sent these policies to The DMA for review.

*E. The DMA's Children's Privacy Policy Generator.*

Similarly, The DMA created the Children's Privacy Policy Generator, which allows direct marketers to create and post effective children's privacy policies. This tool can be used by marketers to help them comply with the requirements of both the Children's Online Privacy Protection Act ("COPPA") and the Federal Trade Commission COPPA Rule that implements the Act.

The DMA's Children's Privacy Policy Generator is easy to use and guides marketers through an online step approach through which marketers answer a series of questions. From these questions, marketers are able to determine which disclosures they need to make in the privacy policies posted on their Web sites based on their information practices.

## III. THE DMA'S ETHICS GUIDELINES.

The DMA's self-regulatory guidelines and procedures provide a comprehensive and meaningful approach to addressing consumer privacy. At the cornerstone of the DMA's self-regulatory approach are The DMA's Guidelines for Ethical Business Practice ("Ethical Guidelines" or "Guidelines"). These Ethical Guidelines were adopted to aid its members and others engaged in direct marketing in determining ethical conduct in dealing with customers and other businesses which will be in the best interest of their customers. The DMA has undertaken extensive efforts to ensure that its members market ethically for the protection of consumers. Indeed, on a daily basis, The DMA gives its members advice on how to ensure that they are complying with its Guidelines.

In an effort to strengthen sound business practices in the marketplace, The DMA established the Committee on Ethical Business Practice to review direct marketing promotions and practices that may violate the Ethical Guidelines. The Committee reviews potential Guidelines violations of both association members and non-members. The Committee has applied the Ethical Guidelines to hundreds of direct marketing cases concerning deception, unfair business practices, personal information protection, and other ethics issues.

*A. The Process.*

The Committee receives promotions and practices for review in a number of ways: through consumers, member companies, non-members, or sometimes consumer protection agencies.

If the majority of the Committee believes that the promotion or practice brought to its attention potentially violates the Guidelines, DMA staff contacts the company

and points out the potential Guidelines violation. The company is then given an opportunity to respond. If the Committee does not believe the promotion violates the Ethical Guidelines, the case is closed and the company is not contacted again. Cases closed without company contact are handled confidentially.

Most companies cooperate with the Committee's efforts and agree to modify the questioned promotion or practice. Because cooperation with the Committee and compliance with The DMA's Ethical Guidelines are voluntary, a confidential and meaningful dialogue about the particular promotion or practices usually occurs, and the Committee and the company are typically able to reach a satisfactory conclusion.

In those cases where the Committee is successful in obtaining the company's cooperation to change the promotion or practice, or where the Committee is persuaded that the violation did not take place, the case proceedings remain confidential. The confidentiality protects all parties and helps ensure that the Committee's goal of obtaining compliance with the Guidelines is met.

In those rare instances where the Committee cannot come to a satisfactory resolution with a member or non-member company, that is, the Committee believes that the violations are continuing, the case may be referred to The DMA's Board of Directors for further action. Cases referred to the Board of Directors are made public by the Committee. Board action could include censure, suspension of membership or expulsion from the DMA. The Board may also decide to publicize its action. Companies with promotions or practices that are found to violate the law in addition to the Ethical Guidelines are referred to appropriate law enforcement authorities for handling.

The Guidelines have proven to be an effective means of ensuring ethical marketing practices by non-members as well. Although non-members are not bound by The DMA Ethical Guidelines, it has been our experience that non-member companies comply with Guidelines and policies so as to comport with industry standard practices. The net effect is to increase good business practices for the industry and to increase consumer confidence in the marketplace. In addition, where a non-member company's practice is illegal, we are able to refer the case to the appropriate federal and/ or state law enforcement authority.

*B. The Committee on Ethical Business Practice's Regulatory Approach.*

The DMA's self-regulatory approach has proven successful in addressing complaints regarding practices contrary to The DMA's Ethical Guidelines. Working with both members and non-members, The DMA has gained voluntary cooperation in adhering to these Guidelines. As a result of The DMA's efforts, many companies have reformed their practices in areas such as sweepstakes, predictive dialing, unsolicited faxes, and e-mail to address the concerns raised by activities that are violations of the Guidelines.

## IV. THE DMA SAFE HARBOR PROGRAM FOR EUROPEAN DATA.

On May 22, 2001, The DMA became the first trade association to provide a European Union Safe Harbor Enforcement Program ("DMASHP" or "Program") at no cost to its members. The DMASHP, which is an effective way for U.S. firms that choose to comply with European Union ("E.U.") data export regulations.

This Program is aimed at compliance with the enforcement element of the Safe Harbor Principles. Technical assistance and educational materials will be provided through the DMASHP to assist participants throughout the process for meeting the Safe Harbor requirements. To provide consumers with an easily recognizable symbol that signifies and distinguishes a Program participant as being in compliance with the Program, The DMA also created an easily recognizable DMASHP mark.

The Third Party Dispute Resolution Mechanism is a major component under the DMASHP that provides businesses seeking to certify under the Safe Harbor with an independent third-party dispute mechanism that complies with the Safe Harbor enforcement requirements. The Safe Harbor requires that the dispute resolution mechanism be readily available to consumers, affordable, and be able to ensure compliance with the Safe Harbor privacy protections. The DMASHP:

- provides a fair and unbiased redress of the consumer's concerns;
- is visible so that consumers with concerns know where to turn for resolution of their problem;
- is accessible so that there are no barriers to the filing of a complaint, whether they be financial or otherwise;
- provides resolution in a timely manner;
- provides finality for the consumer by reaching an independent determination of the dispute; and

• provides enforceability of the final conclusions in the determination of the consumer's dispute.

The DMA also created a DMASHP Committee ("Committee"), which has the power to hear both sides of a dispute and provide a final determination. As mentioned above, when businesses join the DMASHP, they are required to abide by the decisions of the Committee. They are also notified in the DMASHP contract that the Committee will have the authority to issue certain sanctions as a result of their decision. The lynchpin to any dispute resolution mechanism is that it be impartial. One way to ensure impartiality is to ensure openness of the results of the program by publishing the outcomes of the cases on a regular basis and for The DMA's staff to be constantly vigilant that the results are fair and legal.

Overall, this Program will provide consumers with an easy method to bring their disputes before the Committee. It is the goal of the Program to obtain a determination of all cases in a quick and timely manner, but in no case longer than 60 days.

V. TECHNOLOGY SOLUTIONS.

Technology is playing an increasingly important role in helping users determine and enforce the ways that information about them is used and collected. The DMA and marketers have been, and continue to be, instrumental in the development of this important technology by encouraging, supporting, and indeed helping to develop and promote, such software.

Since its inception, The DMA has been involved in an initiative that supports this concept—the Platform for Privacy Principles ("P3P"). This initiative, undertaken by the World Wide Web Consortium, has developed a "negotiation" approach for protecting privacy. A broad coalition of information providers, advertising and marketing specialists, software developers, credit services, telecommunications companies, and consumer and online advocates worked together on P3P to achieve a technological solution that will protect privacy without hindering the development of the Internet as a civic and commercial channel. P3P allows a user to agree to or modify the privacy practices of a Web site, and be fully informed of the site's practices before interacting with or disclosing information to a site. There also have been several announcements by companies in the last few months of other commercial products that will empower consumers with respect to privacy online. As technology continues to improve, so will consumer empowerment tools. We support the continued responsible use of this cutting-edge solution as Congress, businesses, and consumers evaluate it.

VI. PUBLIC EDUCATION.

Another important part of The DMA's efforts is spent in educating consumers and businesses about the numerous DMA programs that are available to them. The DMA has a vital interest in educating its members and the general public about the responsibilities of people who collect and use data, as well as the process. We take great pride in our education initiatives, because through them individuals and businesses will better understand the potential benefits of interactivity and the choices individuals have to control information that they submit to these businesses. Therefore, The DMA has developed a Web page devoted to privacy and launched its Privacy Action Now initiative.

The DMA has also made a special effort to empower children, parents, educators, and librarians by establishing its http://www.cybersavvy.org Web page for them and providing them with tools, information, and resources to ensure safe Web surfing. Additionally, we have produced a "hard copy" version of the Web site, Get CyberSavvy. Get CyberSavvy has the distinction of being awarded first place honors for excellence in consumer education by the National Association of Consumer Affairs Administrators.

VII. CONCLUSION.

The DMA is a long-time leader in the marketing industry's self-regulation and peer regulation. For decades, we have worked to develop practices that will address and protect consumer privacy. We understand that our online and offline worlds are more dynamic than ever and will continue to develop effective business practices in a timely manner to address consumer concerns as these mediums evolve. We congratulate the Subcommittee for taking a closer look at the industry's best practices and technology solutions and look forward to working with the Subcommittee.

[The information on DMA is retained in subcommittee files.]

Mr. SHIMKUS [presiding]. Thank you. Right on time.

Next, we will turn to Mr. Cole, Senior Vice President and General Counsel for the Corporate Secretary of the Council of Better Business Bureaus, Incorporated. Welcome, and you have 5 minutes. And your full written testimony is already submitted in the record.

Mr. Cerasale, your request was granted to put all of that into the record.

**STATEMENT OF STEVEN J. COLE**

Mr. COLE. Thank you very much, and good afternoon. I actually said good morning in my notes, but change that.

Now, you know the Better Business Bureau well, our almost universal brand recognition and our reputation for impartiality in the marketplace. BBB online operates two so-called trust mark or seal programs, reliability and privacy, and both are designed to help consumers identify companies safe to do business with online by looking for sites with one of our trust marks or using our search mechanism to find those sites.

It was our reputation and experience with self-regulation that led the business community to ask us to create an online privacy program. And the phrase "self-regulation" is not boilerplate to us. We take it seriously. Our program standards were formulated voluntarily, sleeves rolled up in work sessions by a working group of about 30 of the most important technology, consumer product, financial service, and information companies in the United States.

Since our 1999 launch, we have received over 1,500 applications from over the United States and from 20 countries, and we have awarded seals covering over 800 websites. And there are now 1,000 sites that are either qualified or in the process of qualifying.

We need to expand our reach, and I will touch on that later, but we do reach companies with a huge share of the market—high-tech companies like Hewlett-Packard, Intel, and Agilent; communications companies like AT&T and MCI; and travel services like American Airlines and Expedia; retailers like Lowe's and Fingerhut; entertainment companies like Lucas Films and Nickelodeon; and information companies like Dun & Bradstreet; and consumer goods firms like Procter & Gamble and Nestle.

In addition, our reliability trust mark now displayed on about 10,000 websites will soon require, among other things, that online advertisers post and adhere to fair information principles. And this will apply to these 10,000 sites whether or not they participate in our separate privacy seal program.

Now, our program that I am here to talk about today covers the collection of personal information online, although a few of our seal holders, such as Tupperware, apply their policies to all information collected, both online and offline.

Disclosure is the cornerstone of our program. We want a transparent environment with no surprises. And one of our key requirements calls for easy-to-find, easy-to-read notices which tell consumers the types of information collected, how their information will be used, the choices available in preventing these uses, and how the consumer could access information and make corrections.

We require the notices be placed wherever personal information is collected at the site, so that consumers are informed at the right

place and the right time about the consequences of their actions, although some of our seal holders like Xerox go further and put the notice on virtually every page.

Mr. Chairman, there has been recent critical media coverage of the complexity of some privacy notices, and we think it may miss an important point. There is a very delicate balance to draw between simple disclosures that may not tell the whole story and full disclosure which does but has a lot of ifs, ands, and buts, and definitions.

We work hard to strike that balance reasonably, and we prefer full disclosure to the consumer with the simplest language possible. But we don't want material information to be hidden solely for the sake of brevity.

Privacy notices mean very little unless backed up by a business' actual conforming practices to their notice. We use a unique assessment tool that inquires into a seal applicant's management processes. We ask about personnel policies and training, about their relationship with third parties like agents and contractors. We inquire into physical security and electronic security procedures.

Our annual assessment process offers ongoing help and tailored advice. Actually, we have been told that applying for a seal is like getting a free consulting service. It is good public policy even if it isn't the best business model.

Our program requirements include other important best practices. Consumers must be allowed to opt out of transfers of their personal information to third parties, and they must be given an opportunity to opt in for certain transfers of sensitive data, such as health care.

Seal holder websites must prominently disclose how consumers can raise questions or complaints with the company and with BBB online. They must participate in our dispute resolution program, and they must afford consumers access to personal information at a reasonable cost, not just to allow correction of inaccuracies, but simply to inform them what is being retained and what is retrievable about them. And some companies like Kodak provide instant online access through password-protected profiles.

Protection of online privacy requires a global outlook, so our standards now incorporate the online safe harbor terms negotiated by our government and the European Union. And I am proud to say that EU officials have singled out BBB's program as the most important factor in persuading them that self-regulation could work.

We apply the safe harbor principles also to U.S. transactions and U.S. customers. That is not done by everybody. And we verify compliance with the requirements rather than rely on self-certification.

On June 1 this month, I signed an agreement in Tokyo with the Japan Information Processing Development Corporation to launch the first ever cross-border, online trust mark program—in this case, the reciprocal privacy seal program.

The program, with the encouragement of Japan's government, provides for common privacy standards and recognition of each organization's award of a seal by the other, and it provides a cobranded privacy seal for use on the websites of either country. And

we think this is going to be a very effective way to promote cross-border commerce.

Let me close by recognizing that there is still a large portion of the marketplace that hasn't responded, and it is fair to ask why this is so. One reason, we suspect, is the marketplace is uncertain about the current legal environment. Will there be legislation or not? Will self-regulation technology have a role? What standards will ultimately govern?

Such uncertainty may fuel a reluctance to embrace any particular voluntary self-regulation program. Now, this is not to say that the business community has ignored privacy. Quite to the contrary. But participating in a seal program is a big commitment closely related to predictions about the future legal framework. And, frankly, these predictions simply cannot be safely made at this time.

Thank you for your interest.

[The prepared statement of Steven J. Cole follows:]

PREPARED STATEMENT OF STEVEN J. COLE, SENIOR VICE PRESIDENT AND GENERAL COUNSEL, COUNCIL OF BETTER BUSINESS BUREAUS, INC. AND BBBONLINE, INC.

Mr. Chairman and members of the Committee, my name is Steven J. Cole, and I am the Senior Vice President, General Counsel, and Corporate Secretary of the Council of Better Business Bureaus, Inc. I am pleased to be here to speak with you about the BBB*OnLine* Privacy Seal Program, one of the significant self-regulatory programs of BBB*OnLine*, the Internet subsidiary of the Council of Better Business Bureaus.

The Council of Better Business Bureaus (CBBB) is the umbrella organization for the nation's Better Business Bureau system, which consists of 129 local BBB's and branches and 270,000 member businesses across the United States. The CBBB is a nonprofit business membership organization tax exempt under section 501(c)(6) of the Internal Revenue Code. More than 325 leading edge companies nationwide belong to the CBBB and provide support for its mission of promoting ethical business practices through voluntary self-regulation and consumer and business education.

Each year, millions of consumers contact the Better Business Bureau for pre-purchase information or for assistance in resolving marketplace disputes. In large part, they are drawn to the BBB by its enormous name recognition, reputation, and proven credibility. The BBB trademark is one of the country's most widely recognized by both business and consumers. The public looks to the Better Business Bureau for impartial and reliable information on a broad range of companies, products and services. We offer consumers and businesses a means to resolve disputes through conciliation, mediation and, when necessary, arbitration.

Our name recognition, the extremely high level of trust we have earned from the public, and our experience in operating self-regulation and dispute settlement programs, including our previous experience with offering another seal program in the BBB*OnLine* Reliability Program, are some of the reasons the business community asked BBB*OnLine* to provide a framework for self-regulation in the area of online privacy.

BBB*OnLine* is a 501(c)(6) tax-exempt organization, supported by leading online marketing and technology companies in the United States. A wholly owned subsidiary of the CBBB, BBB*OnLine* was established by the CBBB and its member sponsors as a means to promote the highest ethical business practices online through self-regulation and consumer education and self-help measures, and thereby help to foster consumer trust and confidence in this new market.

To help online companies distinguish themselves, BBB*OnLine* provides two separate seal programs for online businesses--the Reliability Seal Program and the Privacy Seal Program--and provides consumer information through our website, www.bbbonline.org. Both programs emphasize the importance of posting and adhering to a privacy notice that is based on fair information practices which includes notice, choice, access and security. These important privacy notice disclosures provide the consumer with knowledge so that they may understand the company's privacy and security practices before providing any personally identifiable information. BBB*OnLine*'s Reliability Program has developed a Code of Online Business Practices which will help shape the rules of the road for e-commerce, not only for privacy

but for many other aspects of consumer protection. This Code has become an international model for other countries looking to advise their own online businesses on best practices.

The BBB*OnLine* Privacy Program awards seals to online businesses verified as meeting our high standards including: the posting of online privacy policies meeting rigorous privacy principles, completion of a comprehensive evaluation, monitoring and review by a trusted organization, and participation in a consumer dispute resolution system. Our goal as an organization has and continues to be providing education for businesses and consumers on fair and honest practices in the market place.

Our Privacy Program is a logical extension of this objective. The Privacy Program is designed to be a user-friendly tool that helps foster trust and confidence in online commerce and as a resource for business as a simple, one-stop, non-intrusive way to demonstrate compliance with credible online privacy principles.

The core of the BBB*OnLine* Privacy Program:

- Awards an easily recognizable and affordable "seal" to businesses that post online privacy policies meeting rigorous principles, including notice to consumers, disclosure, choice and consent, access, and security;
- Offers a separate and distinct seal for sites directed at children;
- Provides a thorough and consumer-friendly dispute resolution system;
- Monitors compliance through requirements that participating companies undertake, at application and at a minimum annually thereafter, assessments of their online privacy practices; and,
- Takes specific actions for non-compliance, such as seal withdrawal, publicity and referral to government enforcement agencies.

To ultimately qualify for a privacy seal, applicants must successfully complete a comprehensive assessment process that examines all relevant aspects of an applicant's information practices, including privacy notice content and placement, security measures, transfer and merger of information, access, correction; and (if the website or online service falls within our children's guidelines) a comprehensive set of additional children's requirements. Our assessment is an educational tool, providing business with a template on how to institute and maintain a credible regime promoting fair information practices to foster protection of consumer privacy in the online world.

In the 27 months that the BBB*OnLine* Privacy Program has been in operation, we have already gained much valuable experience. The assessment process involves a careful dialog between ourselves and our applicants, and often we find ourselves learning from each other. For instance, in the process of evaluating the information practices of applicants, we find that we are also educating them on the importance of drafting clear privacy policies that disclose with sufficient specificity what is being collected and how that information is being used. We are talking with applicants about the necessity of providing access to and correction of information, and simultaneously, the importance of having in place verification methods for providing access to only those individuals authorized to obtain it. We are educating applicants on security measures, the many issues that arise in clearly defining the scope of the privacy seal protections, and the best way to protect children's privacy. In this way, we believe we are not only certifying websites that follow the BBB*OnLine* criteria, but also greatly raising the bar by giving applicants the time and guidance needed to make them knowledgeable about the issues surrounding online privacy.

In addition to the assessment process, BBB*OnLine* offers consumers and businesses significant experience in resolving disputes. Using BBB's dispute settlement experience, we stand ready to provide consumers with a specialized forum to air and resolve privacy-related disputes. We will accept complaints from both US residents and non-US residents about companies and organizations with posted privacy notices that misuse information or are alleged to have violated posted privacy policies. Complaints can be about the actions of seal participants and non-seal participants. Companies or organizations that do not cooperate with us in a dispute resolution proceeding can, in turn, be subject to public withdrawal of our seal and/or referral to the appropriate government agency.

Both BBB*OnLine*'s Privacy Program and Reliability Program are designed to foster consumer trust and confidence on the Internet and serve as a valuable resource for business as a simple, one-stop, non-intrusive way to demonstrate compliance with credible online commercial practices. As an aid to both businesses and the consumer, BBB*OnLine*'s privacy standards evolve over time to ensure that they incorporate the rapidly evolving changes in this environment as well as important governmental concerns.

As previously mentioned, the Better Business Bureau is well-known for its role in providing consumers with pre-purchase information and this role has become

even more important with the increasing popularity of the Internet. This medium enables consumers to shop from their home computer instead of leaving home to visit a bricks and mortar establishment. The appearance of a BBB*OnLine* seal on a website provides consumers with a user-friendly tool because they can simply click on the seal to confirm a company's participation in one of our programs. This helps increase a consumer's comfort level when shopping online.

BBB*OnLine* also helps businesses educate their own customers. A disclosure-based program both in process and design, BBB*OnLine* seeks to create a transparent environment with no "privacy surprises." We require clear, easy to find, and easy to read privacy notices that contain relevant disclosures. Consumers of a BBB*OnLine* seal holder must be able to rely on the privacy notice, which means it must be available, must be understandable, and must contain those disclosures that consumers need to make informed choices about the collection and use of their own information. Some of the key disclosures required by BBB*OnLine* include:

- What types of personally identifiable information are being collected from them.
- How their information will be used.
- What choices the consumer has regarding the sharing of personal information
- How the consumer can access his or her personally identifiable information to review and/or make corrections.

Recent critical media coverage of the complexity of some privacy notices may miss an important point here—namely, that we have a very delicate balance to draw between full disclosure, which includes "ifs" "ands" and "buts" and definitions because of the complexity and diversity of the state of privacy practices and ground rules in this country, and simpler disclosures that don't tell the whole story. We work hard to strike that balance in reviewing applicant's policies. We lean towards full disclosure, with an effort at using the simplest language possible. But, we don't want important exceptions or clarifications to be hidden for the sake of brevity.

BBB*OnLine*'s website also serves as a great shopping aid for consumers. One of the most popular features is BBB*OnLine*'s searchable database, a resource for anyone seeking out trustworthy online businesses that have been approved by one of our seal programs. The website also provides guidance should a dispute arise between a consumer and a specific company. If necessary, the consumer also has the opportunity to file a complaint against the company. Online shoppers are increasing in numbers and these steps ensure that confidence levels can rise at the same time.

BBB*OnLine* also serves as an educational resource for business, both for those seeking a seal, and those already carrying one. As an integral part of our application and renewal process, BBB*OnLine* offers ongoing help, guidance, and tailored advice for the creation, maintenance, and improvement of sound information policies.

This educational component for business is critical. It is rare for us to receive an application from a business that is already 100% compliant with our program standards. Privacy remains a new and complex enough issue that many businesses are approaching the issue of online privacy for the first time, and still learning how to best protect privacy.

For instance, in our application and review process it may become apparent that new procedures for consumer choice, access, data security, and site design need to be implemented. Privacy notices must often be amended to provide more meaningful and understandable disclosures. Binding promises must be obtained to guarantee the correct use of information.

The interactive process begins with standards that already incorporate many of the best practices laid out by leading industry coalitions, privacy advocates, and government bodies such as the Federal Trade Commission.

One best practice recommended by these groups is the ability of data subjects to not only correct their own information, but also to later access and review their information. This is also a standard requirement of BBB*OnLine*.

Another is the ability of data subjects to discern not only "what" information is being collected, but by "whom." In the increasingly seamless environment of the Internet, which can visually blur the line between data collectors, BBB*OnLine* requires its seal holders to provide specific disclosures when other data collectors are incorporated into a site design, and to provide visual cues and disclosures when there are links to outside parties that may look like part of a seal-holder's site, either because of co-branding, licensed services, or frames.

Likewise, BBB*OnLine* follows recognized best practices by requiring all its seal holders to explain how they can be contacted in the instance there are questions or concerns. Their participation in BBB*OnLine* itself must be disclosed so that data subjects may take advantage of our dispute resolution process.

Seal holders must provide a statement of their commitment to data security. Seal holders must explain whether or not information is shared with outside parties, and

how that sharing can be prevented. These are all reflections of best practices that have been made an express part of the BBB*OnLine* Privacy Program standards.

Equally important, BBB*OnLine* does not limit its inquiry to just the quality and placement of a seal holder's privacy notice. Because privacy notices mean little unless backed up by a business' actual practices, BBB*OnLine* also uses a unique assessment tool that inquires into a seal applicant's management processes. We ask about staff training. We ask about the relationship a seal applicant has with all parties that have access to data, including agents and contractors. We require the creation of internal security logs. We require confirmation of physical security devices, such as doors and locks, in addition to electronic security procedures such as encryption and passwords.

In some cases, the comprehensive, interactive, and educational back-and-forth that leads to the grant of a BBB*OnLine* Privacy seal leads to exemplary information practices that may even exceed BBB*OnLine*'s own standards. Once a business is educated on areas of privacy concern, and given concrete suggestions on how these concerns can be addressed, we find many companies creating even more creative and effective ways to protect online privacy.

For example, BBB*OnLine* requires posted privacy notices that are easy-to-find, and appear at least on every homepage, every page where information is collected and every page that contains an active email address. Many of our seal-holders, such as Xerox, go beyond this requirement and place a link to their privacy notice on virtually every page of their Web site.

BBB*OnLine* requires privacy notices to clearly explain a business' online policies, as well as what online elements may not be covered. A few of our seal holders, such as Tupperware, go the extra step of applying the promises they make in their privacy notices to all information collected (both online and offline) and honor these promises universally for all the company's sites.

BBB*OnLine* requires its seal holders to provide data subjects access to their own information, subject only to reasonable frequency and fee limits. Practically all the BBB*OnLine* seal holders have chosen to provide access and correction free-of-charge, and many, such as Kodak, go the extra step of providing their customers instant access online through password protected profiles.

In addition to these specific examples of good information practices, it has also become apparent that when an organization sets out with a comprehensive approach to privacy, many of the barriers, costs, and challenges imposed by privacy compliance are reduced. There are significant efficiencies realized when a "privacy plan" is implemented across the board from the beginning of an organization's online presence.

When privacy is folded into a corporate culture, new information practices are implemented more quickly, online content and services are more swiftly modified, costs are kept down, and compliance with third party verification services (like BBB*OnLine*) becomes infinitely easier.

In this respect, we have found that one of the most powerful ways to encourage good privacy practices is to empower businesses with the knowledge, tools, and advice they need to make privacy an integral part of their operation.

Based on leading industry standards and an expert privacy panel, the guidance of the BBB*OnLine* Steering Committee, and the 88 year history of the Better Business Bureau system in providing effective self-regulation, the BBB*OnLine* standards continue to provide some of the most effective and relevant standards for privacy.

To maintain our standards as a relevant education tool, BBB*OnLine* has continued to adapt in the face of new regulation and marketplace needs. BBB*OnLine* is able to do this because one of the inherent advantages of a self-regulatory program is this ability to move quickly and remain responsive, which proves especially important in the fast-paced environment of the Internet.

To offer just one example, the BBB*OnLine* Privacy standards were updated almost a year ago to incorporate the safe harbor privacy principles negotiated between the Department of Commerce and the European Union for the adequate protection of information under the European Union's Directive on Data Protection. This program upgrade has allowed BBB*OnLine* Privacy Seal holders to enter the EU safe harbor. Several BBB*OnLine* seal holders, including Hewlett-Packard and Dun & Bradstreet have since gone on to self-certify on the DOC's safe harbor list. Unlike others, BBB*OnLine*'s safe harbor compliance standards are made applicable to US businesses and US consumers—so we have enhanced protection in the US.

As the EU negotiations highlighted, privacy is not purely a North American issue. In the borderless world of electronic commerce, online privacy protection has become a key component of doing business in today's global economy. Various countries have developed their own country or region specific regulatory approaches to privacy. For the US to remain competitive in e-commerce, privacy concerns need to be

addressed. This is another area where self regulatory programs like BBB*OnLine* can help in the global arena to assist business and consumers in promoting sound privacy practices and offer consumers and business a forum for resolving disputes across borders.

In further response to the global marketplace, on June 1 of this year I signed an agreement in Tokyo, Japan with the Japan Information Processing Development Corporation (JIPDEC), the Japanese Government sponsored privacy mark program, to launch the first ever cross border privacy seal program. The program provides for a reciprocal seal which provides US businesses who wish to market online to Japanese consumers with a combined privacy seal, granted by BBB*OnLine*, which incorporates the JIPDEC seal, which is easily recognizable in Japan. This effort will also provide Japanese online marketers, marketing to the US, with the BBB*OnLine* Privacy Seal for use in the US. Once a US company qualifies for the BBB*OnLine* Privacy Seal, it will also automatically qualify for the reciprocal JIPDEC seal. This groundbreaking agreement will help foster e-commerce across borders and also facilitate resolution of privacy disputes that may arise in cross border transactions.

Since BBB*OnLine*'s Privacy Seal Program has been officially "open for business" we have received over 1500 applications from all over the US and from 20 countries, and have awarded seals covering over 800 websites. When you factor in those currently in the application process, there are over a 1000 sites that have either qualified for or are in the process of qualifying for our seal.

The credible nature of our assessment process is illustrated by the number of sites that do not ultimately qualify for the seal. The reason is our program is tough. However, even those sites that go through our process, but do not actually receive a seal, still benefit from learning how to implement good privacy practices. While this has been a good start, unfortunately, the percentage of applicants, compared to the wider universe of websites that could benefit from the program, is still small. Our applicants come from diverse segments of the market place. Our seal holders include high technology companies like Intel, Hewlett-Packard, Dell, Agilent Technologies; communications companies like AT&T and MCI; travel related companies like American Airlines, Union Pacific Railroad and Expedia; major retailers like Lowe's Companies and Fingerhut; entertainment companies like Lucasfilm, Nickelodeon, and Zagat Survey; major trade associations like the American Electronics Association and the Electronic Retailing Association, as well as major multinational firms like Proctor and Gamble and Nestle. When you consider that significant companies like these have all embraced the rigorous standards of the BBB*OnLine* Privacy Program, you can appreciate the large number of consumers that already benefit from our self regulatory program.

Even so, most of the applications we have received have come from small to medium-sized businesses. The BBB*OnLine* Privacy Seal Program was intentionally priced so that companies of all sizes could apply. The only item keeping a company from participating in the program should be its inability to meet the eligibility requirements; price should not be a factor. The World Wide Web is made up of hundreds of thousands of websites, most of which are not large companies. In order for self-regulation to work it must be accessible to the majority of web marketers, large and small companies alike.

However, even while BBB*OnLine* continues to grow, we recognize that there's still a large portion of the marketplace that hasn't responded to our message. One thing that the Committee might consider is why this is so. One reason we suspect is that the marketplace is still uncertain about the current legal environment. Will there be legislation or not? Will self-regulation and technology be deemed the preferred route? What standards will ultimately define widely accepted best practices? Such uncertainty may fuel a reluctance to embrace any particular rush to voluntary programs such as BBB*OnLine*, which is unfortunate, given what we have already accomplished in such a short time frame. This is not to say that the business community has ignored privacy. To the contrary—as we have all seen, it is doing well in posting privacy policies on web sites—but participating in a seal program is a big step, and is closely related to predictions about the legal environment.

It is our hope that as the program grows, and as consumer awareness and education increases, we will have been able to make the online marketplace a safer place to negotiate for all.

We want to thank the Committee for your attention and hope that you share in our enthusiasm for the tremendous progress already made.

I am available to answer any questions you may have. For those individuals that may be reading this document, I have provided a list of website addresses that may help you in further understanding the various aspects of BBB*OnLine* programs.

Mr. SHIMKUS. Thank you.

Next we will turn to Mr. Jerry—is it pronounced DeVault?

Mr. DEVAULT. Yes, it is.

Mr. SHIMKUS. National Director, Innovative Assurance Solutions. Welcome, and you have 5 minutes.

**STATEMENT OF JERRY R. DEVAULT**

Mr. DEVAULT. Thank you. Good afternoon. Ernst & Young is a leader in providing auditing and assurance services around the globe with 78,000 employees based in 130 countries. I will make three points illustrating how privacy practices have evolved and acquaint you with an emerging best practice independent verification.

First, I would note that the mere existence of a privacy policy, even a policy that includes standard components, is not as impressive as it once was. Not long ago the privacy debate centered on whether a website posted a privacy notice. Having a policy and providing notice was the best practice. Privacy policies were once a rarity.

Last year, all of the 100 most popular sites posted such notices, yet concern remained. Notices did not adequately discuss protections or key components emerging as industry standards. In response, industry groups developed self-regulatory policy, standards, and detailed components of the notices.

Seal programs such as BBB online and trustee provided a seal of approval to sites that pledged to include certain requirements in their privacy policies. But with all of the improvement in the quality and quantity of privacy notices, why does public concern remain high? If effective policy practices have been identified and incorporated into policies, shouldn't that be enough?

This brings me to my second point, that promises alone don't earn consumer trust. Today too many consumers don't trust that organizations will follow through on their promises. Providing notice, choice, access, and security will only work if consumers can trust that companies will enforce them.

Leading companies are recognizing that it is not enough to say what they will do with personally identifiable information. Businesses must also prove to consumers that they are doing what they say they are doing. Leading companies now provide consumers and other stakeholders with more assurance about their actions. They are proactively having third parties test their assertions regarding the people, the processes, and the technologies that operate and enforce their stated policies.

This testing requires that a company earn a compliance report as compared to promising to comply with a set of self-regulatory requirements stated on the website veneer. Businesses increasingly looking for a more effective private sector solution to privacy are turning to independent third parties for verification of their practices.

Independent verification is not a new idea. More and more companies undertake independent verification because they realize it leads to enhanced consumer trust, which in turn can result in more loyal customers and a return on their investment. For example, a large international client credits our independent verification services with contributing significantly to its ability to double its online

closing-to-sale ratio and increasing website revenue by more than 45 percent.

In areas where Congress and the executive branch have regulated treatment of sensitive financial and health data, such as Gramm-Leach-Bliley and HPPA regulations, you have required that more than their promises are in place to safeguard consumer information. You have focused on actions, which brings me to my final point.

Since building trust requires more than promises, the mechanism selected to protect consumers should include independent assurance or independent verification. And there are several ways to police or assure compliance with privacy policies: through the courts and increased litigation, through increased powers of the Federal Government, or through government facilitation of private sector solutions to this public policy concern.

Determining which of these compliance measures to employ, whether individually or in combination, is the policy question faced by government and industry. If it is determined that the private sector is the appropriate venue, industry groups simply pledging to meet tailored promises will likely not be sufficient in the eyes of consumers to achieve the goal.

As I previously indicated, companies will need to provide a high level of assurance that its people, processes, and technologies are operating effectively. The auditing profession has developed a set of principles and criteria for online privacy.

The AICPA and the Canadian Institute's Web Trust Program for Online Privacy, which was mentioned earlier in opening remarks, provides a global best practice, a set of generally accepted privacy principles against which companies and self-regulatory groups can interpret and implement policies, procedures, and controls to maintain compliance with online privacy practice standards.

The AICPA standards are the established criteria used by auditing firms globally in more than 13 countries to test that an organization operates in compliance with online privacy assertions.

In conclusion, independent verification is an emerging best practice. Ultimately, just as notices and standard policy components and test seal programs took time to emerge and be accepted into the framework for internet privacy, so will third party independent verification.

The adoption of independent verification as a best practice can provide increased assurance to consumers and to policymakers alike, and, importantly, it can help stave off more draconian governmental measures that could unduly impede private sector initiatives.

I appreciate the opportunity to be here this morning, and I welcome your questions.

[The prepared statement of Jerry R. DeVault follows:]

PREPARED STATEMENT OF JERRY R. DEVAULT, NATIONAL LEADER, INNOVATIVE ASSURANCE SOLUTIONS

I. INTRODUCTION

Good morning Mr. Chairman, and thank you for the opportunity to appear before your subcommittee on the topic of industry best practices in your series of hearings on the important issue of privacy. I am Jerry DeVault, National Leader of Innovative Assurance Solutions for Ernst & Young LLP. As one of the "big five" accounting

firms, Ernst & Young is a leader in providing accounting and assurance services around the globe, with 78,000 employees based in 130 countries. While the Internet revolution has been occurring, Ernst & Young has been adapting to offer our clients a variety of assurance services aimed at assisting our customers in establishing trust with consumers, businesses, and regulators on privacy and trust issues. Our clients include many of the Fortune 500 companies as well as many new and emerging companies. As a result of providing our services to numerous companies, Ernst & Young has a unique perspective on the best privacy practices of various industry sectors. Today, I would like to share this perspective with you, explain how industry practices have evolved over the past several years, and describe our premiere service in this area, the provision of independent third-party verification services.

II. THE MERE EXISTENCE OF A PRIVACY POLICY ( EVEN A POLICY THAT INCLUDES STANDARD COMPONENTS ( IS NOT AS IMPRESSIVE AS IT ONCE WAS.

Not long ago, the privacy debate centered on whether a web site posted a privacy notice. The idea was that consumer concerns would be alleviated if sites merely explained their practices in public notices. At one point, privacy policies were a rarity. However, by last year, according to the Federal Trade Commission's 2000 report to Congress, all of the 100 most popular sites posted such notices.

Nonetheless, consumers and policymakers remained concerned because many of these notices did not adequately discuss protections or contain the key components emerging as industry standards. In response, industry groups began to develop self-regulatory privacy standards detailing the components of the notices. Seal programs such as BBB*OnLine* and TRUSTe began to provide a seal of approval to sites that pledged to include certain requirements in their privacy policies.

Leading businesses also began to undertake other best practices to ensure that their publicly posted privacy notices were being followed. These measures included developing internal procedures and training for employees to follow the requirements of the organization's privacy policies. Additionally, many businesses have empowered a chief privacy officer or other dedicated official to develop and oversee internal compliance processes.

Yet, even with this progress, consumers' and policymakers' concerns surrounding privacy have not been alleviated. The obvious question is: if effective privacy policies are posted on sites that compose the overwhelming majority of Internet traffic, why does public concern remain so high?

III. PROMISES ALONE DON'T EARN CONSUMERS' TRUST

One reason that concerns remain high is that consumers don't trust that organizations will follow through on their promises. Making a declaration to provide notice, choice, access and security will only work if consumers can trust that companies will enforce them.

In the private sector, leading companies are recognizing that it is not enough to *say* what they will do with personally identifiable information; businesses must also *prove* to consumers that they are doing what they say they are doing. Leading companies now find it valuable to provide consumers and other stakeholders with more assurance about their actions. They are proactively having third parties test their assertions regarding the people, processes, and technologies that operate and enforce their stated practices. This additional step of robust testing requires a company to "earn" a compliance report as compared to simply agreeing to comply with a set of self-regulatory requirements stated on the web site "veneer." Businesses, increasingly looking for a more effective private sector solution to privacy, are turning to independent third parties for verification of their practices.

Independent verification is not a new idea in the e-business arena. More and more companies undertake independent verification as a best practice because they realize that it leads to enhanced consumer trust(which in turn can result in more loyal customers and a return on their investment. For example, a large international client credits our independent verification services with contributing significantly to its ability to double its online "closing the sale" ratio and increasing Web site revenue by more than 45 percent. In addition, our clients recognize value in other ways such as differentiating themselves from their competitors and proactively managing the risks of online business.

Even in those areas in which Congress and the Executive Branch have regulated the treatment of particularly sensitive information like financial and health data, lawmakers have required more than mere promises to safeguard consumer information.

Both the Gramm-Leach-Bliley Act and the HIPAA regulations are focused on actions—they require that organizations have appropriate controls and systems in

place to ensure data is handled appropriately. When the Department of Commerce negotiated a Safe Harbor for compliance with the European Data Directive, they required that qualifying companies certify that their practices comply with the Safe Harbor principles. And certain self-regulatory organizations recognize that a promise to follow policies is not enough. When the Network Advertising companies found themselves under regulatory pressure, they wrote into their self-regulatory program a requirement that participating companies undergo independent verification of their privacy practices.

IV. SINCE BUILDING TRUST REQUIRES MORE THAN PROMISES, THE MECHANISMS SELECTED TO PROTECT CONSUMERS SHOULD INCLUDE INDEPENDENT ASSURANCE.

There are several ways to police or assure compliance with privacy policies: through the courts and increased litigation; through increased powers of the federal government; or through government facilitation of private sector solutions to this public policy concern.

Determining which of these compliance measures to employ—whether individually or in combination—is the policy question faced by members of this Subcommittee, the entire Congress, as well as industry. If it is determined that the private sector is the appropriate venue, industry groups simply pledging to meet tailored promises will likely not be sufficient in the eyes of consumers to achieve the goal. As I previously indicated, companies will need to provide a high level of assurance that its people, processes, and technologies are operating effectively.

Much like other areas where we provide assurance regarding business practices, the auditing profession has developed a set of principles and criteria for online privacy that incorporates an effective assurance component. The American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA) WebTrust Program for Online Privacy provides a global best practice—a set of generally accepted privacy principles—against which companies and self-regulatory groups can interpret and implement policies, procedures, and controls to maintain compliance with online privacy practice standards. In addition to being a set of principles and criteria that have been reviewed by leading online privacy organizations, WebTrust is the established criteria used by auditing firms globally to test that an organization's people, processes and technology operate in compliance with online privacy assertions.

Mr. Chairman, members of the subcommittee, widely adopted independent verification as a "best practice" can provide increased assurance to consumers and policy makers alike. It will reduce the need for enforcement and investigation of information practices that could unduly impede private sector initiatives. It will also serve as a mechanism to demonstrate compliance if Congress ultimately finds it necessary to legislate in this area and to assist companies in limiting litigation risks.

V. CONCLUSION

In conclusion, independent verification is emerging as a best practice. Ultimately, just as notices, standard privacy policy components, and seal programs took time to emerge and be accepted into a framework for Internet privacy, so too will independent third-party verification. The adoption of independent verification as a "best practice" can provide increased assurance to consumers and policymakers alike. And, importantly, it can help stave off more draconian governmental measures that could unduly impede private sector initiatives.

I appreciate the opportunity to be here this morning, and am happy to answer any questions.

Mr. STEARNS. Thank you.

Mr. Rotenberg?

## STATEMENT OF MARC ROTENBERG

Mr. ROTENBERG. Thank you very much, Mr. Chairman, Mr. Towns, members of the subcommittee. My name is Marc Rotenberg. I am Executive Director of the Electronic Privacy Information Center. I have also taught privacy law at Georgetown for the last 12 years.

I am grateful to be here today, and I wanted to particularly thank you, sir, for this series of hearings that you have held on the privacy issue. I think it is very important that we are able to have

this opportunity to carefully study this issue, and I appreciate the time that you and the committee members have spent on this.

I would also like to say that while my organization and the privacy and consumer organizations across the country that we work with favor privacy legislation, we hope that you will introduce a bill to safeguard the right of privacy. We also appreciate the important role that technology plays in safeguarding privacy.

In fact, my own group, EPIC, was one of the leading organizations working to make strong encryption tools available to users of the internet so that when people went online they could do so with some assurance that their personal information would be protected. And today on our website we make many privacy tools available so that people will be able to protect their online privacy.

We have never viewed the use of technology and the passage of legislation as an either/or situation. We think they both go together. And I would like to use a simple example that I think will be familiar to many people about how this operates.

Think about the use of the telephone. You pick up a telephone. You don't have to set a privacy setting on the side. You don't have to figure out how much privacy you are going to need for who you are talking to or who—you know, what you might be talking about.

Federal law protects the privacy of that telephone call. It doesn't matter whether you are rich or poor. It doesn't matter whether you know a lot about how telephones work. The Federal law gives everyone in this country strong privacy protection of their communications when they use the telephone network.

Now it is also the case that when new technologies for telephone came along, like the cordless phone, the cellular phone, for example, that created some new privacy issues. And so it was important to incorporate technological safeguards so that your telephone didn't operate like a radio, like a broadcasting device.

And so my point, simply stated, is that I think we need both technology and law to protect privacy. And I think we need it in particular for the internet, because I have to tell you, frankly, what I am concerned about today, you have heard descriptions of some very powerful privacy tools. Some of these I think will work well; some of them not so well.

But I am afraid what we are opening the door to is a form of privacy survivalism, which says to users of the internet, if you are very sophisticated, if you know the difference between 128-bit crypto and 40-bit crypto, if you can change the settings on your cookies, reconfigure your SSL, you can have very good privacy.

But for the rest of you who are still trying to figure out how to set the VCR that is sitting on top on your television so it doesn't keep blinking, you may have some trouble. It is going to be a little bit more difficult for you, and maybe you have to get used to the idea of not having so much privacy.

And that is why we need legislation, because not all of us are going to be able to figure out how to take advantage of these tools. We need them built into the network. People need to be able to use the internet like they use the telephone, with the assurance that their personal information will not be misused, that it won't be used for unrelated purposes, and that their privacy will be protected.

Now, I would also like to suggest for you that as we look more closely at some of these new privacy technologies, it is very important to ask what type of privacy are they providing. If I say to you, for example, that privacy means giving you a notice about how your personal information might be used, and then I develop a technology that puts notices on your computer screens, on your cell phones, which is an interesting problem by the way—if you are relying on privacy notices, what is going to happen to people who begin doing business through their cell phones. They are looking at a little screen and trying to read a notice. That is a real problem.

But maybe I can do it. Maybe I can put notices everywhere. Then the technology looks very good, because the standard that you have set is actually quite low. It is quite easy to put privacy notices on things. If you say, instead, that privacy means being able to limit how information is being used, or being able to see the information about you that is collected, or, where possible, maybe even minimizing the information so it doesn't stay around longer than it has to, than it is a harder problem.

So I think it is very important as we are talking about these two technologies, these new types of technologies, we distinguish between those that genuinely protect privacy and those that simply provide privacy warning labels.

Now, there is another interesting problem here to think about, and I know the members of the committee don't want to overregulate, and they are concerned about leaving the open nature of the internet. And I think that view is widely shared. But there is a bit of an irony here, and that is that in the past privacy legislation has also given individuals safeguards from government.

We have used privacy laws so that when government agents go to private companies they have to satisfy a Fourth Amendment-like standard before they can get access to your personal information that is held by your bank, or held by your doctor, or held by some other institution that may have aspects of your private life that you don't want freely disclosed to the government.

Now, by failing to enact privacy legislation out of concern that you may be burdening industry, you are also failing to establish traditional Fourth Amendment safeguards that have been put in place for a whole lot of other businesses in this country to safeguard the rights of citizens against their government.

My final point is I think it is important when looking at privacy tools to ask this question. Do they provide better protection than could otherwise be provided in law? And in my testimony I give the example which Mr. Markey referred to earlier of the privacy provision in the Cable Act of 1984. Small provision in there, it is like a page and a half. It is one of the most powerful privacy laws in this country, and it gives every person who uses cable television service a lot of privacy rights.

I don't think there is a single product or service that was presented to you this morning that provides as much privacy protection as that provision that was enacted by Congress more than 15 minutes ago. And so while we encourage these technological developments, we think they are very important for the future privacy, we also think that legislation is vital.

Everyone in America should have the right to protect their privacy online, whether or not they can afford these new techniques or whether or not they understand them.

Thank you very much.

[The prepared statement of Marc Rotenberg follows:]

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

I appreciate the opportunity to appear before the Subcommittee today to discuss privacy issues. My name is Marc Rotenberg. I am Executive Director of the Electronic Privacy Information Center in Washington, and I have taught the Law of Information Privacy at Georgetown since 1990.

I'd like to thank the Subcommittee and you, Mr. Chairman, for your continued interest in these issues and for the series of hearings that you have held. The privacy community remains hopeful that when these hearings are concluded you will introduce legislation to safeguard privacy and encourage confidence in the emerging electronic marketplace.

I'd also like to acknowledge the work of the various companies that are appearing today on privacy issues. While we may disagree with some of their approaches, we recognize the ongoing effort to find technological solutions to the challenge of privacy protection.

The focus of this hearing is on "Industry Best Practices and Technological Solutions." This is an issue that has been central to the work of my organization—the Electronic Privacy Information Center—since our first day and was also discussed in our book *Technology and Privacy: The New Landscape* (MIT Press 1997).

While we favor legislation to protect privacy on the Internet, we clearly understand that technology plays a critical role in safeguarding privacy. In fact, we helped organize the online campaign to reform the United States encryption policy so that Internet users could exchange private communications and engage in secure online transactions. And we have worked to encourage the development of technical standards that allow Internet users to safeguard their data and protect their identity. One of the most popular features on our web site are the Practical Privacy Tools page which allows Internet users to surf anonymously, delete cookies, encrypt private messages, erase files, and filter ads.

DEFINITION OF PRIVACY IS CRITICAL

First, it is important at the beginning when discussing any technological approach to privacy protection to have a clear understanding of what privacy protection means. If you say, for example, that privacy protection is simply telling people how you will use their personal information and then you develop technologies that provide notices on web sites, symbols on cell phone displays, or technical standards for computers to exchange information about privacy preferences, you actually do very little to safeguard personal information. All of these approaches simply provide warnings to consumers about how their personal data will be disclosed to others.

But if you understand that genuine privacy technologies actually promote trust and confidence in the online environment, then you will understand very quickly that notices do very little to protect privacy. For example, one of the most important privacy technologies operating on the Internet today is the Secure Socket Layer in Internet browsers that allows two computers connected by the Internet to exchange information securely.

Because of SSL you can enter a credit card number in your computer and a merchant will receive the number and neither of you have to worry that the number will be intercepted as it travels across the Internet. It is a built-in security feature that protects the privacy of the customer's personal information. SSL operates for Internet transactions much like car safety features, such as air bags or seat belts. It provides a basic level of safety that promotes consumer confidence in the use of technology.

The problem today is that too many of the "privacy solutions" are really just warning labels. They do not provide any actual technical safeguard for personal information. There should be good privacy technologies, such as SSL, built into the network and the services provided to consumers.

EVALUATING PRIVACY TECHNOLOGIES AGAINST PRIVACY LEGISLATION

One critical standard for evaluating the various technical approaches to privacy protection is to ask whether they provide at least as much privacy for the consumer

as would privacy legislation. Consider, for example, the privacy provisions contained in the Cable Act of 1984. Under that law, every consumer in the United States who subscribes to a cable television service receives certain basic privacy rights.

Cable providers must provide written notice to subscribers of their privacy rights at the time they first subscribe to the cable service and, thereafter, at least once a year. These notices must specify the kind of information that may be collected, how it will be used, to whom and how often it may be disclosed, how long it will be stored, how a subscriber may access this information and the liability imposed by the Act on providers.

Subject to limited exceptions, the Act requires cable service providers to obtain the prior written or electronic consent of the cable subscriber before collecting or disclosing personally identifiable information. The Act grants cable subscribers the right to access the data collected about them and to correct any errors. It also provides for the destruction of personally identifiable information if that information is no longer necessary. There is a clear Fourth Amendment standard that limits the circumstances under which government may gain access to our private viewing records. Finally, the law sets out a private right of action including actual and punitive damages, attorney's fees and litigation costs for violations of any of its provisions. State and local cable privacy laws are not preempted by the Act.

This is genuine privacy protection that legislation make possible. Short of techniques that provide actual anonymity, I don't believe there is a single proposal presented to you today that provides the same level of privacy protection for consumers as the Cable Act that was passed by the Congress more than 15 years ago.

## NEED FOR LEGISLATION REMAINS

Over the past thirty years the United States Congress has done a good job developing legislation to safeguard personal privacy even as new technologies have emerged. We have laws to protect the privacy of telephone calls, video rental records, automated health records, and more. And just this past week, the Supreme Court made clear that simply because there is new technology for surveillance does not mean that we must sacrifice our right to privacy.

The problem is clear. Data collection by commercial firms has become more intrusive as more commerce has moved online. The Internet advertising industry, for example, believes there is nothing wrong with creating an online profile of where you go on the Internet as long as they give you the chance to "opt-out." You won't know who is profiling you. You won't be able to see what is collected about you. And you won't know how this information affects your ability to buy goods and services online.

And it is going to get worse.

The interview that appeared in US News and World Report this week with a former industry insider is particularly revealing. An expert in business practices and privacy audits Larry Ponemon told US News that customer profiles, containing detailed personal information typically have an 85% error rate. "As an auditor," he said, "you reach the conclusion that it's pretty awful out there." When asked what the bottom line is for consumers, he answered:

> Most companies don't take privacy seriously. The general view is: Collect as much data as you can, as quietly as possible. It's dirt-cheap to store, and you never know when it will come in handy. I still use the Internet, but I'm more cautious. I won't share any medical data or do financial planning online. I'll use my credit card only if I think the privacy policy is reasonable, but I assume the worst.

## LOOKING AHEAD

It would be tempting to say that industry is developing good solutions, that more needs to be done, and that it is premature to legislate, but I believe this is a shortsighted assessment of what is currently taking place. In the absence of clear standards set out in statute, privacy is being redefined from a set a basic rights to a series of warning notices. The bottom line is that consumers are being asked to trade their privacy when they go online. The companies post privacy policies that are incomprehensible and easily changed.

It doesn't have to be this way. Congress can pass good privacy legislation, similar to the provisions contained in the Cable Act of 1984, and still encourage the development of technological solutions. This is the right way to go. We will need both good technology and good legislation to safeguard privacy in the years ahead.

I appreciate the opportunity to appear before the Committee today and will be pleased to answer your questions.

**References**

Phil Agre and Marc Rotenberg, eds., *Technology and Privacy: The New Landscape* (MIT Press 1997)
EPIC Practical Privacy Tools[http://www.epic.org/privacy/tools.html]
EPIC and Junkbusters, "Pretty Poor Privacy: An Assessment of P3P and Internet Privacy" [http://www.epic.org/Reports/prettypoorprivacy.html]
Privacy Coalition [http://www.privacypledge.org]
Privacy Site [http://www.privacy.org]
Marc Rotenberg, *The Privacy Law Sourcebook 2000: United States Law, International Law, and Recent Developments* (EPIC 2000).
Marc Rotenberg, "Can We Keep a Secret?" *American Lawyer* 57 (January 2001).
Paul M. Schwartz, "Internet Privacy and the State: Charting a Privacy Research Agenda," 32 *Connecticut Law Review* 815 (Spring 2000)

Mr. STEARNS. I thank you for your opening statement. You probably listened with interest to the preceding panel, and particularly Microsoft when they talked about their P3P, in effect that it is a default information privacy standard. Now, I suspect that some of you would disagree and some of you would agree with that.

Let me start with Mr. Hughes. What do you think of the P3P as a default information privacy standard? Do you agree or not?

Mr. HUGHES. Absolutely. The company that I work for, Engage, actually was one of the companies that was involved in the development of P3P. And the cookie management features that you heard about in the Microsoft browser are a result of some early work that Engage had done, our co-founder had done, on something called trust labels.

So from the perspective of my company, we definitely have been very involved in the development of P3P and cookie management features.

Mr. STEARNS. But Mr. Rotenberg I think made a very good point in terms of talking about the Cable Act of 1984, and this one and a half page document which outlined the privacy provisions dealing with your cable. And I think he makes a pretty good case that that same standard has to be applied to the internet. Do you disagree?

Mr. HUGHES. I think there are difficulties on the internet. I think the internet, as a global medium, requires a standard that has comparable ubiquity. And that standard is technology. And by embedding the privacy protections in the technology, you provide the greatest coverage possible. So I believe that the browser is the right place to put those tools.

Mr. STEARNS. So you are saying that you think government has a role to do something like we did with the Cable Television Act of 1984 or not? Just yes or no.

Mr. HUGHES. The Network Advertising Initiative is definitely open to the possibility of Federal legislation. However, we would request or push for or suggest that a safe harbor for self-regulatory regimes that are operating and functional and meaningful, like the NAI self-regulatory regime, be put in place.

Mr. STEARNS. Mr. Cole, you know, he makes the analogy, you pick up your phone and you don't think about privacy, but you already have the privacy in place unless you go to the Fourth Amendment that the government can't get involved and listen to your phone calls—you know, tap into your phone.

Do you agree that we need a privacy bill, an internet privacy bill here in Congress, much like we did for the Cable Act of 1984?

Mr. COLE. I would like to respond to that in two ways, Mr. Chairman.

Mr. STEARNS. Sure.

Mr. COLE. First of all, I am not sure it is as clear-cut as Marc would have it. I used to run Maryland's Consumer Protection Program for the Attorney General, and I remember that it depended often on State law whether or not you actually had all of the privacy you wanted on those phone calls. So it is a very—it is complicated, and it is not as clear. And I am sure the internet——

Mr. STEARNS. Well, I am sure the details of it—but as a broad scope——

Mr. COLE. Well, it is not so clear that we have perfectly legislated privacy, even of those areas where we tried. And there may be a lesson about that. Either we need better legislation or maybe legislation doesn't always work. But let me get also to your question.

Our organization, simply as a matter of policy, does not take position on legislation. Self-regulation could work without legislation. We could help promote voluntary standards for the business community in the absence of legislation, and we could help provide compliance when there is legislation.

I would like to endorse the point made earlier—if there is legislation from the Congress, you should follow the lead that you took with the children's online privacy and in other legislation, and there really should be a safe harbor for voluntary efforts of compliance.

Mr. STEARNS. Mr. DeVault, can you give us a scope of the number of companies Ernst & Young provides privacy service for, and how much revenues does the privacy protections practice take in for your company? And what are the typical ballpark costs for such services? Is that possible, to get this in a broad way?

Mr. DEVAULT. Well, we are, as I mentioned, a global firm. We have thousands of people that are focused on security, privacy, and IT risk advisory services.

Mr. STEARNS. Why don't we just take it in the United States.

Mr. DEVAULT. In the United States, we have approximately 800 to 1,000 people that are, and that employs—obviously, it keeps those people busy. That gives you a degree of the fees that we have out of that business.

Mr. STEARNS. So of the revenues in the United States, is this—I think what we are—in the committee we are starting to realize that this is a whole new area of revenue generation, and that it could be a large segment in the future. When you move to broad band, people will come to you, and so this—what I think is an incipient industry which is going to create a great deal of profit for people like yourself and others.

Mr. DEVAULT. Well, to give you an idea, the web trust principles that I mentioned earlier were released on September 6, 2000. So they are very young, so our independent third party verification services are very nascent as well. We have been helping companies with their privacy policies and compliance now for several years, since really the advent of the commercialized internet.

And we see that this is a large business for software companies, for marketing companies, for professional services companies.

Mr. STEARNS. Do companies tend to overpromise and underdeliver in the privacy area? Mr. DeVault, how many companies

have failed Ernst & Young initial verification tests, if any? How many have failed a followup verification test?

Mr. DEVAULT. At this point in time, we have certified as a profession less than 10 companies. As I said, it is a very new area for us. I would say, though, that every time we test there are gaps between our criteria and the actions that we see, and the good news is that we have clients that are interested in filling those gaps, and we are helping them do that.

I think on a go-forward basis we will see what the experience is in terms of testing as we go through. Our testing is required every 6 months.

Mr. STEARNS. Mr. Rotenberg, I think what you are sort of saying is trust but verify, and the government has to verify in some way by setting up a standard so that the public feels comfortable.

After listening to the first panel, were you impressed, though, that Webwasher—the type of things they can do, and that maybe if that was part of an integral part of a web browser that the legislation would be maybe not required as much but it would help to alleviate the problem?

Mr. ROTENBERG. Well, I think there were a number of good approaches suggested on the first panel. And none of them I think would be incompatible with privacy legislation. In fact, I rather suspect that privacy legislation can provide a foundation that builds support for a number of these techniques. I mean, this has always been our view, that you should have legislation that enables strong tools for privacy.

If you don't have the legislation, I think that is really ultimately the decision that this subcommittee will have to make. And if you say we are going to rely on these techniques and hope this works, I think you are going to head toward a world where people, in effect, will turn to their telephones, know that there is no real legal protection there, and have to figure out, in effect, what are the privacy settings right now? Are the settings appropriate for the call I am about to make? Do I need to purchase a little bit more privacy because this call is particularly sensitive?

And you can imagine that that would evolve in the marketplace. But I think over the long term people would be less willing to use the telephone, because there will be no baseline protection established in law that safeguards privacy. So I really think that the best outcome is one that provides that baseline assurance to everybody that privacy will be protected and allows people to innovate and develop better techniques and take it forward. I think that is the win-win outcome here.

Mr. STEARNS. Yes. My time has expired.

The ranking member, Mr. Towns, is recognized.

Mr. TOWNS. Thank you very much, Mr. Chairman.

Let me begin with you, Mr. Rotenberg. And let me say I was very impressed with your testimony. I want to say that before I ask this question.

Mr. ROTENBERG. Thank you, sir.

Mr. TOWNS. You heard on the other panel, I think it was Mr. Schwarz who said that, yes, eventually we need to pass legislation, that laws should be in effect, but we do not know enough now to do it. What is your response to that?

Mr. ROTENBERG. Well, I would be happy to give him a couple of copies of my books, but I think he has left the room. I mean, I have been teaching privacy law for, you know, I said more than 10 years. I have got a 500-page book that surveys privacy law.

I think that Congress has done a good job over the years. I mean, it was done for telephone. It was done for cable service. It was done for electronic mail. There are a lot of good principles in place, and I think we just need to take advantage of them.

Mr. STEARNS. Could we just have those two books brought up to Mr. Towns and just let him quickly have access to them? And then we will give them right back.

Mr. TOWNS. So the theory in terms of waiting and learning more is ridiculous.

Mr. ROTENBERG. Well, I don't see the benefit of waiting. I see the caution about not passing legislation that creates problems that might discourage innovation. But I do believe that legislation can promote innovation, and that is the approach I hope to end up with.

Mr. TOWNS. Yes. I was around in terms of the cable bill and also the Telecommunications Act of 1996. And, of course, we heard—some of the same arguments that are being put forth now were put forth at that time, that we should not move forward with the Telecommunications Act because things are just moving too quickly, we need to wait and see.

But I don't think they are going to slow down. I think they are going to continue to move. And I agree with you. I think at some point in time that we have to come forward with some legislation in order to make certain that the consumer is protected. The question is in terms of, you know, how quick we do it. I think that is something that we are dealing with.

But, here again, we are having a lot of hearings, and I think we are collecting information. And then I hope that when we do do it that we do not hurt a lot of folks. I think that we want to help people, and that is the key.

The other issue is that, you know, what do we do with the little folks out there that are providing information, that is basically all they are doing. And this is, you know, their business, and if we pass laws that a lot of them could be put out of business. I mean, have you thought about that at all?

Mr. ROTENBERG. Well, I think we need some standards in place about how personal information is being collected and used. I mean, I am concerned about these information brokers, for example, that are getting access to a lot of very private details. You know, and that stuff is being repackaged and sold. There is a debate, as you probably know, taking place right now about whether or not all court records should be put online.

Now, public trials in open courtrooms is critical to the democratic system. But if you put in all of the information in depositions, including, you know, psychologists who testify in child custody cases, I mean, this has enormous implications for personal privacy.

So I think we need to have, you know, a rule that will apply to everybody—I mean, the big folks and the little folks.

Mr. TOWNS. Okay. Mr. DeVault, you talked about in terms of the verification, and what are some of the things you think we should

do in order to verify whether or not a person is actually—the consumer is protected?

Mr. DEVAULT. One of the things we do is we go much further than, as I said, the veneer of the website. We really look past just asking questions. And if a client is saying that they are protecting data, we actually look at the data base, the machine that the data resides on within that data base.

We determine whether it is approachable from the outside, so we actually get into the process, we put together a robust set of tests that we can then opine on and say that we believe that that data has been protected in accordance with their policies. And that is a level of testing that is much different than I think people recognize has been occurring.

Mr. TOWNS. Yes. In your audit, they failed to come up to standards. At what point in time would you say, okay, we are not dealing with you anymore? I mean, how do you do that? I mean, what do you do with this? I mean, I am not clear. It is not clear to me what happens here.

Mr. DEVAULT. Well, if a company has engaged us to provide them with a certification or an audit, and they are granted that opinion, they can post a seal on their site which clicks to our report, and a report from management that says we assert that we are holding these promises to be true, and a report from Ernest & Young which says that we have tested those assertions.

If they fail to continue to maintain that posture, we will take our report away. And so there is a consequence at this point in time because it is voluntary. There isn't a signal necessarily to any kind of a regulator or the government or somebody else, other than the fact that if they had, in the past, disclosed that they had passed the test, and afterwards decided to not pass or fail, then our reports would come off their website.

Mr. TOWNS. Thank you. I yield back. I don't have anything to yield back, do I, Mr. Chairman? I am out of time.

Mr. STEARNS. All right. Thank you, Mr. Towns.

The gentleman from Illinois, Mr. Shimkus?

Mr. SHIMKUS. Thank you, Mr. Chairman.

Mr. Rotenberg, you mentioned the Cable Act. I wasn't a Member of Congress during that time. Can you tell me what the cable industry was doing at that time to warrant this page and a half on privacy that obviously you are very supportive of?

Mr. ROTENBERG. Well, it is very interesting, sir. I have actually studied the period. In the early 1980's when cable television was being developed, people talked about it in a very similar way that they talk about the internet today. You are going to do online banking, you are going to be like watching a football game and answer a poll question about what the next, you know, play should be called.

People had a sense when cable television was being developed in the early 1980's that it had interactive capability. And there was consensus—and this is the key answer—there was consensus then with the industry and with Congress that because of this interactive capability, because of the ability now with the television to collect information from the viewer, which didn't previously exist

because it is a broadcast medium, that privacy safeguards should be established.

And privacy safeguards, as I said, were very good, and I don't believe that the cable industry in 1984 opposed them. So when I come before you, sir, and testify and say basically that I think people today for the internet should have similar protections, it is partly because of this experience 20 years ago that when faced with a very similar issue I think Congress did the right thing, and I think it has worked out.

Now, people can say, well, you know, cable television isn't doing all of those things that the internet might, but the privacy is there.

Mr. SHIMKUS. I appreciate that historical look. But at the time of the Act, the cable industry was not doing that. That was just a forward-looking——

Mr. ROTENBERG. Yes.

Mr. SHIMKUS. [continuing] response based upon what they saw, the evolution. And as we see now, cable now is moving in that shape or form somehow with interactivity, which is very similar to high-speed internet service or the broad band debate, and the like.

Obviously, last year we also talked about, debated, and passed the electronic signatures and electronic records issue. Because of that, we are transmitting actual legal documents, signed, you know, through the vast unknown. We should still be doing that, shouldn't we?

Mr. ROTENBERG. I am sorry. Transmitting authenticated documents?

Mr. SHIMKUS. Yes.

Mr. ROTENBERG. I think so. I mean, I think the Digital Signature Act provides some benefits for online commerce. That is clear. But I don't think it resolves the privacy issue. I mean, I think the privacy issue is still out there.

Now, I will say it was addressed in part by the past Congress in the Children's Online Privacy Protection Act. And there you looked at the situation involving kids under the age of 13 and said, well, it would be nice for kids to be able to go online and use some of these new services, but there are justifiable concerns about the collection of their data. And so you had legislation there to protect, you know, the privacy, so I think that went part way.

Mr. SHIMKUS. I would like to turn to Mr. Cole and ask, in reference to the compliance monitoring that you are attempting to accomplish, first, the question is, how is that—first of all, how is that going in that? And then I am going to really then switch to Mr. DeVault to—in his testimony he talked about the questions of compliance monitoring.

Mr. COLE. Yes, sir. We were talking earlier about trust and verify. The Chairman mentioned that. And I want to make an important distinction. Setting standards, whether it is a voluntary organization doing it or the Congress doing it, it is very different from verification, and we all need to take that into account because finding out whether or not there really is compliance with the standards requires a whole other set of techniques than just writing the standards.

What we do is—I referred to it in my brief remarks is we use a unique assessment device that over a period of weeks brings the

company through a series of questions that are geared to determine whether it has set up the internal processes it needs to comply with the promises it makes in its privacy promise, whether it is training of staff in security techniques within the company, and contracts with agents and contractors with whom they may have to share information. So we work with the company on the details of how it is implementing its privacy policy.

Over the 2 years we have been running our program a few hundred companies have failed to meet our requirements after applying. They either decided they did not choose to meet them, or we found that they were unable to meet them. We have not had a need to withdraw a seal from a company that we granted one to, and that is not surprising, because they have gone through an intense process. They verified their procedures, and they are willing to make corrections when we call it to their attention.

Mr. SHIMKUS. Mr. Chairman, can Mr. DeVault respond?

Mr. STEARNS. Sure. Go ahead. We will probably go another round here, so——

Mr. SHIMKUS. Based upon the auditing aspect, you are probably auditing some that have the seal and some who do not. What is your—can you just give some input on that?

Mr. DEVAULT. I would just say that I think there is a bit of expectation gap between what some of the seals may mean to a consumer and what they are intended to do and what they describe in the practices—what they are doing. And that has been seen in some of the issues that have come up onsites that have had seals on them.

We do see that there is some gap between the promises that are being made and the actual actions within the people, the processes, and the technologies, the real behind-the-scenes processes. But I think that companies that are subscribing to these seal programs really want to have good privacy policies.

Many of them are engaging us to come in and help them, make sure that they can qualify for those seals, and then I think that they are determining whether they want to go further and make a public declaration of their compliance with that. And that is what we are seeing in this next stage.

It is really an evolution from just making a policy that has been read on a website to one that has been read and conforms to some kind of a standard, and there is some inquiry as to whether or not they are really doing what they say they are doing, to the final step, which is some proof that says I have engaged somebody independently to come in and really robustly, in essence, rip my processes apart and determine whether or not they are actually working.

And there are companies that are using that, not necessarily just for a marketing purpose, but they are doing it as a good internal practice, not publicly mentioned, as a risk management approach to determine that the promises they are making are promises that are kept.

Mr. SHIMKUS. Thank you. And I yield back, Mr. Chairman. Thank you.

Mr. STEARNS. Yes. I am just going to close here, and anyone else can close with a question or two. Dealing with what is called legacy

data—and, Mr. Cerasale, this might be approach for you. AT&T came in, and I was talking with them about my cell phone.

And I said to them, "When I delete a—when my answering machine comes in on my cell phone and someone calls me and then I delete it, where does it go?" And they said, "To a hard disk." And I said, "Well, how long do you keep that?" they said, "The law has not determined how long." And I said, "Are you going to keep it a year?" They said, "Well, right now, we are not keeping it very long. We almost arbitrarily—in 30 days we get rid of it. But there is a possibility we might have to keep it a longer period of time."

So that goes to the point that if we today passed a bill, what happens to all of the information that has been collected? And how do we write a bill to allow today a U.S. citizen who has all of their credit cards and all of this legacy data protected? How do you do that? And is there much of that that you think that would be a problem?

Mr. CERASALE. Well, keeping data is expensive, and, of course, that is going to go—that will drop in time. But part of the marketing process is that customers can go pretty freely back to marketers they have dealt with before, and they have information already on file, and so forth, that they use and it can go quickly.

For example, purchasing online through Travelocity, I don't have to enter a lot of data because it is already held in there, including my credit card number. I think that the thing that we have to focus on in this part of privacy, which I think in the first panel we discussed security versus privacy, I think the phone legislation is basically the security of talking.

But if I call a catalog and give them my name and, therefore, address and credit card number, so that they have it, and then it goes to their privacy policy, it is totally outside of that phone law, the law concerning telephones. You have to—it is a problem that we do through self-regulation on anything that you have already before. And if you go, therefore, and change a privacy policy or have something different, what do you do with the information beforehand? Is it expensive to mark that data so that you treat it differently than others?

Part of the situation that we look at is markers would hold, in a sense, legacy data—is a customer, to try and see if they can deal with that customer and how long it is to hold an expense.

Mr. STEARNS. How long do you hold information?

Mr. CERASALE. Well, DMA is not a marketer. It is an association. So each——

Mr. STEARNS. Well, I mean, your account, your clients.

Mr. CERASALE. The client——

Mr. STEARNS. Just on the average.

Mr. CERASALE. Members will hold information—I don't think there is any member that would hold customer information beyond 5 years, and that is probably less—it is probably less than that because you have to try—20 percent of Americans move every year. A phone number is good for only maybe 7 years, so that information gets stale and it is useless after a certain amount of time.

Mr. STEARNS. Mr. Rotenberg, you know, if I want to look at my credit report I can do that. Do you think there should be a way for a consumer to take an active hand in tracking his or her personal

data in the marketer's data base, be able to access and go in and to, you know——

Mr. ROTENBERG. I think so. I think in particular where personal profiles are credited. I mean, the issue of access obviously is a question about how far do you go. Congress said 30 years ago if there are companies out there that are creating these reports that are being used for credit determinations, people should have the right to see those reports to make sure they are accurate.

Now, if it is, you know, a single purchase, I think people would say, well, maybe it is not so important. But what is happening on the internet, and particularly with online advertising, is companies are creating these profiles using cookies very much like credit reports. But they don't have the same obligation to tell you what is in that file about you, and you don't know how that information is being used.

So I think the right of access to the profile would do a lot to allow the individual to figure out how that data is being used. It would keep the companies more honest. They could still collect it. The Fair Credit Reporting Act doesn't say you can't collect the information, but it does make the company accountable to the person.

Mr. STEARNS. Where would I go today to find out if somebody was doing a composite of my personal information?

Mr. ROTENBERG. I don't know the answer to that, sir.

Mr. STEARNS. Does anyone know? Where would you go if—you know, if I wanted to find who had a composite of my information?

Mr. CERASALE. A great deal of information—marketing information is held by the credit bureaus on the marketing side, and all of them—all three major credit reporting companies have—you go to them and see what they have in their marketing side on them. And they all have that ability today.

Mr. STEARNS. I want to thank the second panel for your participation, and we know how busy you are, and also for waiting through the first panel. And this is the—we have one more internet privacy hearing, I think in July, but your participation has been very helpful, and we look forward to perhaps in the future calling you back—or calling you just with any additional questions.

Thank you very much. The subcommittee is adjourned.

[Whereupon, at 1:14 p.m., the subcommittee was adjourned.]