United States.

ELECTRONIC COMMERCE: THE CURRENT STATUS OF PRIVACY PROTECTIONS FOR ONLINE CONSUMERS

key

HEARING

BEFORE THE

SUBCOMMITTEE ON TELECOMMUNICATIONS, TRADE, AND CONSUMER PROTECTION

OF THE

COMMITTEE ON COMMERCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTH CONGRESS

FIRST SESSION

JULY 13, 1999

Serial No. 106–39

Printed for the use of the Committee on Commerce

U.S. GOVERNMENT PRINTING OFFICE
58–511CC WASHINGTON : 1999

For sale by the U.S. Government Printing Office
Superintendent of Documents, Congressional Sales Office, Washington, DC 20402
ISBN 0-16-059396-4

COMMITTEE ON COMMERCE

TOM BLILEY, Virginia, *Chairman*

W.J. "BILLY" TAUZIN, Louisiana
MICHAEL G. OXLEY, Ohio
MICHAEL BILIRAKIS, Florida
JOE BARTON, Texas
FRED UPTON, Michigan
CLIFF STEARNS, Florida
PAUL E. GILLMOR, Ohio
Vice Chairman
JAMES C. GREENWOOD, Pennsylvania
CHRISTOPHER COX, California
NATHAN DEAL, Georgia
STEVE LARGENT, Oklahoma
RICHARD BURR, North Carolina
BRIAN P. BILBRAY, California
ED WHITFIELD, Kentucky
GREG GANSKE, Iowa
CHARLIE NORWOOD, Georgia
TOM A. COBURN, Oklahoma
RICK LAZIO, New York
BARBARA CUBIN, Wyoming
JAMES E. ROGAN, California
JOHN SHIMKUS, Illinois
HEATHER WILSON, New Mexico
JOHN B. SHADEGG, Arizona
CHARLES W. "CHIP" PICKERING,
Mississippi
VITO FOSSELLA, New York
ROY BLUNT, Missouri
ED BRYANT, Tennessee
ROBERT L. EHRLICH, Jr., Maryland

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
RON KLINK, Pennsylvania
BART STUPAK, Michigan
ELIOT L. ENGEL, New York
THOMAS C. 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

JAMES E. DERDERIAN, *Chief of Staff*
JAMES D. BARNETTE, *General Counsel*
REID P.F. STUNTZ, *Minority Staff Director and Chief Counsel*

SUBCOMMITTEE ON TELECOMMUNICATIONS, TRADE, AND CONSUMER PROTECTION

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

MICHAEL G. OXLEY, Ohio,
Vice Chairman
CLIFF STEARNS, Florida
PAUL E. GILLMOR, Ohio
CHRISTOPHER COX, California
NATHAN DEAL, Georgia
STEVE LARGENT, Oklahoma
BARBARA CUBIN, Wyoming
JAMES E. ROGAN, California
JOHN SHIMKUS, Illinois
HEATHER WILSON, New Mexico
CHARLES W. "CHIP" PICKERING,
Mississippi
VITO FOSSELLA, New York
ROY BLUNT, Missouri
ROBERT L. EHRLICH, Jr., Maryland
TOM BLILEY, Virginia,
(Ex Officio)

EDWARD J. MARKEY, Massachusetts
RICK BOUCHER, Virginia
BART GORDON, Tennessee
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
ELIOT L. ENGEL, New York
ALBERT R. WYNN, Maryland
BILL LUTHER, Minnesota
RON KLINK, Pennsylvania
THOMAS C. SAWYER, Ohio
GENE GREEN, Texas
KAREN McCARTHY, Missouri
JOHN D. DINGELL, Michigan,
(Ex Officio)

CONTENTS

ELECTRONIC COMMERCE: THE CURRENT STATUS OF PRIVACY PROTECTIONS FOR ONLINE CONSUMERS

TUESDAY, JULY 13, 1999

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

The subcommittee met, pursuant to notice, at 10 a.m., in room 2322, Rayburn House Office Building, Hon. W.J. "Billy" Tauzin (chairman) presiding.

Members present: Representatives Tauzin, Stearns, Gillmor, Cox, Deal, Largent, Cubin, Rogan, Shimkus, Pickering, Bliley (ex officio), Markey, Boucher, Gordon, Eshoo, Luther, Sawyer, and Green.

Staff present: Paul Scolese, professional staff member, Elizabeth Brennan, legislative clerk, Andy Levin, minority counsel, and Bruce Gwinn, minority counsel.

Mr. TAUZIN. The subcommittee will please come to order. Today the subcommittee will hear testimony on the current status of privacy protection for online consumers. When this subcommittee held a hearing last year on Internet privacy, the effort by industry to create a self-regulatory scheme was still in its infancy.

We heard what the industry planned to do in the coming months and also criticism that industry was not doing enough and that government regulation on privacy might be needed. Let me say categorically that it will not necessarily be how the Internet is taxed. It will not necessarily be how much money flows in electronic commerce. It will certainly be how secure electronic commerce is for consumers and for businesses who wish to deal with them over the Internet. It will most certainly be how much privacy is respected and protected on the Internet that will determine the future of electronic commerce as a vibrant and important part of our Nation's economy. It is our hope that we use this hearing today to gauge just how much progress we have made in protecting online privacy since last year's hearing. Today's dialog should allow us an opportunity to see where efforts have been successful and where efforts have fallen short. I am hopeful that we can have a healthy debate on whether or not we need government regulation or is the threat of government regulation enough to further progress in the industry.

I am pleased that we are having the FTC testify before this subcommittee again. The work that the FTC has done on this issue

has been excellent. We look forward to hearing the recommendations they will make today in public. I know from reading an advanced copy of the testimony that the FTC is not recommending legislation at this time to protect online privacy. We will also be hearing from a number of private sector witnesses who will speak about industry's efforts to protect the privacy of their customers. We will also hear from industry observers who will speak on the issue of self-regulation versus government legislation or regulation.

Last Congress, I introduced H.R. 2368, the Data Protection Act, which would establish voluntary industry guidelines to limit the collection and use of personal information obtained by the Internet. I believed that a private sector approach was best, and I still believe that. As a witness to the ever changing technological advances, enacting government regulations at that time would more than likely have been too inflexible for the rapidly changing electronic commerce industry.

Is that true today? Today's hearing will perhaps give us that answer. The Georgetown Internet privacy policy study which was just released in May gives us a good indication of how far industry has come in self-regulation. I think that the numbers are very encouraging, although there is still more that the industry can, should, must do.

One area that has not been much discussed is how consumers can gain more control over their own personal information and then release that information only when they believe they will receive some benefit in exchange for that information. It is obviously true that some of the software industries are producing software products that would, in fact, enable consumers just that power over their own information. As I stated before, personal information does have value.

In fact, as the Internet has grown, e-commerce has grown. There is more value in data bases now than there are in the company assets themselves. Recently, a company announced that they would give free computers with Internet access to the first 10,000 individuals that applied. In the first few days, over a half million people applied for one of those computers. The only catch was that the applicant had to fill out a very detailed application revealing personal information such as what type of automobile they drove, which magazines they subscribed to; in effect which purchases they liked to make. I think this shows that when consumers get something of value in return, some people are willing to part with detailed personal information.

Before I close, I want to thank all of our witnesses this morning for agreeing to testify on this most important issue. My friend, Mr. Markey, has just arrived. He and I have dedicated ourselves to ensure, along with the chairman of the full committee who is also with us today, that our committee will address thoroughly the issue of online privacy, the privacy of individuals' information, the security of e-commerce for our future. This will be an important step in that effort. We look forward to hearing the testimony today. The Chair yields back the balance of his time, and I welcome and recognize as the ranking minority member, Mr. Markey, from Massachusetts.

Mr. MARKEY. Thank you, Mr. Chairman, very much. I would like to commend you for calling this hearing today on the subject of online privacy.

This hearing coincides with the release of a privacy report from the Federal Trade Commission which reflects the results of an online survey conducted earlier this year by Professor Mary Culnan at the Georgetown Business School. In its previous report to Congress, the FTC articulated a number of core principles for implementing fair information practices in the online environment in order to establish key protections for consumers. The Georgetown survey searched for these key privacy criteria which are comprised of the following items.

Notice, ensuring that consumers receive clear conspicuous notice of the personal information practices of the Web site.

Choice, giving consumers an effective means granting or denying consent to the privacy practices of the Web site.

Access, ensuring that consumers could gain access to the information collected by a Web site for correction and information on whether personal data has been reused, disclosed, or sold and to whom.

And security, ensuring that information collected by a site has reasonable safeguards to protect security and integrity of the personal data.

And five, contact information, ensuring that consumers have a convenient method by which to contact the Web site manager with questions, suggestions, and complaints.

The survey conducted at Georgetown found that less than 10 percent of sites collecting personal information had privacy policies embodying these fair information criteria. Just 10 percent. This survey is quantitative. It doesn't even measure the quality of the notice disclosure or so-called opt-out or opt-in features.

Any privacy policy that doesn't incorporate these key elements for consumers is a failure. The survey has found that only a very small minority of sites have implemented these key privacy elements. The industry as a whole continues to get a failing grade.

The question remaining is how much credit people are willing to give companies for merely taking the course while they fail the subject matter. There is no question that consumer concern over privacy has clearly heightened awareness of the issue in the online business community.

The fact that many web sites are at least posting their privacy policies is an improvement. Even in a failing group, there is still some star pupils. I want to commend those companies and individuals associated with online privacy initiatives, seal programs such as TRUSTe and BBBOnLine as well as the growing number of companies taking steps to better inform consumers and offer comprehensive privacy protections on their own initiative.

I think it is increasingly clear that we need a basic level of privacy protections for all Americans online. I believe that there is a role for a privacy marketplace and a role for industry self-regulatory initiatives. No American, however, should be left without any privacy protection in the online environment.

In my view, we should pursue a legal framework which should:

1) incorporate elements of industry self-regulation, 2) allow technological tools to enhance privacy, and 3) guarantee basic government-backed protections.

Less than 2 weeks ago, the House passed H.R. 10, the Financial Services Act. This legislation includes privacy provisions which purport to provide consumers with the core principles, but with some huge loopholes that must be addressed in conference.

For instance, we need to address the failure to provide consumers with notice and the right to say no when a consumer's information is disclosed to affiliates within a bank holding company rather than an unaffiliated third party. This artificial distinction between affiliates and third party transfers of consumer information makes no sense. It is like outlawing robbery while legalizing embezzlement. I look forward to working with my colleagues on this committee in pursuing privacy protections for consumers in H.R. 10 and for cyberspace. I commend Chairman Tauzin for calling this hearing, and I look forward to the testimony from our witnesses.

Mr. TAUZIN. As usual, I thank my friend and the Chair now yields to the gentleman from Richmond, Virginia, the chairman of the full Committee on Commerce, Mr. Tom Bliley.

Chairman BLILEY. Thank you, Mr. Chairman, for holding this hearing. Protection of personal privacy is one of our most talked about issues facing electronic commerce. All Americans have legitimate concerns about how that personal information they provide to web sites is used by the operator of that Web site. As I have stated many times in the past, I believe that ensuring safety, security, and privacy of online consumers is key to consumer use and acceptance of the Internet. Without these concerns being met, I believe that consumers may lose confidence in electronic commerce.

This committee has been active on the issue of online privacy since the 105th Congress. Online privacy is an issue that I hear about many times from my constituents and also from the many people I speak to in the industry. At the privacy hearing that this subcommittee held last year, industry witnesses laid out their plans to protect privacy of consumers. At the time, I supported this effort rather than a Federal regulatory approach. Electronic commerce changes so quickly that I am concerned that a government-mandated privacy policy would stifle innovation. We would be imposing a static policy on a dynamic and constantly changing industry.

Since that hearing last year, I have been monitoring the progress industry has made in self-regulation. I think the progress to date has been very good. The recently completed Georgetown privacy study showed impressive results in the posting of privacy policy by commercial web sites.

Despite these good results, now is not the time for industry to ease up. There is still much more work to be done. Bricks and mortar businesses that are moving online need to tailor their existing privacy policy to the online world. I know that Commissioner Swindle is particularly interested in the needs of small businesses as they move online. Also the true test of a privacy policy is the remedy to consumers if their privacy is violated. Their privacy policy is worth little if their company can ignore consumers who seek redress.

Another area that deserves attention and which I will be following closely, is the transfer of personally identifiable information to third parties. Consumers should be told when third parties may have access to their information and should have the right to refuse the transfer to others of such information. I know there are some legitimate business uses for the transfer of this information. For example, consumers may enjoy knowing about the benefits of getting a discount on a rental car when they purchase an airplane ticket online. But there are many consumers who would prefer not to have personal information about their online reservations or purchases shared with other parties. They should have the right to opt out of the information sharing.

Before I close, I would like to make an announcement. Very shortly, the Commerce Committee will be posting a privacy policy on the committee Web site. We will be the first committee in Congress to post a privacy policy so that visitors to the committee Web site will know how the committee uses information they provide during a visit to the committee Web site.

I want to thank all of our witnesses today for testifying on this issue before this subcommittee, and I would also like to thank Chairman Pitofsky for all of the work that the FTC has done on this issue. The FTC has been closely following this issue and will be publicly releasing their recommendation on dealing with online privacy. I understand that the FTC will not be recommending legislation to regulate privacy at this time. I welcome this recommendation, and I look forward to reviewing the full set of recommendations.

Thank you, Mr. Chairman, and I yield back what little time I may have left.

Mr. TAUZIN. The Chair thanks Chairman Bliley. The Chair wishes to congratulate him on the announcement he has made today. I know we will all feel a lot more comfortable dealing with the committee online. The Chair is now pleased to recognize the gentlelady from California, Ms. Eshoo, for an opening statement.

Ms. ESHOO. Thank you, Mr. Chairman, for holding this very important hearing and I look forward to the testimony and want to welcome the members—the chairman and the members of the FTC and most especially Robert Lewin, the executive director of TRUSTe who is also a constituent of mine. The issue of privacy is something that every American cares intensely about.

In fact, I think they associate it with being an American. It is a right that they want protected. It is a right that they feel passionately about whether it is the protection of their financial records, medical records, or certainly going online and conducting business with e-commerce. So I think it is very important today that this hearing takes place. We will be measuring, by means of this hearing, the progress that has been made since last year, and I look forward to hearing the witnesses. And I yield back the balance of my time.

Mr. TAUZIN. The Chair thanks the gentlelady, and the gentleman from Illinois, Mr. Shimkus, is recognized.

Ms. ESHOO. Mr. Chairman, you need some water. Perhaps we should pour some water for the chairman.

Mr. SHIMKUS. Mr. Chairman, I have no opening statements.

Mr. TAUZIN. Then the Chair recognizes the gentleman from California, Mr. Rogan.

Mr. ROGAN. Mr. Chairman, thanks. I waive opening statement.

Mr. TAUZIN. Then the Chair recognizes Mr. Luther.

Mr. LUTHER. Thank you, Mr. Chairman. I certainly want to thank you and Mr. Markey for your efforts in putting this hearing together today. This is an important issue that is really grabbing the attention of the public. I think we saw this in hearings that we held on the bank financial modernization legislation. And, of course, my home State is Minnesota.

Minnesota is where we had recent litigation by the attorney general against a banking institution. And so I was able to judge, to some extent, the public response and reaction to that. And so I think the comments that have been made here by Mr. Markey and Ms. Eshoo are very appropriate in that this is an issue taken very seriously by the American public.

I think we are just beginning to see the attention that is going to be paid to this particular issue. So despite the fact that we didn't win all of the issues that we were pursuing, particularly with the Markey amendment on the financial modernization legislation, I am very pleased to see that we are back talking about this issue again.

And so again, I commend you and Mr. Markey and the others who are here today for taking on the issue that I think the public wants us to deal with here in Congress: that is, their privacy, who owns their information, how that ought to be dealt with by other people. So thank you again, Mr. Chairman, and I yield back.

Mr. TAUZIN. I thank the gentleman. I suggest that if anybody misbehaves in Minnesota that we just put Governor "The Body" Ventura on them.

Mr. LUTHER. That is right. You will have to take us seriously now.

Mr. TAUZIN. The Chair recognizes the gentleman from Tennessee, Mr. Gordon, for an opening statement.

Mr. GORDON. Mr. Chairman, I would just briefly thank you for having this important meeting and I want to concur with Ms. Eshoo that this is a very important personal issue for people across the country and also concur with Chairman Bliley, in that if we are going to have full access and use of electronic commerce, then there is going to have to be confidence on the net. This is a good hearing. We need to find where we stand and how we can make this balance and I welcome the panelists.

Mr. TAUZIN. I thank the gentleman from Tennessee. The Chair and I ask unanimous consent that all members might have the ability to introduce written statements into the record and all of the written statements of our witnesses be part of the record. Without objection it is so ordered.

[Additional statements submitted for the record follow:]

PREPARED STATEMENT OF HON. BARBARA CUBIN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF WYOMING

Thank you, Mr. Chairman, for holding this important hearing on electronic commerce.

I think it is interesting to note that according to a 1998 World Wide Web user survey, the most important issue facing the Internet was privacy.

However, I think it is even more interesting to note that government regulation of the Internet was also one of the most important issues on the minds of Internet users.

The hearing today will help us to more fully understand what privacy rights are being threatened and what, if any, government regulations are needed to help protect Internet consumers from having their right to privacy violated.

My preference is that industry work out a way in which to solve the privacy issue.

The difficultly comes in policing many of the bad actors out there that essentially make their living garnering and disbursing a consumer's personal information.

There is a push under way for Congress to address this problem in lieu of an industry solution. We should all know at this point that a government solution will never be as good as industry self-governance.

The issue of privacy and the public's knowledge of privacy is complex and unclear.

I look forward to hearing from the witnesses and hope to learn more about this issue.

I'm also interested in what industry proposals are currently in place and what solutions are currently being looked at to solve this problem.

Thank you, Mr. Chairman. I yield back.

PREPARED STATEMENT OF HON. THOMAS C. SAWYER, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF OHIO

Thank you Mr. Chairman for holding this oversight hearing this morning. I also want to thank the Commissioners from the Federal Trade Commission (FTC) for coming to update us on the status of commercial websites as they relate to online privacy policies.

The flexibility of the relatively unregulated environment has greatly contributed to the growth of the Internet. It is becoming clear to me that a primary reason for the Internet's success haa been because of the entrepreneurial spirit of the companies that have helped to make it so extraordinary. Throughout this decade, the Internet has grown from being used by a select few to being used by millions in the United States and internationally for various purposes. The Internet is having profound effect on the traditional ways human discourse and enterprise are conducted, and on the way users receive and distribute information.

Not long ago, the Department of Commerce estimated that by the end of this year electronic commerce in the United States alone could top $9 billion. That is a significant increase over last year's figures.

Still, the widespread use of the Internet is relatively new; it is less than a decade old. No one really knows what its full potential is. However, one thing is true: if consumers are not confident with using the Internet for fear of privacy invasions, electronic commerce may not soon realize the full measure of its potential.

Consumers deserve assurances that their personal information when using the Internet is safe, secure and available only to those they authorize to have such information. On a similar note, consumers should have the ability to review and modify information that is collected about them. These are just basic principles that make good, sound business practices.

Last year, when the Federal Trade Commission and the Online Privacy Alliance came to testify before us, both recommended that Congress not enact legislation requiring commercial websites to develop an online privacy policy. However, they promoted self-regulation within the industry as the immediate answer to address privacy concerns. They reasoned that companies are different, and a uniform national system of standards may not be adequate.

I am encouraged by the fact that the recent Georgetown and Online Privacy Alliance studies shows that more commercial websites have decided to develop and implement online privacy policies. The reports show a dramatic increase from the Federal Trade Commission's previous survey. I hope that this trend continues. I also want to commend companies like TRUSTe and BBBOnLine certify that its membership companies meet certain online privacy standards.

While it may still be too early to enact more comprehensive online privacy legislation, there remains much room for improvement. And so Mr. Chairman, I am glad you have called this very important oversight hearing. I hope today's hearing will serve as a reminder that we take privacy very seriously in Internet use, and users have every right to keep their personal information private and confidential. Using the Internet does not forgo those basic rights. Finally, Mr. Chairman, as I mentioned before, the Internet is rapidly changing and if e-commerce is going to flourish, then commercial websites need to seriously adopt on-line privacy guidelines.

Thank you.

PREPARED STATEMENT OF HON. KAREN MCCARTHY, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF MISSOURI

Thank you, Mr. Chairman, for holding this hearing today on the very important subject of online consumer privacy. As we progress deeper into the Information Age, it is vital that we address issues of consumer protection and privacy early and often in order to ensure that we are providing our constituents with the security they need and desire to comfortably deal in the Internet marketplace.

Research conducted over the past several years shows that consumers are frustrated by the increasing ability of Internet companies to gather personal information about consumers, often without the consumers' knowledge or consent. In addition, many people, myself included, are concerned about the growing use of the Internet for financial and medical information, and the potential for that highly sensitive and personal information to be shared with third parties.

I look forward to hearing the testimony of our witnesses today, particularly those from the Federal Trade Commission (FTC), because I am eager to work with my colleagues to resolve this issue of personal privacy on the Internet. I hope that we will address consumer concerns about receiving notice when information is being collected or when it will be shared, having choices regarding how that information is used, and being assured that their data is indeed secure, yet accessible by the appropriate authorized parties.

I am confident that we will be able to achieve a balance between consumer privacy and an open Internet marketplace that offers a wealth of opportunity to both entrepreneurs and consumers. Thank you. I yield back the balance of my time.

PREPARED STATEMENT OF HON. JOHN D. DINGELL, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF MICHIGAN

Mr. Chairman, I want to thank you for holding this hearing on the privacy problems consumers face when using the Internet. At the outset, let me welcome Chairman Pitofsky, Commissioner Anthony, Commissioner Thompson, and Commissioner Swindle to the Committee. I admire the important work you do in so many areas, and I look forward to hearing your views on what to do about the very serious privacy problems consumers face.

The Federal Trade Commission is the federal government's consumer protection agency, and consumer privacy, both on and off the Internet, is a matter of growing public concern. Consumers are justifiably alarmed that the uncontrolled dissemination of personal data is affecting their job opportunities, as well as their ability to qualify for credit cards, mortgages, car loans, insurance, and more.

How are we going to make sure that on-line merchants do not violate the consumer's wishes by selling information about drugs or other products he or she purchases to employers, banks, and other retailers? What will prevent a bank from ignoring a consumer's instructions and selling his or her personal and account information to a telemarketer, to a securities firm, or to an insurance company?

Consumer privacy problems demand the Commission's special and immediate attention, and I certainly expect the Commission to give this problem the attention it so rightly deserves.

Today, the consumer is fighting a losing battle to control the dissemination and use of personal medical and financial data. Industry has thus far failed to develop, implement, and enforce safeguards to control how personal information may be used by others. Even when private firms adopt policies that allow consumers to "opt-out" or restrict the transfer of their personal data, the consumer's wishes are too often ignored by banks and others who make huge profits from the sale of personal and account data.

Last month, the Minnesota State Attorney General brought suit against several banks in that State for transferring customer personal and account data to third parties, despite instructions from some of their customers not to do this. These banks had a privacy policy. That privacy policy allowed their customers to "opt-out" from the transfer of personal data to third parties. Yet when customers exercised this right to "opt-out", their right was ignored. Lest anyone wrongly conclude that the problem in Minnesota is unique, the Comptroller of the Currency made a public statement in which he said these same abuses are occurring far too frequently throughout the banking industry and that they must be stopped.

In the on-line world, these privacy problems are magnified. The special nature of the Internet demands greater sensitivity by government to the privacy rights of individuals, and the Federal Trade Commission can and should play a key role in protecting consumers' interests.

Again, I look forward to hearing the testimony of the Commissioners, and I want to thank them for their participation in this hearing.

Mr. TAUZIN. We will now welcome and call forward our first panel which will consist of the chairman and members of the Federal Trade Commission, beginning with the chairman, the Honorable Robert Pitofsky, the Honorable Orson Swindle, the Honorable Sheila Anthony, and the Honorable Mozelle Thompson; all commissioners of the Federal Trade Commission. Ladies and Gentlemen, if you would come forward. While you are coming forward, let me remind you that at our last hearing last year, I asked each of you to give me your letter grade on the progress of the industry of protecting American's privacy online.

Each of you at the termination of that hearing gave me your letter grade estimate. Let me remind you what they were. Mr. Swindle, you gave the industry a rising D. Ms. Anthony, you gave the industry a D plus. Mr. Pitofsky, like a good professor, you gave them an incomplete. Mr. Thompson, you wouldn't give a letter grade, but you said there was considerable room for improvement is the quote we have for you last year. So a rising D, a D plus, an incomplete, and considerable room for improvement. When you complete your testimony today I would ask you—if you can be thinking about it now—give me your latest grade on the industry so that we can track the progress as we would any university.

We begin now by welcoming the Chairman of the Federal Trade Commission, our friend, Mr. Robert Pitofsky, and we welcome your testimony, Mr. Pitofsky.

STATEMENTS OF HON. ROBERT PITOFSKY, CHAIRMAN; HON. ORSON SWINDLE, COMMISSIONER; HON. SHEILA F. ANTHONY, COMMISSIONER; AND HON. MOZELLE W. THOMPSON, COMMISSIONER, FEDERAL TRADE COMMISSION

Mr. PITOFSKY. Thank you, Mr. Chairman, Mr. Markey, and members of the committee. I am delighted to be here again to discuss what we all agree is a tremendously important question and to deliver the Commission's report on online privacy.

Incidentally, many things have changed about online privacy. Statistics change over 2, 3, 4 years. But one thing hasn't changed. If you ask people who don't do business on the Internet, who don't make purchases, what is your reason for not doing so, you will still hear that about 85 percent of the people who avoid buying on the Internet offer as their reason that they don't think that it is a secure transaction. And privacy, of course, is a major element of that.

Let me see if I can start by finding some common ground here. We at the Commission and I think members of the committee all agree that consumers are entitled to have their privacy protected when they do business on the Internet. And we all agree that if we can do it, the best way to get there is through industry self-regulation because this is such a dynamic, changing, vigorous, and new sector of the economy. We begin to see different opinions, however, when you move on to some other questions. And as the opening statements indicated, very reasonable people can differ about how to get there.

First, there are differences about how much has been accomplished over the last year or so in terms of self-regulation and pri-

vacy. And second, and perhaps even more important, how far will self-regulation ever go in protecting consumers? Can we ever get to an accepted level of protection for consumers on the Internet through self-regulation and without some legislation?

You may recall that when we were here a year ago, we delivered a report to this committee indicating disappointment at the levels of privacy protection that existed then. A key fact was that while 90 percent of the firms selling products on the Internet collected personally identifiable private information, only 14 percent even announced that they had a privacy policy of any sort. And only about 2 percent had the broad range of privacy policies that we call fair information practices. I should say that on the busiest web sites, not all, but on the busiest, privacy policies were published in about 44 percent of the instances.

It is now a year later and a good deal has happened. One interesting development is considerable agreement on essentially what are fair information practices. They are pretty much what Mr. Markey outlined. Notice, consent, because if you don't have notice and consent, privacy protection doesn't work at all. If people don't know what their rights are and what is going to happen to the information that they give, then you have no privacy at all. Reasonable access such that consumers can find out what sellers are doing with the information, how they are selling it and whether there are errors in the information. Finally, some security arrangements.

Second, there has been a sharp improvement in the level of notice that people are getting on the Internet. I said it was 14 percent a year ago. The newest Georgetown University study, which is not exactly comparable to the last study but is pretty close, indicates that we have gone from 14 percent to 66 percent of web sites that post privacy policies. Of web sites that have the full range of fair information practices, we have gone from 2 percent up to 10 percent.

I think that is pretty good in 1 year. We have seen in other sectors of the economy that self-regulation doesn't happen overnight. It takes a while. Certainly we have seen strong important steps in the right direction and real progress. We have also seen in the last year the development of seal programs by a number of different organizations. They have established standards for privacy protection and then give out a seal of approval only to those companies that abide by their commitment to those standards.

Now, this is just the beginning. There are a million web sites. Altogether there are probably about a thousand firms that have committed to a seal programs. But TRUSTe, Better Business Bureau OnLine and others do appear to be moving in the direction of seals of approval and in the direction of monitoring whether people abide by their commitment, and to enforcing their seal programs. Because of this progress, the majority of the Commission recommends no legislation at this time.

That is not to say that all that needs to be done has been done. There is a long way to go before we can say that we are at a level at which consumers can be confident that their privacy has been protected. For example, even though 66 percent post privacy policies, that still means that 34 percent have no privacy policies whatsoever. And even though 66 percent post the privacy policy, as we

have heard, only about 10 percent touch all of the bases that we think are necessary to protect privacy.

Therefore, although we don't believe legislation is appropriate at this time, we do believe there has been considerable progress. The FTC certainly is not abandoning the field. We intend to conduct workshops over the next year focussing, for example, on issues like personnel profiling, task forces in which we will work with industry and consumer groups to try to understand particular issues like technology developments, and whether there are technological fixes in this area.

We are going to work with the Department of Commerce on consumer education which in the long run may be one of the more important ways to get to what I have described as the goal line, and we will commit now to monitor this important new marketplace and come back here with a report the next time around, about a year from now. We want to let some time go by to see if there is continued progress.

The next report is going to be different. These reports so far essentially involve counting noses. How many sellers have a privacy policy; how many sellers don't. We want to get at the question of whether those privacy policies are worth the screen that they appear on. We want to ask qualitative questions. We want to ask about access. We want to ask about security.

And we want to ask—if we are going the self-regulation route—we want to ask about monitoring and enforcement. It is not enough to put a privacy policy up there. We have to be confident that people are paying attention to it and are really doing what they say.

In conclusion, let me say that I think developments over the year indicate that the idea of giving self-regulation a chance was the right approach. The business community deserves a lot of credit for working hard to produce the changes that they have produced. On the other hand, this progress must continue. It is not time to declare victory on this issue. I would say this: If the progress does not continue at something like the pace that we have seen in the past year, then I think it is time to reconsider a legislative solution. Thank you.

[The prepared statement of Hon. Robert Pitofsky follows:]

PREPARED STATEMENT OF HON. ROBERT PITOFSKY, CHAIRMAN, FEDERAL TRADE COMMISSION

Mr. Chairman and members of the Subcommittee, I am Robert Pitofsky, Chairman of the Federal Trade Commission ("FTC" or "Commission"). I appreciate this opportunity to present the Commission's views on the progress of self-regulation in the area of online privacy.[1]

I. Introduction and Background

The FTC's mission is to promote the efficient functioning of the marketplace by protecting consumers from unfair or deceptive acts or practices and to increase consumer choice by promoting vigorous competition. As you know, the Commission's responsibilities are far-reaching. The Commission's primary legislative mandate is to enforce the Federal Trade Commission Act ("FTCA"), which prohibits unfair methods of competition and unfair or deceptive acts or practices in or affecting commerce.[2] With the exception of certain industries, the FTCA provides the Commission with broad law enforcement authority over entities engaged in or whose business affects commerce[3] and with the authority to gather information about such entities.[4] Commerce on the Internet falls within the scope of this statutory mandate.[5]

In June 1998 the Commission issued *Privacy Online: A Report to Congress* ("1998 Report"), an examination of the information practices of commercial sites on the

World Wide Web and of industry's efforts to implement self-regulatory programs to protect consumers' online privacy.[6] Based in part on its extensive survey of over 1400 commercial Web sites, the Commission concluded that effective self-regulation had not yet taken hold.[7] The Commission recommended that Congress adopt legislation setting forth standards for the online collection of personal information from children; and indeed, just four months after the 1998 Report was issued, Congress enacted the Children's Online Privacy Protection Act of 1998.[8] As required by the Act, on April 20, 1999, the Commission issued a proposed Children's Online Privacy Protection Rule, which implements the Act's fair information practices standards for commercial Web sites directed to children under 13, or who knowingly collect personal information from children under 13.[9] Commission staff is reviewing comments on the proposed rule and will issue a final rule this fall.

When the 1998 report was released, there were indications that industry leaders were committed to work toward self-regulatory solutions. As a result, in Congressional testimony last July the Commission deferred judgment on the need for legislation to protect the online privacy of consumers generally, and instead urged industry to focus on the development of broad-based and effective self-regulatory programs.[10] In the ensuing year, there have been important developments both in the growth of the Internet as a commercial marketplace and in consumers' and industry's responses to the privacy issues posed by the online collection of personal information. The Commission has just issued a new report on these developments, *Self-Regulation and Online Privacy: A Report to Congress* (June 1999) ("1999 Report").[11] The 1999 Report assesses the progress made in self-regulation to protect consumers' online privacy since last June and sets out an agenda of Commission actions in the coming year to encourage industry's full implementation of online privacy protections. I am pleased to present the 1999 Report's findings to the Committee.

II. The Current State of Online Privacy Regulation

The Commission believes that self-regulation is the least intrusive and most efficient means to ensure fair information practices online, given the rapidly evolving nature of the Internet and computer technology. During the past year the Commission has been monitoring self-regulatory initiatives, and the Commission's 1999 Report finds that there has been notable progress. Two new industry-funded surveys of commercial Web sites suggest that online businesses are providing significantly more notice of their information practices than they were last year. Sixty-six percent of the sites in the Georgetown Internet Privacy Policy Survey ("GIPPS")[12] post at least one disclosure about their information practices.[13] Forty-four percent of these sites post privacy policy notices.[14] Although differences in sampling methodology prevent direct comparisons between the GIPPS findings and the Commission's 1998 results,[15] the GIPPS Report does demonstrate the real progress industry has made in giving consumers notice of at least some information practices. Similarly, 93% of the sites in the recent study commissioned by the Online Privacy Alliance ("OPA Study") provide at least one disclosure about their information practices.[16] This, too, represents continued progress since last year, when 71% of the sites in the Commission's 1998 "Most Popular" sample posted an information practice disclosure.[17]

The new survey results show, however, that, despite the laudable efforts of industry leaders, significant challenges remain. The vast majority of the sites in both the GIPPS and OPA surveys collect personal information from consumers online.[18] By contrast, only 10% of the sites in the GIPPS sample,[19] and only 22% of the sites in the OPA study,[20] are implementing all four substantive fair information practice principles of Notice/Awareness, Choice/Consent, Access/Participation, and Security/Integrity.[21] In light of these results, the Commission believes that further improvement is required to effectively protect consumers' online privacy.

In the Commission's view, the emergence of online privacy seal programs is a particularly promising development in self-regulation. Here, too, industry faces a considerable challenge. TRUSTe, launched nearly two years ago, currently has more than 500 licensees representing a variety of industries.[22] BBBOnLine, a subsidiary of the Council of Better Business Bureaus, which launched its privacy seal program for online businesses last March, currently has 42 licensees and more than 300 applications for licenses.[23] Several other online privacy seal programs are just getting underway.[24] Together, the online privacy seal programs currently encompass only a handful of all Web sites. It is too early to judge how effective these programs will ultimately be in serving as enforcement mechanisms to protect consumers' online privacy.

III. Conclusion

The self-regulatory initiatives discussed above, and described in greater detail in the 1999 Report, reflect industry leaders' substantial effort and commitment to fair

information practices. They should be commended for these efforts. Enforcement mechanisms that go beyond self-assessment are also gradually being implemented by the seal programs. Only a small minority of commercial Web sites, however, have joined these programs to date. Similarly, although the results of the GIPPS and OPA studies show that many online companies now understand the business case for protecting consumer privacy, they also show that the implementation of fair information practices is not widespread among commercial Web sites.

Based on these facts, the Commission believes that legislation to address online privacy is not appropriate at this time. We also believe that industry faces some substantial challenges. Specifically, the present challenge is to educate those companies which still do not understand the importance of consumer privacy and to create incentives for further progress toward effective, widespread implementation.

First, industry groups must continue to encourage widespread adoption of fair information practices. Second, industry should focus its attention on the substance of web site information practices, ensuring that companies adhere to the core privacy principles discussed earlier. It may also be appropriate, at some point in the future, for the FTC to examine the online privacy seal programs and report to Congress on whether these programs provide effective privacy protections for consumers.

Finally, industry must work together with government and consumer groups to educate consumers about privacy protection on the Internet. The ultimate goal of such efforts, together with effective self-regulation, will be heightened consumer acceptance and confidence. Industry should also redouble its efforts to develop effective technology to provide consumers with tools they can use to safeguard their own privacy online.

The Commission has developed an agenda to address online privacy issues throughout the coming year as a way of encouraging and, ultimately, assessing further progress in self-regulation to protect consumer online privacy:

- The Commission will hold a public workshop on "online profiling," the practice of aggregating information about consumers' preferences and interests gathered primarily by tracking their movements online. The workshop, jointly sponsored by the U.S. Department of Commerce, will examine online advertising firms' use of tracking technologies to create targeted, user profile-based advertising campaigns.
- The Commission will hold a public workshop on the privacy implications of electronic identifiers that enhance Web sites' ability to track consumers' online behavior.
- In keeping with its history of fostering dialogue on online privacy issues among all stakeholders, the Commission will convene task forces of industry representatives and privacy and consumer advocates to develop strategies for furthering the implementation of fair information practices in the online environment.
  - One task force will focus upon understanding the costs and benefits of implementing fair information practices online, with particular emphasis on defining the parameters of the principles of consumer access to data and adequate security.
  - A second task force will address how incentives can be created to encourage the development of privacy-enhancing technologies, such as the World Wide Web Consortium's Platform for Privacy Preferences (P3P).
- The Commission, in partnership with the U.S. Department of Commerce, will promote private sector business education initiatives designed to encourage new online entrepreneurs engaged in commerce on the Web to adopt fair information practices.
- Finally, the Commission believes it is important to continue to monitor the progress of self-regulation, to determine whether the self-regulatory programs discussed in the 1999 Report fulfill their promise. To that end, the Commission will conduct an online survey to reassess progress in Web sites' implementation of fair information practices, and will report its findings to Congress.

The Commission is committed to the goal of full implementation of effective protections for online privacy in a manner that promotes a flourishing online marketplace, and looks forward to working with the Subcommittee as it considers the Commission's 1999 Report.

ENDNOTES

[1] The Commission vote to issue this testimony was 3-1, with Commissioner Anthony concurring in part and dissenting in part. Commissioner Anthony's statement is attached to the testimony. Commissioner Swindle's concurring statement is also attached. My oral testimony and responses to questions you may have reflect my own views and are not necessarily the views of the Commission or any Commissioner.

[2] 15 U.S.C. §45 (a).

[3] The Commission does not have criminal law enforcement authority. Further, certain entities, such as banks, savings and loan associations, and common carriers, as well as the business of insurance are wholly or partially exempt from Commission jurisdiction. *See* Section 5 (a) (2) of the FTC Act, 15 U.S.C. §45 (a) (2), and the McCarran-Ferguson Act, 15 U.S.C. §1012 (b).

[4] 15 U.S.C. §46 (a). However, the Commission's authority to conduct studies and prepare reports relating to the business of insurance is limited. According to 15 U.S.C. §46 (a): "The Commission may exercise such authority only upon receiving a request which is agreed to by a majority of the members of the Committee on Commerce, Science, and Transportation of the Senate or the Committee on Energy and Commerce of the House of Representatives. The authority to conduct any such study shall expire at the end of the Congress during which the request for such study was made."

The Commission also has responsibility under approximately forty additional statutes governing specific industries and practices. These include, for example, the Truth in Lending Act, 15 U.S.C. §§1601 *et seq.*, which mandates disclosures of credit terms, and the Fair Credit Billing Act, 15 U.S.C. §§1666 *et. seq.*, which provides for the correction of billing errors on credit accounts. The Commission also enforces over 30 rules governing specific industries and practices, *e.g.*, the Used Car Rule, 16 C.F.R. Part 455, which requires used car dealers to disclose warranty terms via a window sticker; the Franchise Rule, 16 C.F.R. Part 436, which requires the provision of information to prospective franchisees; and the Telemarketing Sales Rule, 16 C.F.R. Part 310, which defines and prohibits deceptive telemarketing practices and other abusive telemarketing practices.

[5] The Commission held its first public workshop on online privacy in April 1995. In a series of hearings held in October and November 1995, the Commission examined the implications of globalization and technological innovation for competition issues and consumer protection issues, including privacy concerns. At a public workshop held in June 1996, the Commission examined Web site practices in the collection, use, and transfer of consumers' personal information; self-regulatory efforts and technological developments to enhance consumer privacy; consumer and business education efforts; the role of government in protecting online information privacy; and special issues raised by the online collection and use of information from and about children. The Commission held a second workshop in June 1997 to explore issues raised by individual reference services, as well as issues relating to unsolicited commercial e-mail, online privacy generally, and children's online privacy.

These efforts have served as a foundation for dialogue among members of the information industry and online business community, government representatives, privacy and consumer advocates, and experts in interactive technology. Further, the Commission and its staff have issued reports describing various privacy concerns in the electronic marketplace. *See, e.g., Individual Reference Services: A Federal Trade Commission Report to Congress* (December 1997); FTC Staff Report: *Public Workshop on Consumer Privacy on the Global Information Infrastructure* (December 1996); FTC Staff Report: *Anticipating the 21st Century: Consumer Protection Policy in the New High-Tech, Global Marketplace* (May 1996).

The Commission has also brought enforcement actions under Section 5 of the Federal Trade Commission Act to address deceptive online information practices. In 1998 the Commission announced its first Internet privacy case, in which GeoCities, operator of one of the most popular sites on the World Wide Web, agreed to settle Commission charges that it had misrepresented the purposes for which it was collecting personal identifying information from children and adults through its online membership application form and registration forms for children's activities on the GeoCities site. The settlement, which was made final in February 1999, prohibits GeoCities from misrepresenting the purposes for which it collects personal identifying information from or about consumers, including children. It also requires GeoCities to post a prominent privacy notice on its site, to establish a system to obtain parental consent before collecting personal information from children, and to offer individuals from whom it had previously collected personal information an opportunity to have that information deleted. *GeoCities*, Docket No. C-3849 (Feb. 12, 1999) (Final Decision and Order available at http://www.ftc.gov/os/1999/9902/9823015d&o.htm).

In its second Internet privacy case, the Commission recently announced for public comment a settlement with Liberty Financial Companies, Inc., operator of the Young Investor Web site. The Commission alleged, among other things, that the site falsely represented that personal information collected from children, including information about family finances, would be maintained anonymously. In fact, this information was maintained in identifiable form. The consent agreement would require Liberty Financial to post a privacy policy on its children's sites and obtain verifiable consent before collecting personal identifying information from children. *Liberty Financial*, Case No. 9823522 (proposed consent agreement available at http://www.ftc.gov/os/1999/9905/lbtyord.htm).

Since the fall of 1994, the Federal Trade Commission has brought 91 law enforcement actions against over 200 companies and individuals to halt fraud and deception on the Internet. The FTC has not only attacked traditional schemes that have moved online, like pyramid and credit repair schemes, but in addition, the FTC has brought suit against modem hijacking, fraudulent e-mail marketing, and other hi-tech schemes that take unique advantage of the Internet. The Commission pioneered the "Surf Day" concept and has searched the Net in tandem with law enforcement colleagues around the world, targeting specific problems and warning consumers and new entrepreneurs about what the law requires. The Commission has also posted "teaser pages" online, i.e., fake scam sites that give consumers education just when they are about to fall victim to an Internet ruse.

[6] The Report is available on the Commission's Web site at http://www.ftc.gov/reports/privacy3/index.htm.

[7] 1998 Report at 41.

[8] Title XIII, Omnibus Consolidated and Emergency Supplemental Appropriationa Act, 1999, Pub. L. No. 105-277, 112 Stat. 2681, ———— (Oct. 21, 1998), *reprinted at* 144 Cong. Rec.

H11240-42 (Oct. 19, 1998). The Act requires, *inter alia*, that operators of Web sites directed to children under 13 or who knowingly collect personal information from children under 13 on the Internet: (1) provide parents notice of their information practices; (2) obtain prior, verifiable parental consent for the collection, use, and/or disclosure of personal information from children (with certain limited exceptions); (3) upon request, provide a parent with the ability to review the personal information collected from his/her child; (4) provide a parent with the opportunity to prevent the further use of personal information that has already been collected, or the future collection of personal information from that child; (5) limit collection of personal information for a child's online participation in a game, prize offer, or other activity to information that is reasonably necessary for the activity; and (6) establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of the personal information collected.

[9] 64 Fed. Reg. 22750 (1999) (to be codified at 16 C.F.R. pt. 312).

[10] Commission testimony on *Consumer Privacy on the World Wide Web* before the House Subcommittee on Telecommunications, Trade and Consumer Protection, Committee on Commerce (July 21, 1998) (available at http://www.ftc.gov/os/1998/9807/privac98.htm). The Commission also presented a legislative model that Congress could consider in the event that then-nascent self-regulatory efforts did not result in widespread implementation of self-regulatory protections. *Id.* at 5-7.

[11] A copy of the Report is attached as an appendix. The Report is available on the Commission's Web site at www.ftc.gov/reports/privacy99/index.html.

[12] The report is available at http://www.msb.edu/faculty/culnanm/gippshome.html [hereinafter "GIPPS Report"]. The following analysis is based upon the Commission's review of the GIPPS Report itself; Commission staff did not have access to the underlying GIPPS data.

[13] GIPPS Report, App. A at 5.

[14] *Id.*

[15] The GIPPS Report discusses findings on the information practices of 361 Web Sites drawn from a list of the 7,500 busiest servers on the World Wide Web. The list, a ranking of servers by number of unique visitors for the month of January 1999, was compiled by Media Metrix, a site traffic measurement company. As larger sites are more likely to have multiple servers, the largest sites on the Web had a greater chance of being selected for inclusion in the sample drawn for the GIPPS survey. *See* GIPPS Report, App. A at 2; App. B at 9 n.iii. The Commission's 1998 Comprehensive Sample was drawn at random from all U.S., ".com" sites in the Dun & Bradstreet Electronic Commerce Registry, with the exception of insurance industry sites. 1998 Report, App. A at 2. Unlike the Media Metrix list used in the GIPPS sample, the Dun & Bradstreet Registry does not rank sites on the basis of user traffic.

[16] Online Privacy Alliance, *Privacy and the Top 100 Sites: A Report to the Federal Trade Commission* at 3, 8 (1999) (available at http://www.msb.edu/faculty/culnanm/gippshome.html). The following analysis is based upon the Commission's review of the OPA Study report itself; Commission staff did not have access to the underlying OPA Study data.

[17] 1998 Report at 28.

[18] Ninety-three percent of the sites in the GIPPS survey, GIPPS Report, App. A at 3, and 99% of the sites in the OPA Study, OPA Study at 3, 5, collect personal information from consumers.

[19] The GIPPS results show that thirty-six sites in the sample (or 10%) posted at least one survey element, or disclosure, for each of the four substantive fair information practices. GIPPS Report at 10 and App. A at 12 (Table 8C). Thirty-two of these sites (or 8.9%) also posted contact information. *Id.* Georgetown University Professor Mary Culnan, author of the GIPPS Report, reports the number of sites posting disclosures for the four substantive fair information practice principles and for contact information in two additional ways: as a percentage of sites in the sample that collect at least one type of personal information (9.5%); and as a percentage of sites in the sample that both collect at least one type of personal information and post a disclosure (13.6%). GIPPS Report, App. A at 12 (Table 8C).

[20] Twenty-two sites in the OPA Study (or 22%) posted at least one survey element, or disclosure, for each of the four substantive fair information practices. OPA Study at 9-10 and App. A at 10 (Table 6C). Nineteen of these sites (or 19%) also posted contact information. *Id.* Professor Culnan also reports the number of sites posting disclosures for the four substantive fair information practice principles in two additional ways: as a percentage of sites in the sample that collect at least one type of personal information (22.2%); and as a percentage of sites in the sample that both collect at least one type of personal information and post a disclosure (23.7%). OPA Study, App. A at 10 (Table 6C).

[21] The Commission's 1998 Report discussed the fair information practice principles developed by government agencies in the United States, Canada, and Europe since 1973, when the United States Department of Health, Education, and Welfare released its seminal report on privacy protections in the age of data collection, *Records, Computers, and the Rights of Citizens.* 1998 Report at 7-11. In addition to the HEW Report, the major reports setting forth the core fair information practice principles are: The U.S. Privacy Protection Study Commission, *Personal Privacy in an Information Society* (1977); Organization for Economic Cooperation and Development, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980); U.S. Information Infrastructure Task Force, Information Policy Committee, Privacy Working Group, *Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information* (1995); U.S. Dept. of Commerce, *Privacy and the NII: Safeguarding Telecommunications-Related Personal Information* (1995); The European Union Directive on the Protection of Personal Data (1995); and the Canadian Standards Association, *Model Code for the Protection of Personal Information: A National Standard of Canada* (1996). The 1998 Report identified the core principles of privacy protection common to these government reports, guidelines, and model codes: (1) Notice/Awareness; (2) Choice/Consent; (3) Access/Participation; (4) Integrity/Security; and (5) Enforcement/Redress. 1998 Report at 7-11.

The Notice/Awareness principle is the most fundamental: consumers must be given notice of a company's information practices before personal information is collected from them. The scope

and content of the notice will vary with a company's substantive information practices, but the notice itself is essential. The other core principles have meaning only if a consumer has notice of an entity's information practices and his or her rights with respect thereto. *Id.* at 7.

The Choice/Consent principle requires that consumers be given options with respect to whether and how personal information collected from them may be used. Although choice in this context has been traditionally thought of as either "opt-in" (prior consent for use of information) or "opt-out" (limitation upon further use of information), *id.* at 9, interactive media hold the promise of making this paradigm obsolete through developments in technology. *Id.* The Access/Participation principle requires that consumers be given reasonable access to information collected about them and the ability to contest that data's accuracy and completeness. *Id.*

The Integrity/Security principle requires that companies take reasonable steps to assure that information collected from consumers is accurate and secure from unauthorized use. *Id.* at 10. Finally, the effectiveness of the foregoing privacy protections is dependent upon implementation of the Enforcement/Redress principle, which requires governmental and/or self-regulatory mechanisms to impose sanctions for noncompliance with fair information practices. *Id.* at 10-11. The 1998 Report assessed existing self-regulatory efforts in light of these fair information practice principles.

[22] Information about TRUSTe is taken from materials posted on TRUSTe's Web site, http://www.truste.org, and from public statements by TRUSTe staff. Several hundred additional companies have joined the TRUSTe program but are not yet fully licensed. *See "TRUSTe Testifies Before House Judiciary Committee,"* May 27, 1999 (press release available at http://www.truste.org/about/about—committee.html).

[23] Information about BBB*Online* is taken from materials posted on the BBB*Online* Web site, located at http://www.bbbonline.com, and from other public documents and statements by BBB*OnLine* staff.

[24] CPA WebTrust, the online privacy seal program created by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants, currently has 19 licensees (program description available at http://www.cpawebtrust.org). The Electronic Software Rating Board's ESRB Privacy Online program was launched on June 1, 1999 (description available at http://www.esrb.org).

SELF-REGULATION AND PRIVACY ONLINE: A REPORT TO CONGRESS

FEDERAL TRADE COMMISSION
JULY 1999

TABLE OF CONTENTS

I. INTRODUCTION AND BACKGROUND

In June 1998 the Federal Trade Commission issued *Privacy Online: A Report to Congress* ("1998 Report"), an examination of the information practices of commercial sites on the World Wide Web and of industry's efforts to implement self-regulatory programs to protect consumers' online privacy.[1] Based in part on its extensive survey of over 1400 commercial Web sites, the Commission concluded that effective self-regulation had not yet taken hold.[2] In both the 1998 Report and in subsequent testimony before Congress, the Commission raised concerns about protecting the privacy of children's personal information online and recommended that Congress pass legislation to address these concerns.[3] In its testimony, the Commission also raised concerns about the progress of industry self-regulation, but noted that industry leaders had indicated their commitment to work toward self-regulatory solutions. Accordingly, the Commission did not recommend legislative action in the area of online privacy for consumers generally, and instead urged industry to focus on developing and implementing broad-based and effective self-regulatory programs.[4]

In the ensuing year, there have been important developments both in the growth of the Internet as a commercial marketplace and in consumers' and industry's responses to the privacy issues posed by the online collection of personal information. The Commission has examined these developments and now presents its views on the progress made in self-regulation since last June, as well as its plans to encourage industry's full implementation of online privacy protections.

A. The Growth of Electronic Commerce

Commerce on the World Wide Web is booming. The United States Department of Commerce recently announced that online sales tripled from approximately $3 billion in 1997 to approximately $9 billion in 1998.[5] Online revenues of North American retailers in the first half of 1998 were approximately $4.4 billion.[6] Online advertising revenues have grown from $906.5 million in 1996 to $1.92 billion in 1998.[7] In 1998, revenues for Internet advertising

exceeded those for advertising on outdoor billboards.[8] It is estimated that almost 80 million adults in the United States are using the Internet.[9] They are finding a vast array of products, services, and information in a marketplace that has experienced exponential growth since its beginnings only a few years ago.

The Web is also a rich source of information about online consumers. Web sites collect much personal information both explicitly, through registration pages, survey forms, order forms, and online contests, and by using software in ways that are not obvious to online consumers. Through "cookies" and tracking software, Web site owners are able to follow consumers' online activities and gather information about their personal interests and preferences. These data have proved extremely valuable to online companies because they not only enable merchants to target market products and services that are increasingly tailored to their visitors' interests, but also permit companies to boost their revenues by selling advertising space on their Web sites.[10] In fact, an entire industry has emerged to market a variety of software products designed to assist Web sites in collecting and analyzing visitor data and in serving targeted advertising.[11]

B. Consumer Privacy Concerns

Notwithstanding the substantial benefits that consumers may derive from using the Internet, consumers still care deeply about the privacy of their personal information in the online marketplace. Eighty-seven percent of U.S. respondents in a recent survey of experienced Internet users stated that they were somewhat or very concerned about threats to their privacy online.[12] Seventy percent of the respondents in a recent national survey conducted for the National Consumers League reported that they were uncomfortable providing personal information to businesses online.[13] Consumers are particularly concerned about potential transfers to third parties of the personal information they have given to online businesses.[14] It is not surprising that only about one-quarter of Internet users go beyond merely browsing for information to actually purchasing goods and services online.[15]

II. THE COMMISSION'S APPROACH TO ONLINE PRIVACY

For almost as long as there has been an online marketplace, the Commission has been deeply involved in addressing online privacy issues.[16] The Commission's goal has been to understand this new marketplace and its information practices, to assess the impact of these practices on consumers, and to encourage and facilitate effective self-regulation as the preferred approach to protecting consumer privacy online. The Commission's efforts have been based on the belief that greater protection of personal privacy on the Web will not only benefit consumers, but also benefit industry by increasing consumer confidence and ultimately their participation in the online marketplace.

The Commission's 1998 Report discussed the fair information practice principles developed by government agencies in the United States, Canada, and Europe since 1973, when the United States Department of Health, Education, and Welfare released its seminal report on privacy protections in the age of data collection, *Records, Computers, and the Rights of Citizens*.[17] The 1998 Report identified the core principles of privacy protection common to the government reports, guidelines, and model codes that have emerged since 1973: (1) Notice/Awareness; (2) Choice/Consent; (3) Access/Participation; (4) Integrity/Security; and (5) Enforcement/Redress.[18]

The Notice/Awareness principle is the most fundamental: consumers must be given notice of a company's information practices before personal information is collected from them. The scope and content of the notice will vary with a company's substantive information practices, but the notice itself is essential. The other core principles have meaning only if a consumer has notice of an entity's information practices and his or her rights with respect thereto.

The other core principles are briefly summarized here. The Choice/Consent principle requires that consumers be given options with respect to whether and how personal information collected from them may be used.[19] The Access/Participation principle requires that consumers be given reasonable access to information collected about them and the ability to contest that data's accuracy and completeness.[20] The Integrity/Security principle requires that

companies take reasonable steps to assure that information collected from consumers is accurate and secure from unauthorized use.[21] Finally, the effectiveness of the foregoing privacy protections is dependent upon implementation of the Enforcement/Redress principle, which requires governmental and/or self-regulatory mechanisms to impose sanctions for noncompliance with fair information practices.[22]

The 1998 Report assessed existing self-regulatory efforts in light of these fair information practice principles and set out the findings of the Commission's extensive survey of commercial Web sites' information practices. The survey found that, although the vast majority of sites collected personal information from consumers – 92% in the sample representing all U.S.-based commercial sites likely to be of interest to consumers – only 14% posted any disclosure regarding their information practices, and only 2% posted a comprehensive privacy policy.[23] The results of the Commission's census of the busiest sites on the World Wide Web were more positive: while 97% collected personal information, 71% posted a disclosure and 44% posted a comprehensive privacy policy.[24] The Commission's survey of sites directed to children revealed that 89% collected personal information from children, 24% posted privacy policies and only 1% required parental consent prior to the collection or disclosure of children's information.[25]

The 1998 Report concluded that an effective self-regulatory system had yet to emerge and that additional incentives were required in order to ensure that consumer privacy would be protected. Noting its particular concern about the vulnerability of children, the Commission recommended that Congress adopt legislation setting forth standards for the online collection of information from children. Furthermore, in Congressional testimony last July, the Commission deferred judgment on the need for legislation to protect the online privacy of adult consumers, but presented a legislative model that Congress could consider if industry failed to develop and implement effective self-regulatory measures.[26]

III. CONGRESSIONAL RESPONSE

On October 21, 1998, the President signed into law the Children's Online Privacy Protection Act of 1998 ("COPPA").[27] The Act, passed by Congress just four months after the Commission's 1998 Report, requires that operators of Web sites directed to children under 13 or who knowingly collect personal information from children under 13 on the Internet: (1) provide parents notice of their information practices; (2) obtain prior, verifiable parental consent for the collection, use, and/or disclosure of personal information from children (with certain limited exceptions); (3) upon request, provide a parent with the ability to review the personal information collected from his/her child; (4) provide a parent with the opportunity to prevent the further use of personal information that has already been collected, or the future collection of personal information from that child; (5) limit collection of personal information for a child's online participation in a game, prize offer, or other activity to information that is reasonably necessary for the activity; and (6) establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of the personal information collected.[28] The Act directs the Commission to adopt within one year regulations implementing these requirements.[29]

On April 20, 1999, the Commission issued a proposed Children's Online Privacy Protection Rule and is now in the midst of this rulemaking effort.[30] The proposed rule requires Web site operators to post prominent links on their Web sites to a notice of how they collect and use personal information from children under the age of 13, and sets out, among other things, standards for complying with the Act's notice, parental consent, and access requirements.[31] As required by the COPPA, the proposed rule also includes a safe harbor provision under which industry groups or others may seek Commission approval for self-regulatory guidelines. Web site operators who participate in such approved programs may be subject to the review and disciplinary procedures provided in those guidelines in lieu of formal Commission investigation and law enforcement.[32] The safe harbor would serve both as an incentive for industry self-regulation, and as a means of ensuring that the Act's protections are implemented in a

manner sensitive to industry-specific concerns and developments in technology. Commission staff is reviewing comments on the proposed rule and will hold a public workshop this month to solicit further discussion and comment on the issue of verifiable parental consent. The Commission will issue a final rule this fall.

IV. THE STATE OF ONLINE PRIVACY SELF-REGULATION TODAY

As noted in the Commission's 1998 Report, self-regulation is the least intrusive and most efficient means to ensure fair information practices, given the rapidly evolving nature of the Internet and computer technology. During the past year the Commission has been monitoring self-regulatory initiatives to address the privacy concerns of online consumers. In some areas, there has been much progress. The results of two new surveys of commercial Web sites suggest that online businesses are providing significantly more notice of their information practices than they were last year. In addition, several significant and promising self-regulatory programs, including privacy seal programs, are underway.

There are also major challenges for self-regulation. The new survey results show that, despite the laudable efforts of industry leaders, the vast majority of even the busiest Web sites have not implemented all four substantive fair information practice principles of Notice/Awareness, Choice/Consent, Access/Participation, and Security/Integrity. In addition, the seal programs discussed below currently encompass only a handful of all Web sites. Thus, it is too early to judge how effective these programs will ultimately be in serving as enforcement mechanisms to protect consumers' online privacy.

The Commission believes that there are additional steps that it can take, together with industry, and consumer and privacy groups, to build upon the progress in self-regulation to date and to work toward full implementation of effective online privacy protections. Some recent developments and plans for future work to achieve this goal are discussed below.

A. Recent Assessments of Web Sites' Compliance with Fair Information Practice Principles

Professor Mary Culnan of the McDonough School of Business at Georgetown University recently announced the results of two industry-funded surveys of commercial Web sites, conducted during the week of March 8, 1999. The Georgetown Internet Privacy Policy Survey ("GIPPS")[33] reports findings on the information practices of 361 Web sites drawn from a list of the 7,500 busiest servers on the World Wide Web.[34] Ninety-three percent of the sites in this survey collect personal information from consumers, and 66% post at least one disclosure about their information practices.[35] Forty-four percent of these sites post privacy policy notices.[36] Although differences in sampling methodology prevent direct comparisons between the GIPPS findings and the Commission's 1998 results,[37] the GIPPS Report does demonstrate the real progress industry has made in giving consumers notice of at least some information practices. On the other hand, only 10% of the sites in the GIPPS sample are implementing all four substantive fair information practice principles of Notice/Awareness, Choice/Consent, Access/Participation, and Security/Integrity.[38] The GIPPS Report findings discussed above are summarized in Figure 1.

Professor Culnan also conducted a census of the top 100 Web sites commissioned by the Online Privacy Alliance, a coalition of more than eighty online companies and trade associations that formed early in 1998 to encourage self-regulation in this area ("OPA Study").[39] As is true of the GIPPS sample, nearly all (99%) of the sites in the OPA Study collect personal information from consumers. Ninety-three percent of these sites provide at least one disclosure about their information practices, while 81% of these sites post privacy policy notices.[40] This represents continued progress since last year, when 71% of the sites in the Commission's 1998 "Most Popular" sample posted an information practice disclosure.[41] Only 22% of the sites in the OPA study address all four of the substantive fair information practice principles of Notice/Awareness, Choice/Consent, Access/Participation and Security/Integrity, however.[42]

FIGURE 1

	1999 GIPPS Report	1999 OPA Study
Number of sites in sample	361	100
Number of sites collecting personal information	337	99
Percent of sites in sample collecting personal information	93%	99%
Number of sites posting any privacy disclosure	238	93
Percent of sites in sample posting any privacy disclosure	66%	93%
Number of sites posting a privacy policy notice	157	81
Percent of sites in sample posting a privacy policy notice	44%	81%
Number of sites posting a disclosure for all four substantive fair information practice principles	36	22
Percent of sites in sample posting a disclosure for all four substantive fair information practice principles	10%	22%

The GIPPS and OPA Study results suggest that the majority of the more frequently-visited Web sites are implementing the basic Notice/Awareness principle by disclosing at least some of their information practices. The findings also indicate, however, that only a relatively small percentage of these sites is disclosing information practices that address all four substantive fair information practice principles. Both studies indicate that there has been real progress since the Commission issued its 1998 Report. Nevertheless, the low percentage of sites in both studies that address all four substantive fair information practice principles demonstrates that further improvement is required to effectively protect consumers' online privacy.

B. THE ONLINE PRIVACY ALLIANCE[43]

On June 22, 1998, the Online Privacy Alliance (OPA), a coalition of industry groups, announced its Online Privacy Guidelines, which apply to individually identifiable information

collected online from consumers.[44] Pursuant to these guidelines, OPA members agree to adopt and implement a posted privacy policy that provides comprehensive notice of their information practices. The notice includes a statement of what information is being collected from consumers and how it is being used; whether the information will be disclosed to third parties; consumers' choices regarding the collection, use and distribution of the information; data security measures; and the steps taken to ensure data quality and access to information. The OPA Guidelines also include provisions on choice, feasible consumer access to identifiable information, and data security, and call for self-enforcement mechanisms, such as online seal programs, that provide consumers with redress.

The OPA Guidelines have been used by the leading privacy seal programs, which have adapted them to fit their own program requirements. Unlike the seal programs, however, the OPA does not monitor members' compliance or provide sanctions for noncompliance. The central focus of OPA's efforts since release of its Guidelines has been business education to promote widespread adoption of online privacy policies.

C. Seal Programs

An encouraging development in the private sector's efforts toward self-regulation is the emergence of online seal programs. These programs require their licensees to abide by codes of online information practices and to submit to various types of compliance monitoring in order to display a privacy seal on their Web sites. Seal programs offer an easy way for consumers to identify Web sites that follow specified information practice principles, and for online businesses to demonstrate compliance with those principles.

1. TRUSTe[45]

TRUSTe, an independent, non-profit organization founded by the CommerceNet Consortium and the Electronic Frontier Foundation, was launched nearly two years ago, on June 10, 1997. The first online privacy seal program, TRUSTe currently has more than 500 licensees

representing a variety of industries.[45] Since December 1998, TRUSTe's license agreement,[47] which governs licensees' collection and use of "personally identifiable information,"[48] has taken a more comprehensive approach to privacy by requiring licensees to follow standards for notice, choice, access and security based upon the OPA Guidelines. The license agreement also requires licensees to submit to monitoring and oversight by TRUSTe, as well as a complaint resolution procedure.

The TRUSTe program includes third-party monitoring and periodic reviews of licensees' information practices to ensure compliance with program requirements. These reviews include "Web Site reviews," in which TRUSTe examines and monitors changes in licensees' privacy statements and tracks unique identifiers in licensees' databases (a practice known as "seeding") to determine whether consumers' requests to be removed from those databases are being honored; and "On-Site reviews" in which a third-party auditing firm can be called in, should TRUSTe have reason to believe that a licensee is not in compliance with the terms of the license agreement. Licensees must provide consumers with a way to submit concerns regarding their information practices, and agree to respond to all reasonable inquiries within five days. TRUSTe also plays a part in resolving consumer complaints. TRUSTe provides for public reporting of complaints, and, in appropriate circumstances, will refer complaints to the Commission.

2. BBBOnLine Privacy Seal Program[49]

BBB*OnLine*, a subsidiary of the Council of Better Business Bureaus, launched its privacy seal program for online businesses on March 17, 1999. Forty-two sites currently post BBB*OnLine* seals, and the program has received more than 300 applications. In order to be awarded the BBB*OnLine* Privacy Seal, applicants must post a privacy policy that comports with the program's information practice principles,[50] complete a "Compliance Assessment Questionnaire," and must agree to participate in a consumer dispute resolution system and to

submit to monitoring and review by BBB*OnLine*.[51]

The BBB*OnLine* Privacy Seal Program covers "individually identifiable information,"[52] as well as "prospect information," which is identifying, retrievable information that is collected by the company's Web site from one individual about another.[53] The BBB*OnLine* Privacy Seal Program's consumer complaint resolution procedure is bolstered by several compliance incentives, including public reporting of decisions, and suspension or revocation of the BBB*OnLine* seal, or referral to federal agencies, as sanctions for noncompliance. BBB*OnLine* has committed to adopting a third-party verification system, although this aspect of the program has not yet been implemented. The Commission looks forward to assessing BBB*OnLine*'s enforcement mechanisms when they are fully in place.

3. Other Seal Programs

Several other seal programs have been developed or are under development. One is CPA WebTrust, created by the American Institute of Certified Public Accountants ("AICPA") and the Canadian Institute of Chartered Accountants and announced in September 1997.[54] The CPA WebTrust program, which licenses the CPA WebTrust seal to qualifying certified public accountants, requires participating Web sites to disclose and adhere to stated business practices, maintain effective controls over the security and integrity of transactions, and to maintain effective controls to protect private customer information. Web sites are awarded the CPA WebTrust seal by certified public accountants who conduct quarterly audits to ensure compliance with the program's standards.

Although primarily intended to provide assurance for consumers that a site displaying the seal is a legitimate business that will process transactions and protect sensitive information like credit card numbers, CPA WebTrust also has a privacy component. The information practice requirements in the latest version of the program, introduced in May 1999, conform to the OPA Guidelines. Currently, 19 Web sites have been awarded the CPA WebTrust seal.

Industry sector-specific programs are also beginning to emerge. For example, in October

1998 the Interactive Digital Software Association ("IDSA") adopted its own fair information practice guidelines for its members' Web sites.[55] In addition, on June 1, 1999, the Entertainment Software Rating Board ("ESRB"), an independent rating system for entertainment software and interactive games established by IDSA in 1994, launched ESRB Privacy Online.[56] This online seal program requires participants to adhere to information practice standards that parallel the IDSA guidelines.[57] The program monitors compliance through a verification system that includes unannounced audits and seeding. The program also includes a consumer online hotline for reporting privacy violations and alternative dispute resolution services to resolve consumer complaints.

V. CONCLUSION

The self-regulatory initiatives described above, including the guidelines adopted by the OPA and the seal programs, reflect industry leaders' substantial effort and commitment to fair information practices. They should be commended for these efforts. Enforcement mechanisms that go beyond self-assessment are also gradually being implemented by the seal programs. Only a small minority of commercial Web sites, however, have joined these programs to date. Similarly, although the results of the GIPPS and OPA studies show that many online companies now understand the business case for protecting consumer privacy, they also show that the implementation of fair information practices is not widespread among commercial Web sites.

Based on these facts, the Commission believes that legislation to address online privacy is not appropriate at this time. We also believe that industry faces some substantial challenges. Specifically, the present challenge is to educate those companies which still do not understand the importance of consumer privacy and to create incentives for further progress toward effective, widespread implementation.

First, industry groups must continue to encourage widespread adoption of fair information practices. Companies like IBM, Microsoft and Disney, which have recently announced,

among other things, that they will forgo advertising on sites that do not adhere to fair information practices are to be commended for their efforts, which we hope will be emulated by their colleagues. These types of business-based initiatives are critical to making self-regulation meaningful because they can extend the reach of privacy protection to small and medium-sized businesses where there is great potential for e-commerce growth.

Second, industry should focus its attention on the substance of Web site information practices, ensuring that companies adhere to the core privacy principles discussed earlier. It may also be appropriate, at some point in the future, for the FTC to examine the online privacy seal programs and report to Congress on whether these programs provide effective privacy protections for consumers.

Finally, industry must work together with government and consumer groups to educate consumers about privacy protection on the Internet. The ultimate goal of such efforts, together with effective self-regulation, will be heightened consumer acceptance and confidence. Industry should also redouble its efforts to develop effective technology to provide consumers with tools they can use to safeguard their own privacy online.

The Commission has developed an agenda to address online privacy issues throughout the coming year as a way of encouraging and, ultimately, assessing further progress in self-regulation to protect consumer online privacy:

- The Commission will hold a public workshop on "online profiling," the practice of aggregating information about consumers' preferences and interests gathered primarily by tracking their movements online, and, in some cases, combining this information with personal information collected directly from consumers or contained in other databases. The workshop, jointly sponsored by the U.S. Department of Commerce, will examine online advertising firms' use of cookies and other tracking technologies to create targeted, user profile-based advertising campaigns.

- The Commission will hold a public workshop on the privacy implications of electronic identifiers that enhance Web sites' ability to track consumers' online behavior.

- In keeping with its history of fostering dialogue on online privacy issues among all stakeholders, the Commission will convene task forces of industry representatives and privacy and consumer advocates to develop strategies for furthering the implementation of fair information practices in the online environment.

  - One task force will focus upon understanding the costs and benefits of implementing fair information practices online, with particular emphasis on defining the parameters of the principles of consumer access to data and adequate security.

  - A second task force will address how incentives can be created to encourage the development of privacy-enhancing technologies, such as the World Wide Web Consortium's Platform for Privacy Preferences (P3P).

- The Commission, in partnership with the U.S. Department of Commerce, will promote private sector business education initiatives designed to encourage new online entrepreneurs engaged in commerce on the Web to adopt fair information practices.

- Finally, the Commission believes it is important to continue to monitor the progress of self-regulation, to determine whether the self-regulatory programs discussed in this report fulfill their promise. To that end, the Commission will conduct an online survey to reassess progress in Web sites' implementation of fair information practices, and will report its findings to Congress.

In undertaking these efforts, the Commission will be better able to assess industry progress in meeting its self-regulatory responsibilities, while fostering the implementation of effective protections for online privacy in a manner that promotes a flourishing electronic marketplace.

ENDNOTES

1. The Report is available on the Commission's Web site at http://www.ftc.gov/reports/privacy3/index.htm.

2. 1998 Report at 41.

3. 1998 Report at 42. Commission testimony on *Consumer Privacy on the World Wide Web* before the House Subcommittee on Telecommunications, Trade and Consumer Protection, Committee on Commerce (July 21, 1998) at 4-5 [hereinafter "1998 Privacy Testimony"] (available at http://www.ftc.gov/os/1998/9807/privac98.htm).

4. 1998 Privacy Testimony at 4. The Commission also presented a legislative model that Congress could consider in the event that then-nascent self-regulatory efforts did not result in widespread implementation of self-regulatory protections. *Id.* at 5-7.

5. Remarks of Secretary of Commerce William M. Daley, Feb. 5, 1999 (text available at http://204.193.246.62/public.nsf/docs/commerce-ftc-online-shopping-briefing).

6. The Boston Consulting Group, *The State of Online Retailing* 7 and App. A (Nov. 1998).

7. Internet Advertising Bureau, *Advertising Revenue Report* (May 1999) (major findings available at http://www.iab.net/news/content/1998results.html).

8. *Id.*

9. Intelliquest, Inc., *Worldwide Internet/Online Tracking Service 4th Quarter 1998 Report* (results available at http://www.intelliquest.com).

10. *See* Forrester Research, Inc., *Media & Technology Strategies: Making Users Pay* at 4-6 (1998).

11. *See, e.g.*, Rivka Tadjer, *"Following the Patron Path,"* ZD Internet Magazine, Dec. 1997, at 95; Thomas E. Weber, *"Software Lets Marketers Target Web Ads,"* Wall St. J., Apr. 21, 1997, at B1.

12. Lorrie Faith Cranor, et al., *Beyond Concern: Understanding Net Users' Attitudes About Online Privacy* at 5 (1999) [hereinafter "AT&T Study"] (available at http://www.research.att.com/projects/privacystudy).

13. Louis Harris & Associates, Inc., *National Consumers League: Consumers and the 21st Century* at 4 (1999).

14. AT&T Study at 2, 10.

15. Intelliquest, Inc., *Worldwide Internet/Online Tracking Service 1st Quarter 1999 Report* (findings summarized at http://www.intelliquest.com/press/release78.asp) (28%); Louis Harris & Associates, Inc. and Alan F. Westin, *E-Commerce & Privacy: What Net Users Want* at 1 (1998) (23%).

16. The Commission held its first public workshop on privacy in April 1995. In a series of hearings held in October and November 1995, the Commission examined the implications of globalization and technological innovation for competition issues and consumer protection issues, including privacy concerns. At a public workshop held in June 1996, the Commission examined Web site practices in the collection, use, and transfer of consumers' personal information; self-regulatory efforts and technological developments to enhance consumer privacy; consumer and business education efforts; the role of government in protecting online information privacy; and special issues raised by the online collection and use of information from and about children. The Commission held a second workshop in June 1997 to explore issues raised by individual reference services, as well as issues relating to unsolicited commercial e-mail, online privacy generally, and children's online privacy.

These efforts have served as a foundation for dialogue among members of the information industry and online business community, government representatives, privacy and consumer advocates, and experts in interactive technology. Further, the Commission and its staff have issued reports describing various privacy concerns in the electronic marketplace. *See, e.g., Individual Reference Services: A Federal Trade Commission Report to Congress* (December 1997); FTC Staff Report: *Public Workshop on Consumer Privacy on the Global Information Infrastructure* (December 1996); FTC Staff Report: *Anticipating the 21st Century: Consumer Protection Policy in the New High-Tech, Global Marketplace* (May 1996).

The Commission has also brought enforcement actions under Section 5 of the Federal Trade Commission Act to address deceptive online information practices. In 1998 the Commission announced its first Internet privacy case, in which GeoCities, operator of one of the most popular sites on the World Wide Web, agreed to settle Commission charges that it had misrepresented the purposes for which it was collecting personal identifying information from children and adults through its online membership application form and registration forms for children's activities on the GeoCities site. The settlement, which was made final in February 1999, prohibits GeoCities from misrepresenting the purposes for which it collects personal identifying information from or about consumers, including children. It also requires GeoCities to post a prominent privacy notice on its site, to establish a system to obtain parental consent before collecting personal information from children, and to offer individuals from whom it had previously collected personal information an opportunity to have that information deleted. GeoCities, Docket No. C-3849 (Feb. 12, 1999) (Final Decision and Order available at http://www.ftc.gov/os/1999/9902/9823015d&o.htm).

In its second Internet privacy case, the Commission recently announced for public comment a settlement with Liberty Financial Companies, Inc., operator of the Young Investor Web site. The Commission alleged, among other things, that the site falsely represented that personal information collected from children, including information about family finances, would be maintained anonymously. In fact, this information was maintained in identifiable form. The consent agreement would require Liberty Financial to

post a privacy policy on its children's sites and obtain verifiable consent before collecting personal identifying information from children. Liberty Financial, Case No. 9823522 (proposed consent agreement available at http://www.ftc.gov/os/1999/9905/lbtyord.htm).

17. 1998 Report at 7-11. In addition to the HEW Report, the major reports setting forth the core fair information practice principles are: The U.S. Privacy Protection Study Commission, *Personal Privacy in an Information Society* (1977); Organization for Economic Cooperation and Development, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980); U.S. Information Infrastructure Task Force, Information Policy Committee, Privacy Working Group, *Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information* (1995); U.S. Dept. of Commerce, *Privacy and the NII: Safeguarding Telecommunications-Related Personal Information* (1995); The European Union Directive on the Protection of Personal Data (1995); and the Canadian Standards Association, *Model Code for the Protection of Personal Information: A National Standard of Canada* (1996).

18. 1998 Report at 7-11.

19. Although choice in this context has been traditionally thought of as either "opt-in" (prior consent for use of information) or "opt-out" (limitation upon further use of information), *id.* at 9, interactive media hold the promise of making this paradigm obsolete through developments in technology. *Id.*

20. *Id.* at 9.

21. *Id.* at 10.

22. *Id.* at 10-11.

23. *Id.* at 23, 27.

24. *Id.* at 24, 28.

25. *Id.* at 31, 35, 37.

26. 1998 Privacy Testimony at 5-7.

27. Title XIII, Omnibus Consolidated and Emergency Supplemental Appropriations Act, 1999, Pub. L.105-277, 112 Stat. 2681, _____ (October 21, 1998), *reprinted at* 144 Cong. Rec. H11240-42 (Oct. 19, 1998). The goals of the Act are: (1) to enhance parental involvement in a child's online activities in order to protect the privacy of children in the online environment; (2) to help protect the safety of children in online fora such as chat rooms, home pages, and pen-pal services in which children may make public postings of identifying information; (3) to maintain the security of children's personal information collected online; and (4) to limit the collection of personal information from children without parental consent. 144 Cong. Rec. S12741 (Oct. 7, 1998) (Statement of Sen. Bryan).

28. Title XIII, Omnibus Consolidated and Emergency Supplemental Appropriations Act, 1999, Pub. L.105-277, 112 Stat. 2681, _____ (October 21, 1998), *reprinted at* 144 Cong. Rec. H11240-42 (Oct. 19, 1998).

29. *Id.*

30. 64 Fed. Reg. 22750 (1999) (to be codified at 16 C.F.R. pt. 312).

31. *Id.* at 22753-58 (Proposed Rule §§ 312.4-312.6)

32. *Id.* at 22759-60 (Proposed Rule § 312.10).

33. The report is available at http://www.msb.edu/faculty/culnanm/gippshome.html [hereinafter "GIPPS Report"]. The following analysis is based upon the Commission's review of the GIPPS Report itself; Commission staff did not have access to the underlying GIPPS data.

34. GIPPS Report at 1; App. B at 4. The list, a ranking of servers by number of unique visitors for the month of January 1999, was compiled by Media Metrix, a site traffic measurement company. As larger sites are more likely to have multiple servers, the largest sites on the Web had a greater chance of being selected for inclusion in the sample drawn for this survey. *See* GIPPS Report, App. A at 1; App. B at 9 n.iii.

35. GIPPS Report, App. A at 3, 5.

36. GIPPS Report, App. A at 5.

37. The Commission's 1998 Comprehensive Sample was drawn at random from all U.S., ".com" sites in the Dun & Bradstreet Electronic Commerce Registry, with the exception of insurance industry sites. 1998 Report, App. A at 2. Unlike the Media Metrix list used in the GIPPS sample, the Dun & Bradstreet Registry does not rank sites on the basis of user traffic.

38. The GIPPS results show that thirty-six sites in the sample (or 10%) posted at least one survey element, or disclosure, for each of the four substantive fair information practices. GIPPS Report at 10. Thirty-two of these sites (or 8.9%) also posted contact information. *Id.* and App. A at 12. Professor Culnan also reports the number of sites posting disclosures for the four substantive fair information practice principles and for contact information in two additional ways: as a percentage of sites in the sample that collect at least one type of personal information (9.5%); and as a percentage of sites in the sample that both collect at least one type of personal information and post a disclosure (13.6%). GIPPS Report, App. A at 12 (Table 8C).

39. Online Privacy Alliance, *Privacy and the Top 100 Sites: A Report to the Federal Trade Commission* (1999) (available at http://www.msb.edu/faculty/culnanm/gippshome.html). The following analysis is based upon the Commission's review of the OPA Study report itself; Commission staff did not have access to the underlying OPA Study data.

40. OPA Study at 3, 5, and 8.

41. 1998 Report at 28.

42. Twenty-two sites in the OPA Study (or 22%) posted at least one survey element, or disclosure, for each of the four substantive fair information practices. OPA Study at 9-10 and App. A at 10 (Table 6C). Nineteen of these sites (or 19%) also posted contact information. *Id.* Professor Culnan also reports the number of sites posting disclosures for the four substantive fair information practice principles in two additional ways: as a percentage of sites in the sample that collect at least one type of personal information (22.2%); and as a percentage of sites in the sample that both collect at least one type of personal information and post a disclosure (23.7%). OPA Study, App. A at 10 (Table 6C).

43. The information included in this section is drawn from the OPA Web site (http://www.privacyalliance.org) and OPA members' testimony before the Senate Judiciary Committee's Hearing on *Privacy in the Digital Age: Discussion of Issues Surrounding the Internet* on April 21, 1999. The testimony is available on the OPA Web site, and at http://www.senate.gov/~judiciary/42199kb.htm.

44. The Guidelines are available at http://www.privacyalliance.org/resources/ppguidelines.shtml.

45. The information in this section is taken from materials posted on TRUSTe's Web site, http://www.truste.org, and from public statements by TRUSTe staff.

46. Several hundred additional companies have joined the TRUSTe program but are not yet fully licensed. *See "TRUSTe Testifies Before House Judiciary Committee,"* May 27, 1999 (press release available at http://www.truste.org/about/about_committee.html).

47. Not all of TRUSTe's current licensees are subject to the latest version of the license agreement.

48. "Personally identifiable information" is defined as any information that can be used to identify, contact, or locate a person, including information that may be linked with identifiable information from other sources, or from which other personally identifiable information can easily be derived.

49. The information in this section is taken from materials posted on the BBB*Online* Web site, located at http://www.bbbonline.com, and from other public documents and statements by BBB*OnLine* staff.

50. The BBB*OnLine* Privacy Seal Program establishes requirements for notice, choice, access, and security. Comprehensive notice disclosures are required. Consumers must be allowed to prohibit unrelated uses of individually identifiable information not disclosed in the site's privacy policy and disclosure to third parties for marketing purposes. Consumers must also be permitted access to information about them to correct inaccuracies.

51. License fees to display the BBB*OnLine* Privacy logo are determined by a sliding scale according to the participant's revenues. Currently, the annual license fee ranges from $150 for companies with under $1 million in sales, to $3,000 for companies with sales over $2 billion.

52. "Individually identifiable information" is defined as information that (1) can be used to identify an individual, (2) is elicited by the company's Web site through active or passive means from the individual, and (3) is retrievable by the company in the ordinary course of business.

53. "Prospect information" would be collected when, for example, a visitor to a site orders a gift for another person and supplies that person's mailing address.

    It is not clear whether demographic information about a consumer that is collected at a site and tied to an identifier is covered by the BBB*Online* program, although licensees are required to provide notice if they merge or enhance individually identifiable information with data from third parties for the purposes of marketing products or services to the consumer.

54. Information about CPA WebTrust is available at http://www.cpawebtrust.org.

55. *Privacy in the Digital Age: Discussion of Issues Surrounding the Internet*, before the Senate Judiciary Comm., 106th Cong., April 21, 1999 (prepared statement of Gregory Fischbach).

56. Information regarding the ESRB privacy seal program is available at http://www.esrb.org.

57. The program guidelines include standards for notice and disclosure; choice; limiting data collection and retention; data integrity/security; data access; and enforcement and accountability.

Mr. TAUZIN. Thank you, Mr. Chairman.

The Chair is now pleased to welcome for his opening statement Commissioner Orson Swindle.

STATEMENT OF ORSON SWINDLE

Mr. SWINDLE. Thank you, Mr. Chairman. I appreciate the opportunity to speak before the committee and Mr. Markey and the rest of the committee members. I voted to submit "Self-Regulation and Privacy Online: A Report" to Congress because it ultimately reaches what I believe to be the correct and obvious conclusion, that no legislative action at this time is required.

I do not believe, however, that the report accurately reflects reality. Strangely, the unfavorable 1998 FTC study results are prominently described in the first seven pages of the report while the current and more favorable 1999 Georgetown survey results are only briefly mentioned in the middle of the report. In my mind, the report is a good example of damning with faint praise.

Second, the report overemphasizes the failure of industry to sufficiently implement all elements of comprehensive fair information practices, and I happen to agree with those practices, which the Commission first articulated only a year ago.

Third, the report only sparingly mentions the leadership on privacy issues that IBM, Microsoft, Disney, AOL, The Direct Marketing Association, privacy seal organizations and many others in the

private sector have demonstrated over the past year. The no legislative action recommendation appears at the very end of the report, almost as if the recommendation was some trivial afterthought.

The report should have emphasized prominently and in the beginning that cooperative and creative efforts by a public-private partnership have achieved substantial progress and will achieve more progress far more quickly than more laws and more regulation. I think significant progress has been made on the privacy issue. However, we must strive for more. We all recognize that.

More laws and regulations are not the answers. Industry, privacy and consumer advocates, and the Commission will make further progress by continuing to work hard and work together. I would caution industry that there are many in Congress and the government eager and willing to regulate the industry on privacy matters. Industry, both large and small, must continue to lead the way if it wishes to have the freedom to adopt privacy policies and practices in response to market incentives rather than government regulation.

Last month, the University of Texas Business School introduced a study of the current status of electronic commerce. It was one of the very first attempts to measure this thing that we talk about as the Internet economy. According to the study sponsored by Cisco Systems, the Internet economy generated an estimated $301 billion in revenue in 1998 and was responsible for the creation of over 1.2 million jobs. The Internet economy is already bigger than the energy industry, the telecommunications industry, and almost as big as the automobile industry. Retail Internet commerce is tripling annually. Obviously, consumers are not inching timidly into this new form of choice in purchasing.

As John Chambers, the CEO of Cisco Systems commented, "We need to be very careful not to rush in and really stifle the opportunity this gives our country in terms of job growth and economic growth by applying old world regulations to this new world." I could not agree with him more.

In our deliberations as law makers and regulators, let us remember first, do no harm.

Thank you, Mr. Chairman. I look forward to answering questions.

[The prepared statement of Hon. Orson Swindle follows:]

PREPARED STATEMENT OF HON. ORSON SWINDLE, COMMISSIONER, FEDERAL TRADE COMMISSION

Mr. Chairman, Members of the Committee, thank you for the opportunity to testify today.

I voted to submit "Self-Regulation and Privacy Online: A Report" (the "Report") to Congress *because it ultimately reaches the correct and obvious conclusion: no legislative action is necessary at this rime.*

I do not believe, however, that the Report accurately reflects reality. Strangely, the unfavorable 1998 FTC Study results are prominently described in the first seven pages of the Report, while the current and favorable 1999 Georgetown Survey results are only briefly mentioned in the middle of the Report. *The Report is a good example of damning with faint praise.*

Second, the Report overemphasizes the failure of industry to sufficiently implement all elements of comprehensive "fair information practices," which the Commission first articulated in detail only last year.

Third, the Report only sparingly mentions the leadership on privacy issues that IBM, Microsoft, Disney, AOL, The Direct Marketing Association, privacy seal orga-

nizations, and many others in the private sector have demonstrated over the past year.

The "no legislative action?" recommendation appears at the very end of the Report, almost as if the recommendation were some trivial afterthought. The Report Should have emphasized prominently that cooperative and creative efforts by a public-private partnership have achieved substantial progress and will achieve more progress far more quickly than will more laws and regulations.

I think significant progress has been made on the privacy issue. However, we must strive for more. More laws and regulation are not the answers. Industry, privacy and consumer advocates, and the Commission will make further progress by continuing to work hard and work together. I would caution industry that there are many in Congress and government eager and willing to regulate. Industry, both large and small, must continue to lead the way if it wishes to have the freedom to adopt privacy policies and practices in response to market incentives rather than government regulation.

Last month, the University of Texas Business School introduced a study of the current status of electronic commerce—one of the very first attempts to measure the Internet economy. According to the study, sponsored by Cisco Systems, the Internet economy generated an estimated $301 billion in revenue in 1998 and was responsible for over 1.2 million jobs.[1]

The Internet economy is already bigger than the energy industry ($230 billion) or the telecommunications industry ($270 billion) and is almost as big as the automobile industry ($350 billion). Retail Internet commerce is tripling annually. Obviously, consumers are not inching timidly into this new form of choice and purchasing.

As John Chambers, CEO of Cisco Systems Inc., commented, "We need to be very careful not to rush in and really stifle the opportunity this gives our country in terms of job growth and economic growth by applying old-world regulations to this new world." I could not agree more.

In our deliberations as lawmakers and regulators, let us remember first: "Do no harm."

Mr. TAUZIN. Thank you, Commissioner Swindle.

Now, the Chair is pleased to welcome Commissioner Anthony for her opening statement. Would you please pass the mike to her, Mr. Swindle? Thank you. Ms. Anthony.

STATEMENT OF HON. SHEILA F. ANTHONY

Ms. ANTHONY. Mr. Chairman, members of the subcommittee, thank you for holding this hearing today on an issue of great importance to the American people. As the commission's report states, only 10 percent of the well-traveled sites on the Internet in a recent survey had privacy disclosures that cover all four substantive information practices of notice, consent, access, and security.

Even among the top 100 most frequently visited Internet sites, only some 20 percent have privacy disclosures addressing these four principles. This chart illustrates the substantial gap that exists between the online collection of personal information in which 93 to 99 percent of the surveyed companies engaged, and the opportunity of customers, consumers, to transact their online business under notice, consent, access, and security. Some industry leaders have taken significant efforts to protect online privacy. To name a few, they are Disney Online, IBM, Microsoft, AT&T, Eastman Kodak, Dell Computer, Fox Broadcasting, the Boston Globe, the San Francisco Chronicle, the Wall Street Journal, CyberBills, Educational Communications, Inc., and worldtravelcenter.com.

Mr. TAUZIN. And the Commerce Committee.

[1] These estimates are based on worldwide sales of Internet-related products and services by U.S.-based companies.

Ms. ANTHONY. And the Commerce Committee and the FTC. In addition, the seal programs show promise. But some companies have made a business out of collecting, buying and selling individually identifiable information. I was shocked to discover shortly after I joined the Commission that at least one of the several information brokers operating in the marketplace had my name, my husband's name, our Social Security numbers, our address, the value of our home, the years in which our Social Security numbers were issued, our mothers' maiden names, the address where we lived before coming to Washington in 1978, our two daughters' names, their husbands' names, their Social Security numbers, their addresses at every place they had lived, and even our 3-year-old grandchild's name and Social Security number. I might add there were several mistakes in this report.

We in the government, especially those of us who have gone through a confirmation process or you who have stood through election are accustomed of having your lives laid bare. But most Americans are not and do not want to. The studies of which I am aware consistently show a high level of concern about online privacy. For example, a study just released by Harvard, MIT, AT&T Labs and the University of California, Irvine, in April found that 87 percent of Internet users were concerned about personal privacy threats. One year ago, these online privacy concerns were held by 81 percent of Internet users. So over the years, public concern has increased not decreased as shown plainly by this chart.

I respectfully disagree with my colleagues in that I believe the time is ripe for Congress to enact Federal legislation to protect online consumer privacy, at least to the extent of providing minimum Federal standards. As a whole, industry progress has been far too slow since the Commission first began encouraging the adoption of voluntary fair information practices in 1996.

Notice, while an essential first step, is not enough if the privacy policies themselves are toothless. I do believe that Congress is the appropriate place for the debate about this issue, and I notice that there are several bipartisan online privacy bills pending in both the House and the Senate, at least one, by members of this committee. These bills can serve as starting points to craft balanced privacy legislation.

I am concerned without widespread implementation of fair information practices on commercial web sites and absent effective privacy protections, several results are inevitable. First, the dissatisfaction of the American people will grow in pitch and intensity as it has in the past.

Second, a patchwork of State laws to protect online privacy will emerge. Several States, for example California, Connecticut, Delaware, Washington, and Maine have moved in that direction. Consider the confusing environment that could result for consumers, online marketers, and the courts under such a patchwork.

Third, consumer confidence will be undermined which will hinder the advancement of electronic commerce and trade. Sometimes the personal information such as health and financial information will require heightened security and protection. Without the widespread adoption of fair information practices, however, not even an across-the-board minimum standard of protection exists.

Let me conclude by saying that I am troubled by the results of the Georgetown surveys that show much less progress than I had hoped. I am pleased to say the Commission will continue its involvement in the privacy area, and our report sets out a number of initiatives for the coming year.

Thank you for the opportunity to share my views.

[The prepared statement of Hon. Sheila F. Anthony follows:]

PREPARED STATEMENT OF HON. SHEILA F. ANTHONY, COMMISSIONER, FEDERAL TRADE COMMISSION

Mr. Chairman and members of the Subcommittee on Telecommunications, Trade, and Consumer Protection, I am delighted to be here this morning, and I appreciate your holding this hearing today to address a topic of extreme importance to the American people. I will speak briefly about online privacy protection.

As the Commission's 1999 report to Congress states, only 10% of well-traveled Internet sites in a recent survey have privacy disclosures that speak to all four substantive fair information practice principles of notice, consent, access, and security.[1] Even among the top 100 most frequently visited Internet sites, only some 20% have privacy disclosures addressing these four principles.[2]

Last year I was asked to grade the online privacy performance of the industry as a whole. I generously gave industry a D+.[3] I expected industry's performance to substantially improve.

Some industry leaders have undertaken significant efforts to protect online privacy, including Disney Online, IBM, Microsoft, AT&T, Eastman Kodak, Dell Computer, Fox, the Boston Globe, the San Francisco Chronicle, the Wall Street Journal, CyberBills, Educational Communications, Inc., and Worldtravelcenter.com. In addition, the seal programs show promise. But some companies have made a business out of collecting, buying, and selling individually identifiable information online.

I was shocked to discover, shortly after I joined the Commission, that at least one of the several "information brokers" operating in the marketplace had my name and my husband's name, our address, the value of our house, our social security numbers, the year they were issued, our mothers' maiden names, the address where we lived before coming to Washington in 1978, our two daughters' names, their husbands' names, their social security numbers, every address where they had lived, and even our 3-year-old grandchild's name and social security number. I might add that there were several mistakes in that report on me.

We in the government, and especially those of us who have experienced a confirmation process or you who have stood for election, know what it is to have our private lives laid bare. But most Americans do not, nor do they want to.

I am disappointed that sufficient progress by industry as a whole has not been made toward the protection of online privacy under a self-regulatory approach. Such a lack of progress is surprising, given the Commission's clear articulation of fair information practice principles in our 1998 Online Privacy Report. Even prior to my arrival at the Commission, the Agency had encouraged industry to adopt voluntary fair information practices.[4] Indeed, Secretary of Commerce Brown plainly expressed the fair information principles of notice and consent as long ago as 1995.[5] The self-regulatory environment has not advanced the ball as far as I would have expected. Thus, consumer privacy remains an issue about which 87% of online Americans, including me, are extremely concerned.

---

[1] FEDERAL TRADE COMMISSION, SELF-REGULATION AND PRIVACY ONLINE: A REPORT TO CONGRESS, 7 n.10. (July 1999) [hereinafter REPORT].

[2] REPORT at 7 n.42; *see FIPs Compliance Gap*, chart *infra*.

[3] Statement of the Honorable Sheila F. Anthony before the House of Representatives, Committee on Commerce, Subcommittee on Telecommunications, Trade, and Consumer Protection (July 21, 1998).

[4] Federal Trade Commission Letter to Senator John McCain 6 n.2 (July 31, 1997).

[5] RONALD H. BROWN, U.S. DEPARTMENT OF COMMERCE, PRIVACY AND THE NII: SAFEGUARDING TELECOMMUNICATIONS-RELATED PERSONAL INFORMATION pt. III.A-B(Oct. 1995), *available at* NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION, *Privacy and the NII: Safeguarding Telecommunications-Reloted Personal Information* (visited June 23, 1999) <http://www.ntia.doc.gov/ntiahome/ privwhitepaper.html> at 13-16.

Privacy is "one of our most cherished freedoms."[6] Too often, however, the debate about privacy and the protection of personal information that is surreptitiously gathered takes on an ethereal quality and looks for proof of direct harm. Direct harm is not necessary to justify fair information practices, but is evident, for example, in cases of cyberstalking and identity theft.

The American public deeply values its privacy, quite apart from notions of direct harm. The studies of which I am aware consistently show a high level of concern about online privacy. For example, a study just released by Harvard, MIT, AT&T Labs, and the University of California-Irvine in April found, as I mentioned earlier, that 87% of Internet users were concerned about personal privacy threats.[7] One year ago these online privacy concerns were held by 81% of Internet users.[8] So, over the years public concern has increased, not decreased.[9]

In reporting on the status of self-regulation and online privacy protection, the Commission has fulfilled its promises to collect information regarding online privacy and provide a response to the Congress.[10] I respectfully disagree with my colleagues in that I believe that the time is ripe for Congress to enact federal legislation to protect online consumer privacy, at least to the extent of providing minimum federal standards. As a whole, industry progress has been far too slow since the Commission first began encouraging the adoption of voluntary fair information practices in 1996.[11] Notice, while an essential step, is not enough if the privacy practices themselves are toothless. I do believe that Congress is the appropriate place for the debate on the online protection of consumer privacy, and I note that several bipartisan online privacy bills are pending in both the House and the Senate, including at least one by members of this Committee. These bills can serve as starting points to craft balanced privacy legislation.

I am concerned that, without widespread implementation of fair information practices on commercial Web sites and absent effective privacy protections, several results are inevitable. First, the dissatisfaction of the American people will grow, as it has in the past, in both pitch and intensity.

Second, I am concerned that a patchwork of state laws to protect online privacy will emerge. Several states, for example, California, Connecticut, Delaware, Washington, and Maine, have moved in that direction.[12] Consider the confusing environment that could result for consumers, online marketers, and the courts under such a legal patchwork.[13]

---

[6] Statement of President Clinton, Morgan State University (May 18, 1997), *available at* THE WHITE HOUSE, *Commencement Address by the President at Morgan State University* (May 18, 1997) http://www.pub.whitehouse. gov/ uri-res/I2R?urn:pdi://oma.eop.gov.us/1997/5/19/1.text.1.

[7] LORRIE FAITH CRANOR ET AL., BEYOND CONCERN: UNDERSTANDING NET USERS' ATTITUDES ABOUT ONLINE PRIVACY, RESEARCH TECHNICAL REPORT, TR 99.4.3 (Apr. 14, 1999), *available at* AT&T LABS, *Beyond Concern: Understanding Net Users' Attitudes About Online Privacy* 3, 5-6 (visited June 22, 1999) <http://www.research.att. com/library/trs/TRs/99/99.4/99.4.3/report.htm [hereinafter AT&T Labs].

[8] *See id.*, *available at* AT&T Labs, *supra* note 7, at 4.

[9] *See Growing Public Concern*, chart *infra;* CRANOR, *supra* note 7, *available at* AT&T Labs, *supra* note 7, at 5-6 (1999 figure); LOUIS HARRIS & ASSOCIATES, *Privacy & American Business, summarized in* PRIVACY EXCHANGE, *Consumers & Credit Reporting 1994* (visited July 6, 1999) <http:www.privacyexchange.org/iss/surveys/con—cre. html> at 1 n.1 (1993 figure); LOUIS HARRIS & ASSOCIATES, *The Road After 1984, summarized in* EQUIFAX, *Equifax Executive Summary 1990* (visited July 6, 1999) <http:www.privacyexchange.org/iss/surveys/eqfx.execsum.1990. html> at 1 (1983 figure); LOUIS HARRIS & ASSOCIATES, *Dimensions of Privacy, summarized in* EQUIFAX, *Equifax Executive Summary 1990, supra*, at 1 (1978 figure).

[10] *See* Letter to Senator McCain, *supra* note 4; FEDERAL TRADE COMMISSION, PRIVACY ONLINE: A REPORT TO CONGRESS (June 1998).

[11] *See* FEDERAL TRADE COMMISSION, *Public Workshop on Consumer Privacy on the Global Information Infrastructure*, Staff Rept. (Dec. 1996).

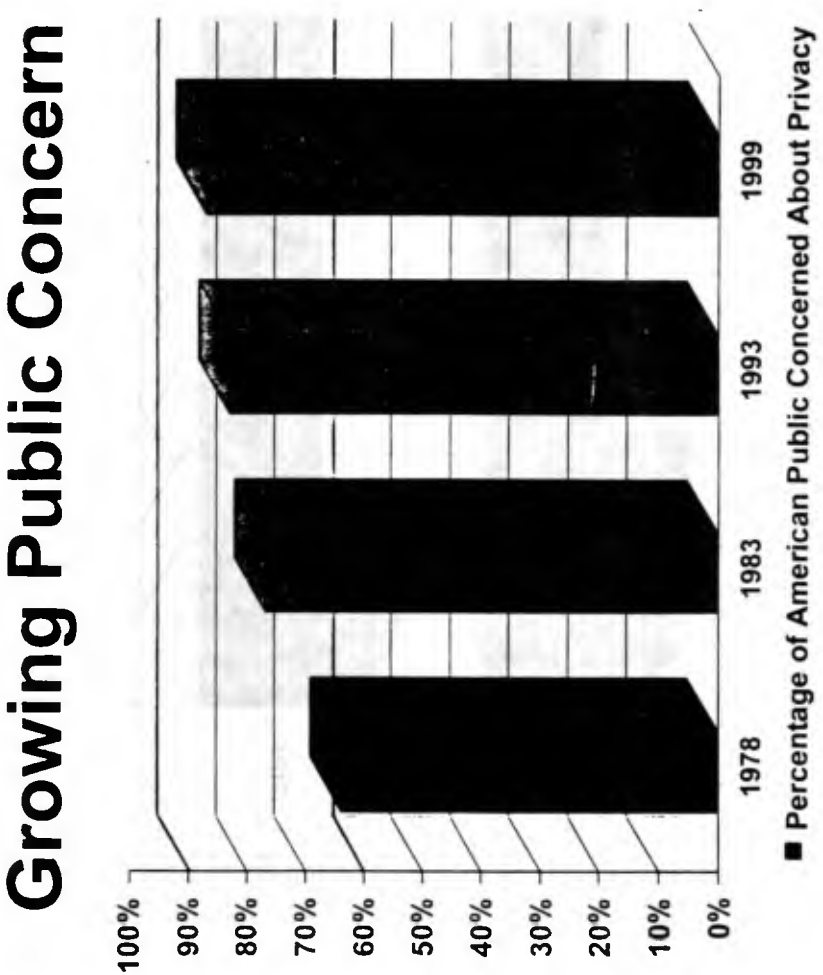
[12] *See, e.g.*, Conn. H. B. 6895, File No. 608, *as amended by* House Amendment Schedule A (reissued and approved by Legislative Commissioner on May 7, 1999) (passing law to prohibit state from requiring social security numbers of voter registrars); Cal. S.B. 417, Supermarket Club Card Disclosure Act of 1999 (heard June 15, 1999 by Assembly Committee on Consumer Protection, Governmental Efficiency & Economic Development); Del. H.B. 100 (House concurred in Senate amendments with additional amendments and forwarded bill to Senate for concurrence on June 17, 1999) (making videography or photography where reasonable expectation of privacy exists a felony); Wash. H.B. 2220 (to House Committee on Criminal Justice and Corrections on Feb. 22, 1999), *amending* ch. 9.73 RCW (making visual surveillance where reasonable expectation of privacy exists a misdemeanor); *see also* Thomas Shapley, *A Move to Ban Videos that Invade Privacy*, SEATTLE POST-INTELLIGENCER, Mar. 2, 1999, *available at* SEATTLE POST-INTELLIGENCER, *Seattle PI-Plus* (visited June 24, 1999) <http://www.seattle-pi.com/local/peep02. shtml>; Maine S.P. 93—L.D. 232—P.L. 17 (interim enactment on Mar. 19, 1999), *amending* §1 20-A MRSA §6001, *as amended by* P.L. 1989, c. 911 §1.

[13] The point about courts goes to establishing a uniform legal standard of a "legitimate expectation of privacy." *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 735 (1979).

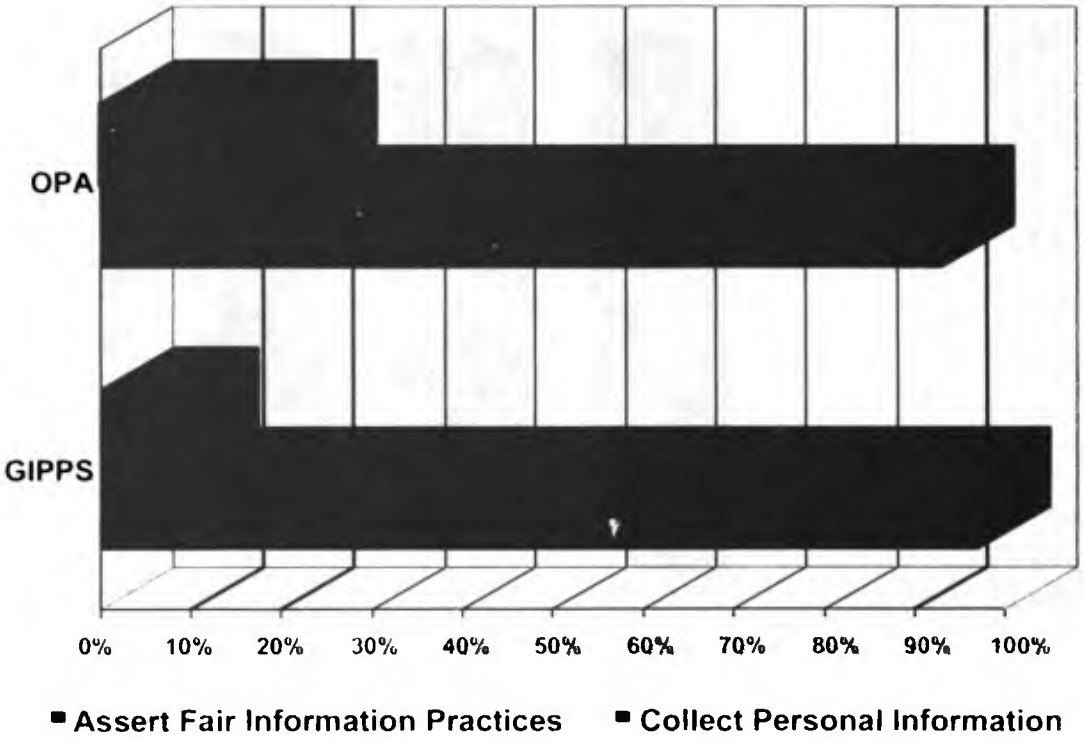
Third, I am concerned that the absence of online privacy protections will continue to undermine consumer confidence and hinder the advancement of electronic commerce and trade, specifically of trade with the European Union and its 320 million consumers. Some types of personal information, such as health and financial information, will require heightened privacy protections. Without the widescale adoption of fair information practices, however, not even an across-the-board minimum standard of protection exists.

Let me conclude by saying that I am troubled by the results of the Georgetown surveys that show much less progress than I had hoped. I am pleased to say that the Commission will continue its involvement in the privacy arena, and our report sets out a number of initiatives for the coming year.

Thank you for the opportunity to share my views.



FIPs Compliance Gap



Mr. TAUZIN. Thank you, Commissioner Anthony.

Following is the Honorable Mozelle Thompson of the Federal Trade Commission. Commissioner Thompson.

STATEMENT OF HON. MOZELLE W. THOMPSON

Mr. THOMPSON. Good morning, Mr. Chairman. I also thank the committee for allowing us to appear this morning.

Today we discuss the FTC's latest report on online privacy. Almost exactly a year ago, we appeared before this committee to discuss the state of that issue. At that time, we noted that consumer's confidence that their personal information would not be misused was a key element for gaining consumer acceptance for the electronic marketplace. Yet we were disappointed about industry progress.

I specifically voiced my concerns about coverage, the breadth of total web sites actually posting privacy policies, and the development and implementation of enforcement mechanisms. Those concerns remain. Now 1 year later, I find the record of progress mixed.

If we are going to be a leader in a global system of electronic commerce and e-commerce is going to continue to lead our new economy, we must reach collective understanding on principles that will provide consumers with the confidence that they need to accept e-commerce as a way of life. I would point out that the Commission is already on record in our testimony last July as to the exact elements we consider necessary to ensure fair information practices.

During the past year, industry leaders have expended substantial effort to build self-regulatory programs. They should be commended for their efforts and encouraged to buildupon them. However, as the Georgetown and OPA studies clearly show, while many leading online companies understand the business case for protecting consumer privacy, the implementation of their information practices is not widespread among commercial web sites.

In fact, a mere 10 percent of the companies in the Georgetown survey have done so. Although the OPA does not audit its members for compliance with privacy guidelines, the results of its own studies show that only 22 percent of the top 100 web sites, most of which are OPA members, have implemented all four elements of fair information practices. These findings suggest that even these industry leaders are only slowly rising to the challenge they have set.

As our report suggests, the important challenges to be addressed include reaching those businesses that have not taken steps to protect consumer privacy, especially small- and medium-sized businesses that will provide the real base for real growth in e-commerce and encouraging widespread adoption of all of the information practices including educating consumers about the value of self-regulatory efforts. The workshops and other activities that the Commission has planned for the coming months are designed to help us pinpoint specific problem areas for action. Congressional review of privacy issues is also helpful in this regard, and I feel strongly that there is a value to continued hearings and debate about legislative proposals.

And so, despite my concerns about the pace of industry progress, I believe it may be more appropriate to defer decision on legislative

action until our newly developed agenda sheds more light on these issues. I continue to be hopeful that industry can solve this problem. The recent initiatives by IBM, Microsoft, Disney, and others on Internet advertising are steps in the right direction. But I would ask the industry redouble its efforts to develop effective technological tools that consumers can use to safeguard their own privacy online because even well-crafted legislation will not achieve 100 percent compliance. Ideally, easy to use technology will empower consumers by allowing them to predetermine the circumstances under which they will share personal information. I am pleased to note that one of our proposed workshops for the coming months deals specifically with this issue.

In sum, achieving a robust level of privacy protection will require cooperation between industry, government, and consumers. While we have chosen to let industry lead in solving this public policy problem, public confidence in electronic commerce will erode if they fail to live up to the challenge. Ultimately, government officials like us are directly accountable to the public, and we must also continue to play a role in shaping solutions. In any case, the FTC will continue to pursue its enforcement role against those who deceive consumers by misusing personal data.

So has progress been made since the last report to Congress? Absolutely. Have we solved the problem of online privacy? No. But I believe that self-regulation will succeed only if industry acts on the specific shortcomings that these recent studies document. Moreover, Congress, the administration, and others must remain vigilant and should not foreclose the possibility of legislative and regulatory action if we cannot make swift and significant additional progress. Thank you.

[The prepared statement of Mozelle W. Thompson follows:]

PREPARED STATEMENT OF HON. MOZELLE W. THOMPSON, COMMISSIONER, FEDERAL TRADE COMMISSION

I am pleased to appear before the Commerce Committee with my fellow Commissioners to discuss the FTC's latest report on online privacy. As you are aware, the Commission has spent much time and energy working on this issue, and each of us thought it important to share our individual views and insights.

Almost exactly one year ago, we appeared before this Committee to discuss the state of on-line privacy. At that time, we noted that consumers' confidence that their personal information would not be misused was a key element for gaining consumer acceptance for the electronic marketplace; yet, we were "disappointed" about industry progress. I specifically voiced my concerns about coverage (i.e., the breadth of total web sites actually posting privacy policies) and the development and implementation of enforcement mechanisms. Now, one year later (and three years after the FTC first started working with industry on Internet issues), I find the record of progress is mixed.

If we are going to be the leader in a global system of electronic commerce, and e-commerce is going to continue to lead our "New Economy", we must reach a collective understanding on principles that will provide consumers with the confidence they need to accept e-commerce as a way of life. And I would point out that the Commission is already on record in our testimony of last July as to the exact elements that we consider necessary to ensure fair information practices.

During the past year, industry leaders have expended substantial effort to build self regulatory programs. They should be commended for these efforts and encouraged to build upon them. However, as the Georgetown and OPA studies clearly show, while many leading online companies understand the business case for protecting consumer privacy, the implementation of fair information practices is not widespread among commercial web sites. In fact, a mere ten percent of companies in the survey have done so. Although the OPA does not audit its members for compliance with its privacy guidelines, the results of its own study show that only 22

percent of the top 100 web sites (most of which are OPA members) have implemented all four elements of fair information practices. These findings suggest that even these industry leaders are only slowly rising to the challenge they have set.

As our report suggests, the most important challenges to be addressed include:

1) Reaching those businesses which have not taken steps to protect consumer privacy, especially small and medium-sized businesses which will provide the base for real growth in e-commerce; and
2) Encouraging widespread adoption of all of the fair information practices, including educating consumers about the value of these self-regulatory efforts.

The workshops and other activities the Commission has planned for the coming months are designed to help us pinpoint specific problem areas for action. Congressional review of privacy issues is also helpful in this regard and I feel strongly that there is a value to continued hearings and debate about legislative proposals. And so, despite my concerns about the pace of industry progress on privacy, I believe that it may be more appropriate to defer a decision on legislative action until our newly developed agenda sheds more light on these issues.

I continue to be hopeful that industry can solve this problem. Recent initiatives by IBM, Microsoft and Disney on Internet advertising are steps in the right direction. I would also ask industry to redouble its efforts to develop effective technology tools that consumers can use to safeguard their own privacy on line, because even well-crafted legislation will not achieve 100 percent compliance with fair information practices. Ideally, easy-to-use technology will empower consumers by allowing them to predetermine the circumstances under which they will share personal information. I am pleased to note that one of our proposed workshops for the coming months deals specifically with these issues.

In sum, achieving a robust level of privacy protection will require cooperation between industry, government and consumers. While we have chosen to let industry lead in solving this public policy problem, public confidence in electronic commerce will erode if they fail to live up to the challenge. Ultimately, government officials like us are directly accountable to the public and we must also continue to play a role in shaping solutions to the privacy problem. In any case, the FTC will continue to pursue its enforcement role against those who deceive consumers by misusing their personal information.

Has progress been made since our last report to Congress? Absolutely. Have we solved the problem of online privacy? Of course not. But, I believe that self-regulation will succeed only if industry acts on the specific shortcomings that these recent studies document. Moreover, Congress and the Administration must remain vigilant and should not foreclose the possibility of legislative and regulatory action if we cannot make swift and significant additional progress.

Mr. TAUZIN. Thank you, Commissioner Thompson.

Let me ask you all quickly now what I had asked you to do at the beginning. Starting with you, Mr. Chairman, you gave the industry a considerable room for improve grade last year. What do you give them this year?

I am sorry, you gave them an incomplete.

Mr. PITOFSKY. I have to break it down in two ways. If the question is how much progress they have made over the last year, I would give them a pretty good grade. I would give them a B plus, maybe even better than that. If the question is are we there yet, do we have a privacy policy that is acceptable to all of us, I would still say they are down around a C, and there is a long way to go.

Mr. TAUZIN. Let's go to you, Mr. Swindle. You gave them a rising D last year.

Mr. SWINDLE. Yes, sir. And I agree with the chairman on his assessment and would point out that we will get there. I think the cooperation between industry and consumer privacy groups and the FTC in our role as regulators and enforcers, will get us there.

Mr. TAUZIN. You gave them an overall C with a B plus for improvement. Ms. Anthony, you gave them a D plus last time, barely passing.

Ms. ANTHONY. This year I would give the leaders of the class, the industries whose names I mentioned this morning and others who have adopted all four information practices an A. They deserve it. They have stepped up to the plate. Industry as a whole still gets get a D plus in my view.

Mr. TAUZIN. Mr. Thompson, you said considerable room for improvement. I have seen that in my report a few times. What does that mean? Are you prepared to raise that grade?

Mr. THOMPSON. I would give them a C minus. While I still think there are some industry leaders, unfortunately from a consumer's perspective, the industry is going to be judged by its totality and not necessarily by its individuals.

Mr. TAUZIN. The reason I did this, of course, is because it kind of—perhaps as we go through these hearings it kind of gauges for us where you see the progress of the industry and where it is currently positioned.

Let me first thank Chairman Pitofsky and all of you, the commissioners of the FTC, for the work that you are doing. I think the oversight, consumer education forums, I think are critical elements of industry progress. Much of the progress that I think that you have cited today can be attributed to the fact that you are doing such good work, and I want to commend you for it and encourage you.

Let me ask you in that regard. In that, 66 percent of the sites now have at least some notice policy, that notice may say that we collect no information or it may say we collect it and here is our policy. In regard to that—and Mr. Chairman, you sort of agreed with Mr. Markey that the four elements of a good notice policy would be notice, consent, access, and security.

Has anyone—the seal organizations or OPA—has anyone ever considered doing what the old Siskel and Roberts thing used to do with movies? Some kind of rating system, but not a Government imposed one; a private rating system so that consumers have an easy way of gauging whether or not this is a good privacy policy or a bad one? For example, a four star system for those that have all four elements or three stars that have all three out of the four?

If we are going to have self-regulation, if consumers are going to look at these notices and make judgments about whether there is a site they want to trust, this is a business they want to deal with, this is a service provider who is literally helping them deal with companies or firms to which they can trust for their information, should there be a simple way for them to gauge how well or how good that industry is, in fact, performing on a privacy policy? Is that a good idea, or is that something you would encourage in the private industry? Mr. Pitofsky.

Mr. PITOFSKY. On your first question, I don't really know what every one of these seal groups—there must be almost a half dozen of them now. I think as to most of them, the ones that I know the best, I would grade them on a pass-fail basis. Either you get the seal or you don't get the seal. The seal is an indication that people are abiding by the information practices.

Is it a good idea? I'm not sure.

I certainly think that the pass/fail with monitoring and enforcement is critical. If you want to go further than that, two stars,

three stars, four stars, it wouldn't hurt. The more information in the marketplace, the better off consumers are. I guess I would think it is a good approach. I would be concerned about administration, who is going to make these decisions between two stars and three stars. It may be that it is easier and better and adequate to go pass/fail.

Mr. TAUZIN. In regards to—Siskel and Ebert. I don't know why I said Roberts.

The concern that some have expressed about the bad players, and assuming everybody continues to make progress, but there are still some bad players out there who just refuse to put up a notice policy, refuse to put up any privacy. Some will say, well, then, let the consumer beware. If there is no notice policy, don't deal with those people.

Others would say that there ought to be some fallback, some safety net to make sure that those individuals who will not agree to be part of the online privacy organization or the alliance part of one of the seal programs, there ought to be some sort of fallback requirement for someone who refuses to submit to self-regulation within the industry.

What are your thoughts on that?

Mr. PITOFSKY. Let me start, and then I will ask my colleagues to pitch in. That is a problem with self-regulation in every sector of the economy. No matter how good self-regulation is, there are a few sellers who will just ignore it. You don't get 100 percent law enforcement either when you pass a law, although it can be argued that you can get closer to universal coverage with a law than with self-regulation.

I do believe that once the seals are adopted and effective that buyers will then have the information and they can protect their own interests. There was a study that came out just last week that says that most people, if they have notice and an opportunity to opt out, are content. That is really what they want. We are talking about 85, 86, 87 percent. So most people will be satisfied with that. This is an Alan Westin study that was published last week.

So I think giving people information, letting them protect their own interests, is a pretty good way to go.

Mr. TAUZIN. Anybody else want to comment on that? Ms. Anthony.

Ms. ANTHONY. My comment is that self-regulation doesn't need to end if Federal legislation establishing a basic standard exists. We have self-regulation in a lot of industries where there is a baseline minimum standard set by the Congress.

The seal programs do furnish an impetus to industry, and some comfort for consumers. But at present, it may be difficult for consumers to distinguish among the various seal programs. So that would be my comment. Self-regulation doesn't need to end, and the seal programs are a good way to continue.

Mr. TAUZIN. Anyone else? Mr. Thompson?

Mr. THOMPSON. Sure. I think your question was an important one, in that is there a core group that you might not be able to get to, and how big is it? I think that that is one of the things that we may try to assess because it is important to look at scale here as well. If you take all of the companies who are in seal programs

now, who are applying, have the application pending, if you take the companies in the online privacy alliance, and add that all together, you maybe have 1,000 companies. Now, there are a million Web sites out there. If you assume that only 1 percent actually sell to people, that is 10,000.

So what we are talking about is how to get the market moving so that there is a condition under which consumers feel comfortable that their privacy is going to be protected. It is going to take a larger effort on the part of government, industry and consumers alike. So there probably isn't any one element.

Mr. TAUZIN. Mr. Swindle.

Mr. SWINDLE. Yes, sir. I believe the question had to do with the existence of bad players, people who will perhaps refuse to participate in a voluntary program of seals. I call it the bad player assumption, that is, those who do not participate are bad players. I think that is a highly questionable assumption that everybody who doesn't have a privacy statement is doing something wrong. Commercial Web sites are increasing at some indescribable rate right now. So the reality is, we are never, ever going to have everybody under any kind of program, seals or laws or otherwise. That is just a reality.

With regard to the 10,000 commercial sites versus 1,000 seal programs, I think a better way to look at it is to focus on the sites that people visit the most to do commerce. We can narrow this thing down through survey techniques to discover where 90 percent of the people are going. If those sites have privacy policies, I think we are accomplishing or getting toward accomplishing our goal. I think the point that I would like to make is first, let's don't assume that anybody who doesn't have a privacy policy is bad. This country is not founded on that principle. Second, if we keep encouraging and working toward it, we will get there.

One more point, Mr. Chairman. The problem that I see, when you establish a law that says you will all have it, then you have to enforce it. I am trying to imagine how the FTC or any other agency can enforce this. Then, if you do not obey the law, and it could be that you didn't know you had to and many people like that, then we must punish. That represents a heck of a dilemma for us in government, I think.

Mr. TAUZIN. We will leave that issue, and I will ask my last question, but just to let you know that what is hanging out there is a question as to whether or not there is anything either the government can do through the FTC or through the legislative process that encourages people to want to be part of a self-policing operation, rather than to submit some system of either government regulatory authority or what have you. That is sort of hanging out there. I don't think we get to the answer until we know exactly what that universe of bad—so-called, maybe, bad players is.

Last question. The Washington Post, June 27, 1999. Uncle Sam has all your numbers.

Chairman Bliley today, before most of the members got here, announced that our Commerce Committee is posting a privacy policy. The FTC has posted its own privacy policy. I want to commend Chairman Bliley again and commend the FTC for your examples

of government agencies, saying what we are going to do with information we obtain in our work in regard to constituents.

But, here is the headline and the story in the Washington Post, June 27, 1999: As part of a new and aggressive effort to track down parents for child support, the Federal Government has created a vast, computerized data monitoring system that includes all individuals with new jobs and names and addresses, Social Security numbers and wages of nearly every working adult in the United States. Government agencies have long gathered personal information for specific reasons, such as collecting taxes, but never before has a Federal official had the legal authority or technical ability to locate so many Americans found to be delinquent parents or such potential to keep tabs on Americans accused of nothing.

The system was established under the little known part of the law forming welfare reform a few years ago. Starting next month, the system will reach further. Large banks and other financial institutions will be obliged to search for data about delinquent parents by name on behalf of the government providing authorities with details about bank accounts, money markets, mutual funds, other holdings of the parents, et cetera.

The story goes on to detail about other government data collection systems at the IRS and at other Federal agencies dealing with citizens.

Mr. Pitofsky, is anybody doing any analysis of how well Government itself is providing privacy notices and privacy protections in regards to how it gathers information on citizens in this country?

Mr. PITOFSKY. We have not been investigating collection of data by the government. But I do—now I would like to join my colleague, Shiela Anthony here. I had the same reaction when I first came to the Commission this time around.

It is astonishing how much information is collected in various ways, and this isn't just an online issue now. We are talking online, off-line, collection of information in a variety of ways. I know Congress is concerned about this. I know that members have been addressing it, and I really do think that this is something that we have to pay attention to.

When people realize how much information is available about them for a price, they are shocked at the sort of resume of information that Commissioner Anthony noted. And we do have to keep an eye on this issue.

Often information is collected with what purports to be good reasons, but you never know how it is actually used.

Mr. TAUZIN. But no one is doing any kind of analysis of government collection of data and governments and agencies of government's ability or willingness to post any kind of policy on the use of that data and the collection of that data?

Mr. PITOFSKY. I don't know about no one. We have not—that is a little outside our jurisdiction.

Mr. TAUZIN. Mr. Swindle.

Mr. SWINDLE. Mr. Chairman, I applaud you bringing up this subject, because when I saw the article back on June 27 or whenever it was, my first reaction was that I was appalled that this kind of an operation could come into existence in today's environment where we have so many—I mean there are daily stories about con-

sumer and privacy advocates, and I think in a great sense rightfully, clamoring for something to get better in this matter of protecting people's privacy.

I have subsequently been astounded that there has been no clamoring on this particular point. In fact, if I recall correctly, there has only been about a 1-day story on that. It just sort of disappeared. If people are concerned about mom and pop operations selling chile sauce over the Internet not having a privacy statement, where is the concern about the Federal Government collecting data on every single person in this country?

Mr. TAUZIN. Obviously, it is being collected in many cases for a good purpose. The question is, what can it be used for and what are the rules? Mr. Thompson.

Mr. THOMPSON. Just two short points. One is, I don't want us to forget that there is still the Privacy Act. It covers the Federal Government and contains limits on how we use and share information about individuals in this country. That is one.

Second of all, I am aware that the folks at the Office of Management and Budget are working with agencies right now to work on their Web sites, to post privacy policies. So I know that is an initiative that they are undertaking right now.

Mr. TAUZIN. Thank you, Mr. Commissioner.

The Chair now recognizes the gentleman from Massachusetts, Mr. Markey.

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

First of all, with regard to some of the grades that were given out here today to the online industry, I think we really are in the era of great inflation, Mr. Chairman. Giving a B plus to this industry and its effort is, from my perspective, absolutely inappropriate. This industry deserves a big, fat F. It is not, as an industry, providing real privacy to consumers in our country online. Ninety percent of the industry is auditing the course, the Georgetown study makes that clear.

Now, if we are going to deal with this realistically, we are going to say, I guess that is what I am hearing from some of the people out here, that we believe that we really don't need Federal agencies, and if we don't need the Securities and Exchange Commission, because most people are honest. We don't need the Federal Trade Commission. We can repeal most of the statutes we have empowered them to look at in terms of fraud, because most people are honest.

If we believe that this industry is ever going to reach 100 percent compliance, and I guess that is what we are going to hear today, that you believe that self-regulation will lead to 100 percent compliance, then we don't need any laws in most areas where the Federal Trade Commission is now empowered, or with the Securities and Exchange Commission, or with the Federal Communications Commission. Because as Mr. Swindle is saying, that is not what this country is all about. We don't believe that people do things wrong. I don't know why anyone would even want to serve on a Commission like this, Mr. Swindle, if that is what we believe.

Mr. SWINDLE. Can I respond, sir?

Mr. MARKEY. When I finish, yes.

Mr. SWINDLE. Yes.

Mr. MARKEY. Mr. Pitofsky, do you believe that core privacy criteria of notice, choice, access, and security are a good idea, a noble gesture by online sites, or a necessary consumer protection for privacy online?

Mr. PITOFSKY. Necessary protection.

Mr. MARKEY. Are they essential?

Mr. PITOFSKY. Yes, I believe they are. The only question is how to get there.

Mr. MARKEY. Is disclosure alone enough protection?

Mr. PITOFSKY. Well, I think it is the most important of the various protections, but I don't think it is enough.

Mr. MARKEY. Is it enough?

Mr. PITOFSKY. I don't think so.

Mr. MARKEY. Okay. Now, in your testimony, Mr. Chairman, on page 5 of your testimony, you say, only a small minority, only a small minority of commercial Web sites, however, have joined these programs, these voluntary programs, to date. They also show that as a study, that the implementation of fair implementation practices is not widespread amongst commercial Web sites.

Then your very next sentence says, based on these facts, the Commission believes that legislation to address online privacy is not appropriate at this time.

How long will we have to wait, Mr. Chairman, for this administration to take a stand on this issue? How long will it take, deep into, now, the online commerce era for us to realize that most of the participants in this industry won't have a privacy protection policy which is meaningful unless the Federal Government puts one on the books to provide that for all Americans?

Mr. PITOFSKY. May I answer a couple of your earlier points and then come to how long? As an academic, I have to respond to the question of grade inflation. Remember, all I said was, on energy, effort, commitment, they get a B plus. As far as where we are now, I give them a C, so there is a long way to go.

Do I think that we don't need any law because everybody is honest? Of course not. We bring hundreds of cases every year in the antitrust and consumer protection fields. Self-regulation only works when the industry comes to the conclusion that it is in their interests to abide by certain principles. That is not true in many areas of law, and therefore, the government has to crack down. It remains to be seen whether industry will come to the view in this area, as they should, that consumers want, care about, and need privacy, and that it is in industry's interests to make sure it is introduced.

How long should we take? You know, the most, I have often said, the most effective self-regulation program in this country is the advertising industry's National Advertising Review Board. If we had come along 2 years after people started thinking about that, and said, forget it, we are going to handle this by law and law alone, you wouldn't have that kind of self-regulation. You have to give some time for these programs to develop.

I would say—I would say this. We had a good year, good progress; internet industry leadership is committed to self-regulation. If we have the same sort of year next year, then I would say that we are going to make vast progress. As a matter of fact, at

the pace that notice is being made available, you will practically see universal notice within a year.

Mr. MARKEY. Do you believe we are going to reach 100 percent compliance next year?

Mr. PITOFSKY. No.

Mr. MARKEY. The year after?

Mr. PITOFSKY. No, sir.

Mr. MARKEY. One hundred percent compliance.

Mr. PITOFSKY. Mr. Markey, I don't think we ever will.

Mr. MARKEY. Okay. Then do we need a law?

Mr. PITOFSKY. No, I don't think so.

Mr. MARKEY. You don't think we will need a law if there is not going to be 100 percent compliance with protection of privacy in the country?

Mr. PITOFSKY. As I said earlier, you pass a law and you still won't get 100 percent compliance.

Mr. MARKEY. So your standard is because you cannot get 100 percent compliance with any law, then there should be no laws. Is that your position?

Mr. PITOFSKY. No, not at all.

Mr. MARKEY. That is what you just said.

Mr. PITOFSKY. No.

Mr. MARKEY. That applies to every law, sir, not just privacy.

Mr. PITOFSKY. Mr. Markey, if I appeared to say that I misspoke. Let me be clear.

Mr. MARKEY. You said that the protections were essential. You said that there would never be 100 percent compliance, and yet you say that we shouldn't pass laws just because there isn't going to be 100 percent compliance with essential protections which Americans need.

Mr. PITOFSKY. It is "just because" that I have to explain. We are at the dawn of the most impressive new marketing sector of the economy that this country has ever seen. It is dynamic. It is fast changing. It is remarkable—the extent to which people are becoming committed to doing commerce on the Internet. In a circumstance like that, you want to stay flexible about the nature of regulation that you impose.

Mr. MARKEY. Mr. Chairman, technology is changing rapidly. So what? Are people not entitled to privacy? Are people not entitled to protection against fraud, just because technology is moving rapidly? Are we to say for the next whole generation of e-commerce that we can never pass any laws to protect people's privacy or protect them against fraud or protect their children online because the technology moves rapidly? I think that it is our responsibility, Mr. Chairman, to move forward in a way that ensures the protections are put on the books against people who will exploit people just because they are online and they are on no protections.

I think this argument that you are making runs completely contrary to the whole history of the Federal Trade Commission and its commitment to try to stay apace of the changes which are happening with the economy, rather than saying that we can't catch up because it is moving too rapidly. I don't think that is a standard which we can use. Fraud, privacy, and protection of the consumer are standards which are eternal regardless of the industrial era,

the information era that we happen to be in. I don't think that those are standards which we should say can't be, can't be maintained.

In fact, we have it upside down. The people who put privacy protections online, we can sue them for deceptive practices, but if the industry participants don't put any privacy protections on the books, then we don't have any right to go against them because they haven't deceived anyone, because they have no protections whatsoever.

And what you are saying is that the system is broken, but we are going to ask the people who have allowed it to remain broken throughout all of the 1990's to continue to try to improve it even though they have a 90 percent failure rate. I don't believe that the American people, looking at those statistics that were produced earlier in this hearing, indicate that the American people are getting more confident; in fact, I believe they are getting less confident in this online industry's ability to provide security, be able to provide privacy, to be able to provide access, to be able to provide notice that their information is being compromised.

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

The gentleman had offered to Mr. Swindle a chance to respond to his comments. I think the chairman probably ought to do that.

Mr. SWINDLE. I applaud the Chairman's position on this. I think he did state the case correctly. I don't believe any one of us here, and we have obviously different views on how we should approach this, have made statements as Mr. Markey alluded to. Each of us has been out meeting with industry and attempting to get—encourage industry, and I think we have been successful on that from our different perspectives, and I think the Commission is doing good work in that regard.

I don't recall anyone saying that is no need for Federal agencies, not even the slightest insinuation of such. I certainly didn't. The idea of self-regulation reaching 100 percent or a law reaching 100 percent, I think I said in my earlier statement, there is no way. We will not get there. Today we just got behind again, because there are 100,000 more Web sites out there. We will never catch up with that. That is reality.

As far as needing a law to get 100 percent, we have the Fair Credit Reporting Act. We prosecute cases on a monthly basis under that because we have not stopped it, and we will never stop it. I just—I am a little mind-boggled at the idea that we would think that we can pass a law and solve all of these problems.

We at the Commission and the staff at the Commission do remarkable work in trying to implement and enforce our laws, but we will never get to everyone, all of them. So I can't buy that point.

Mr. MARKEY. Mr. Swindle, we have laws against murder on the books. We will never catch all of them, but we are not taking the murder statutes off the books.

What statutes are you prosecuting people right now under that you are claiming credit for. Obviously you need laws to——

Mr. TAUZIN. The gentleman's time has expired. He has made his point. We have to move on.

The gentleman from Georgia, Mr. Deal.

Mr. DEAL. I will pass at this time.

Mr. TAUZIN. Mr. Cox is recognized, from California.

Mr. COX. Thank you. I would like to welcome our panel and thank you especially for the report that you have provided to us. I would note that Chairman Pitofsky and I spent some time together a quarter of a century ago when you were my antitrust teacher at Harvard Law School. That was when you were 29 and I was 15, and I continue to be educated, and I appreciate it very much.

We are going to hear from the Direct Marketing Association a little later, and in the testimony that the Direct Marketing Association has provided to us, they have said that as a condition of membership of the DMA, they are going to require that all companies, including those who market to consumers on the Internet, provide notice to consumers if they transfer data to others, and if they provide consumers the ability to opt out of such transfers.

It seems to me that that provides the essential ingredient for an enforcement system based on the licensure of personal, private information as if it were a property right. That is to say that in the same way that all of us accept a license when we rip open a package of software or sign a license agreement when we buy computer products of significance, that we would be able to license the provision, the publication of our personal information by others if we chose to do so, and we would have a cause of action for conversion of our private property if we chose not to do so. That would require only this in order to make it work, and that is a legal system that protected private property in that way.

Is that a reasonable approach? I would ask any of the panel to address that.

Mr. PITOFSKY. It is consistent with the way people feel about this issue. They don't mind their personal information being used. They don't mind getting catalogs or receiving materials as a result of target marketing. What they mind is that happening without their consent. And if we can get there one way or another, by law or by self-regulation, so that people have that option, have that choice, I think the approach that you describe is one that we would be comfortable with.

Mr. COX. Does any other commissioner wish to comment on that?

Mr. THOMPSON. Sure. I think that notice and opt-out are important elements, but they are not the only elements. I think that giving consumers, depending on what industry it is, access to correct information is also appropriate. I think security is important. I also think enforcement is important. I am not saying necessarily enforcement by the government, but providing meaningful remedies for consumers who feel that the representations that were made by a Web site about how information was going to be used were not lived up to. That is the kind of confidence people need. I think that it begins with the industries themselves.

I think DMA should be saluted for taking a fairly tough line with their members. But what is important is that it is not just them, it is everyone, that that has to be an important tenet how buyers and sellers deal with each other online. That has to be a part of the climate.

So there is a question of how you deal with those who choose not to participate at all. That is a very important question. But I salute

those parts of the industry who really understand that it is in their best interests, as well as consumers, all of our best interests, to see this part of the economy grow, that they provide that kind of balance.

Mr. COX. And therefore, the shortcoming in the DMA approach is that not everyone is a member of DMA, for starters.

Mr. THOMPSON. I think that is one.

Mr. COX. So what we would want is a regime that applies across the board to good actors as well as bad actors.

Second, you point out that we need enforcement. I think Mr. Swindle's point earlier when you have an increment of 100,000 new Web sites over what period of time?

Mr. SWINDLE. Very short. I am not sure. But it is growing.

Mr. COX. We have, as we all know, these exponential rates of growth in Internet usage and the addition of Web sites. The notion that a government agency is going to be able to police it fails facially, but what might work is, if consumers have the tools that they need to enforce it, which is why I am talking about this private property notion, if you have an enforceable property right and you can go to court and you have a cause of action, and let us pick out of the air $1,000 maximum statutory damages for an unintentional violation and $10,000 for an intentional violation or some reasonable limit so that we don't have the next $6 billion jury award in this area, you might have a much broader base of enforcement and so-called voluntary enforcement might get a lot closer to 100 percent.

Mr. PITOFSKY. I think at the end there you put your finger on the problem. A private right of action is something that people ought to consider. It is a real possibility. On the other hand, they also have to consider whether or not you want some Web site that makes some mistake about opt-in or opt-out being hit with a class action that will just blow them right out of that sector of the economy.

So it is a fair question to raise; it is not one that we have addressed.

Mr. COX. I assure you that is not my plan. I am working in the other direction.

Mr. PITOFSKY. There are some reasons for thinking about a private right of action, but you would want to be careful about it.

Mr. COX. I thank the chairman.

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

The gentlewoman from California, Ms. Eshoo is recognized.

Ms. ESHOO. Thank you, Mr. Chairman. And thanks, once again, to our distinguished witnesses here today. Chairman Pitofsky, during your opening statement, you mentioned that the Commission is going to hold a workshop soon on online profiling, which is the practice of collecting information about consumers as their movements are tracked online. It doesn't settle all that well with me. I have a sense of a little online stalking. But it is the way—I mean in hearing it, it is the way I—my sensibilities react that way.

But at any rate, would you discuss how this practice works? In particular, do consumers generally have knowledge that their movements are being tracked, and what kind of information is able to be—is actually collected in this way?

Mr. PITOFSKY. Well, one of the reasons for the workshop is to try to find answers to the questions you raise.

Ms. ESHOO. But there must have been some indications to you; therefore, the workshop?

Mr. PITOFSKY. Yes. Profiling is it is not limited to just online information. It is a combination of online and offline information, which produces the kind of body of information about people often available for sale that is very—that is very troubling.

On the question of whether people know this is going on, I don't think they do. I think it is being collected without notice. This new medium has an incredible technological ability to marshal, analyze, and present data about individuals.

How much of that is going on, how it is being handled, whether the information is being marketed and sold, and particularly whether it is being sold in personally identifiable ways, as opposed to aggregate averages, which I don't think anybody is terribly troubled about, that is what the workshop will be about.

Ms. ESHOO. I think that this committee in particular would very much like to have a report back from the Commission after you have completed the workshop and what you have pulled out of it. I think that we could make, hopefully, some positive use of whatever information flows from that. Because the idea that it is personally identifiable and tracked is a form, at least I think could be thought of as a form of online stalking, stalking.

Do you know of any agency that sells any private information that comes through it?

Mr. PITOFSKY. I do not. Anyone?

Mr. SWINDLE. Well, I don't know about Federal agencies, but we know for a fact that State agencies, which are part of the problem too, I guess, they sell information off of driver's license registration and car registration. That is commonly done in many States from what I understand, and I don't think any consumers or citizens gave them the right to do that, but they do it.

This phenomena, collection of information is mind-boggling. We are going to be dealing with this for years to come. My concerns are that we deal with it in a manner that is as practical as possible without throwing impediments to developing this, as the chairman described earlier, perhaps one of the most phenomenal changes in the way we do commerce that we have seen in our country's history. If we get overly emotional about this and start running around trying to stop it, we will very likely overstep our bounds and do more harm than good.

Ms. ESHOO. Does the Commission have any ideas about how we can educate people on how private information might be used? Have you grappled with that?

Mr. THOMPSON. I think that——

Ms. ESHOO. Relative to commerce? You know, obviously within the areas of your jurisdiction.

Mr. THOMPSON. I think the Bureau of Consumer Protection has been very active in consumer education, but also has been working with groups like the Direct Marketing Association and other industry-based initiatives to talk to consumers about how their information is being used and collected and what choices they have for how that information is shared. I know that on our Web site, FTC.gov.,

there is a privacy page that tells consumers how to get their names off mailing lists and other things.

Ms. ESHOO. What you are suggesting is that the Commission puts out information on how this can be done technologically?

Mr. THOMPSON. We have brochures and other information available to educate consumers. But what I think is going to be important here though is what broader initiatives industry, together with government and consumer groups create to deal with specific problems and specific concerns to let the public know a little bit more.

Ms. ESHOO. I have the sense that we are trying to get socks on an octopus, and I think if we don't—I mean if we really don't come out with something that has clarity for the American people, that maybe the description I just gave will continue. I don't know what these ratings really mean. I mean if we see the Good Housekeeping Seal of Approval, that means something to us. I guess I can't really describe it, but there is confidence in that. And while we have some markers, I don't have a sense that people know what that is, and I don't think that we can be necessarily self-congratulatory that they are out there if, in fact, the representation doesn't give people the kind of confidence that they need.

I think the hearing is demonstrating that we have a ways to go so far. I appreciate the work that you are doing. I don't think I have made my mind up about which is the best way to go, but we will keep at it. Thank you.

Mr. TAUZIN. I thank the gentlewoman.

The Chair now recognizes the gentleman from Mississippi, Mr. Pickering, for a round of questions.

Mr. PICKERING. Thank you, Mr. Chairman. I appreciate you holding this hearing on a very important issue.

Mr. Pitofsky, let me ask quickly, under section 5 of the Federal Trade Commission act concerning unfair and deceptive practices, do you feel like you have the current authority to, if progress is not made, to take additional action, not only under fraudulent cases, but to say require certain business practices of notice and opt-out, do you have that authority, or do you interpret your authority that broadly?

Mr. PITOFSKY. We certainly have the authority, when people are misled into providing information under false pretenses, and we have brought cases, we have brought important cases in that area.

The problem arises where the information gatherers say nothing. They collect the information and they use it in unexpected ways. We have not brought that case. We have put out an advisory opinion saying that where that kind of information is collected from young people, we believe we clearly have the authority in that area. Where it is collected more generally from adults, we have not brought that case, and I am not so sure that we could win it. But certainly, if they put out a privacy policy, as firms are doing, many firms are doing, and then they don't abide by their own privacy policy, that is actionable.

Mr. PICKERING. This seems to be the crux of the problem. It seems like there could be an incentive to have no privacy policy, to put themselves at no liability or at risk of violating, intentionally or unintentionally, their privacy policy. And the question is what

incentives can we give, short of legislation, that would require all companies to adopt certain practices and certain privacy policies.

Mr. PITOFSKY. I think you are exactly right. I think an incentive is there in the marketplace, and that grows from the fact that 85 percent of the people who are not doing business on the Internet say it is because they don't think it is a secure medium, and the business community has to come around to the view, as I believe many of them have done, many of the best players, that it is in their interest to protect the privacy of people who do business on the Internet.

The other—frankly, the other incentive is, if that progress does not occur as it has been occurring in the past year, then the FTC and this committee and the Congress will take action. We are challenging these folks. We are saying to them, if you don't want legislation, you better move along on self-regulation. They have made some progress, I hope it will continue.

Mr. PICKERING. Any other comments from the panel as far as incentives that we can ensure the progress of self-regulation from the Internet community and the business community on a going-forward basis?

Mr. SWINDLE. I would just like to add, I think one of the main things we can do at the Federal Trade Commission is continue to expand the educational efforts that we have already undertaken. Our staff does an excellent job in putting out very informative pieces of information. We have conferences, we mentioned, I think it is mentioned in our report of conferences to come. I think that process of consumer education will coincide with industry's awareness that this is important. It is in their own self interests to do it right.

The incentive is profit, and profit comes from satisfied customers, and that takes you to the next level. The marketplace will demand that we find some level of acceptable private practice on the part of industry; otherwise, consumers won't go there. Any consumer with one click can leave a Web site if they aren't satisfied with it. And I share with the chairman the concern, and I think we all share it, that in these practices where the consumer has no idea that information is being collected, and therefore, has no option of choice because they don't know the problem exists.

But, I think that is where we are back to the education cycle. The more we inform the public, the more we all become informed as to how this medium is going to work. It is new, we are learning every day. Industry is learning, consumers are learning, and certainly we in the Federal Trade Commission are learning, and I think it is that ongoing process that will make this an economic engine that we will all sit back and marvel at and we will be quite surprised with it. As I said, consumers are not inching slowly to this form of commerce, it is tripling every year, and I think that is an indication that they like it.

Now, if they hear things that scare them, I hope not unnecessarily so, they will back away from certain sites and make reasonable choices.

Mr. THOMPSON. I agree with what has been said. Time is really important here, that if 1 year in Internet time equals 3 years of

other time, then we should be concerned about how quickly industry progresses.

But what I will also say is it has to be a fabric, it has to be not just government saying we are going to do X if you do something bad, it is also industry acting in enlightened self-interest. I think that we all have a stake in seeing that that occurs.

Now, one of the things—the reason that at least I don't think legislation is appropriate at this time is to measure what is not being done, what industry resistance there is, is it the tail, or is it the hub? That has to be an important factor to know, because that will tell you what is the appropriate way to address the problem.

The industry leaders do recognize the importance of bringing the rest, finally, the rest of the market along. That is not only based on consumer education, telling consumers what they should be asking for, but also telling business what are the necessary elements for doing business in this area. I think that what they would find is that if they do a cost-benefit analysis, the amount that they have to gain, even small- and medium-sized businesses of doing a privacy policy is great. But that information has to get out to them.

Mr. PICKERING. Thank you, Mr. Chairman.

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

The gentlewoman from California commented about socks on an octopus. That stirred my data banks, and I couldn't remember where I had heard that phrase. It was Earl K. Long who used it, I think. There is a wonderful book entitled Socks on a Rooster about his life. He once said when they tried to put a tuxedo on him at his first inaugural in Louisiana that putting a tuxedo on Earl K. Long is like putting socks on a rooster, and he refused to wear it. It is a good analogy.

The gentleman from Minnesota, Mr. Luther, is recognized.

Mr. LUTHER. Thank you, Mr. Chairman. This really is to any member of the panel. It just seems that if we applied common sense, it would tell us that we will, over time, achieve a degree of voluntary compliance; that would be common sense, and in the interest of businesses to do this.

But it seems like common sense would also tell us—and I would like your thoughts on this—that if companies are profiting from using, selling, and disseminating this information, they would be very unlikely to be the ones who would voluntarily comply. So in other words, as voluntary compliance goes up, it seems to me that we still would not be dealing with the real problem, which is those companies that have a self-interest in not complying, or not either posting or adhering to the policy. Isn't that the crux of the problem here? How could we ever expect voluntary compliance from companies when it is against their self-interests to voluntarily comply? That simply is not going to occur, right? There is nothing to motivate them. So I guess that is where I am getting a little lost with some of the comments about voluntary compliance. Even if it increases greatly, we are not going to be dealing with the ones we want to deal with.

Mr. PITOFSKY. Let me start. Mr. Luther, it is a fair question, and it is something that we ought to explore. I am not sure it doesn't work the opposite way. The big companies who gather the kind of information that is valuable enough to sell, they are the ones who

are complying, the Disneys of the world, the AOLs of the world, the Microsofts and so forth, they are the ones who gather vast amounts of information that is valuable to sell and they are the ones who are going along with self-regulation.

The company that will probably never go along is some individual who has a Web site and is selling chile beans, they are not collecting the information, they couldn't sell the information if they did collect it, it is not going anywhere at all. I say that as a hypothesis. I don't know that that is true.

I do know that many—most of the big companies that collect the kind of information that others want have seen it in their interests to go along with self-regulation.

Mr. LUTHER. Well, just to follow up, if I may, aren't there a lot of examples between those two extremes. That would be my response to that answer. And in fact, aren't some of the examples in-between exactly what we are trying to deal with here—the people that are truly profiteering today; there is not one reason for them to comply with some voluntary compliance system.

And I would add an additional point, and that is how fair is it to the legitimate businesses—that are out there competing on a fair basis—how fair is it to them to be undercut, for example, by a business who is making their profits by using that information for some other purpose? I mean, legitimate businesses want fair rules that everyone lives by; don't they? I would ask that question to anyone on the panel.

Mr. SWINDLE. I am having a little difficulty imagining the business that is undercutting another business, because that business is gathering information to sell to somebody. They might be undercutting another business that does that, but if they are in the business of gathering and selling this information, you know, wrongfully or without consent, who are they competing against?

My concern is that if we choose to legislate, legislation applies to the universe. The number of people who are in this business that we don't like, the invasion of privacy, and selling this information, by comparison to those who are legitimate in every sense of the word, but may not know the necessity to meet this law, we will burden the universe in order to capture a few. I just don't think that is the way to do it.

Now, the question then comes back, to the Congressman's original question. How do we get at those few, and they are relatively few, in my mind, how do we get those without burdening the rest of the universe. That is the problem, and I think that is something we have to consider and look toward resolving. But, passing a law would apply to everybody. Then we, all of a sudden, have to enforce that law against people who, by no evil intent whatsoever are not complying, which, I would suggest, the vast majority of Americans fit that category. There are bad guys out there, we all recognize that. But now, we have to enforce this law against all who violated it, and now we have to penalize them. This doesn't make sense.

Mr. THOMPSON. I appreciate your question, because I think it is exactly that kind of a question that we need to find out a little bit more about. There are large companies who presumably should know that this is in their enlightened self-interests that the efforts are clearly not reaching. We need to find out a little bit more about

why in order to—if legislation is appropriate, determine what kind of legislation.

But I would also be hesitant to talk about legislation if it is an all-or-nothing proposition as well. Because in the sense that I think when we came last July, we talked about any legislative vehicle at all should at least provide some safe harbors for companies who are doing the right thing; for independent industries that are doing the right thing, because we think that those industries should be rewarded and not be subjected to a "free riders," others who are not doing the right thing benefits from the industry efforts. So we have to get at that. We don't know. I think we need a little bit more time to figure that out.

Mr. LUTHER. Thank you, Mr. Chairman.

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

The gentleman from California, Mr. Rogan, does he have any questions?

Mr. ROGAN. Mr. Chairman, if I may, just briefly.

Mr. TAUZIN. The gentleman is recognized.

Mr. ROGAN. Thank you. I will throw this out to the members of the panel. I did have a chance to review the summary materials on the Georgetown Internet Policy Privacy Survey, and I am just wondering, do any of the members of the panel have an opinion as to the validity of that survey?

It claimed that two-thirds of Web sites surveyed had established a privacy policy, but when I looked at the universe of sites that were examined, there were only 361. That seemed like an awfully small sampling for what must be tens of thousands, if not hundreds of thousands of Web sites that are out there right now. Has anybody had a chance to review that in depth, and does anybody have any opinion as to whether that is an appropriate figure?

Mr. PITOFSKY. We did spot check the survey. We didn't just accept it without reservation, and so far as we could tell, it was a reliable survey conducted in a very professional way.

The sample is the sample. I mean it seems to me, when you get up to 361 or something like that, you get a fair picture of what the industry is doing. It may not be perfect, it could be off by 3 points either way. But the important thing is that the industry moved from 14 percent notice to 60-something percent notice in 1 year. And we are comfortable that that is a reliable count.

Ms. ANTHONY. I was just going to comment that you have to recall that these are the most well-traveled sites, not every site. The sampling was the most well-traveled sites on the Internet.

Mr. ROGAN. Thank you, Ms. Anthony.

I have to assume when we look at the explosion on the Internet over the last 8 or 9 years, I think I saw a figure sometime ago that in 1990 almost nobody was on the Internet and by 1999 we have millions and millions of people, and that figure is being added to every day.

I have to assume that as each day goes by, and as more and more people are going online, there has to be a lot of consumer pressure also on businesses to adopt privacy regulations and also to have their privacy rights enforced. Are you finding, as you oversee these issues, that there is an awful lot of that dynamic in play?

Mr. PITOFSKY. Great consumer concern, and in my view, the reason why you have so many of the leaders of the industry moving to privacy policies is because they see that it is in their interests to do so.

Mr. ROGAN. Yes, Mr. Commissioner.

Mr. THOMPSON. I think just to take a look at who is really leading the charge here, we are looking at companies who have decided that it is in their best interests, because first of all, it allows them to distinguish themselves in the market versus other Web sites who might be selling something, or technologically based sites that believe that this is an important part for the technology industry to play a part in.

The real question is whether those industry leaders can essentially have an influence on all of those who sell, to make sure that they know that it is in their best interests to concision the market generally, so that consumers feel that confidence no matter where they go. That is the real challenge for them. So while we have great respect for the industry leaders here, the real question is, is there an industry to be led?

Mr. ROGAN. Thank you, Mr. Chairman, thank you, Mr. Thompson.

Mr. TAUZIN. The Chair now recognizes the gentleman from Tennessee, Mr. Gordon.

Mr. GORDON. Thank you, Mr. Chairman.

Ms. Anthony, I think it is always healthy to have informed and thoughtful dissent on the commission, and so I will—on any issue, and I will give you a chance in a few minutes if I have some time left if you want to expound on any more on what your thoughts are on what type of regulation might be successful.

But first let me ask you, Mr. Chairman, in your testimony you said that you thought considerable progress has been made with industry, a long way to go, and there should be no legislation at this time. You said a year from now there should be another report and that you want to get to the goal line.

Let me ask you, what is the goal line? You know, when you come here a year from now, what do you think should be the various benchmarks, and what progress should be made with those benchmarks so that you at that time would either say we need legislation, here it is, or still making progress, and we don't.

Mr. PITOFSKY. Well, in one sense, if the industry makes as much progress in the present year as they did last year, we are going to be pretty close to universal coverage in terms of notice, about putting a policy out there, and that would be remarkable. I would like to get beyond simple notice. I want to ask other questions about access, about security, about monitoring, and about enforcement.

I don't think you are ever going to get 100 percent self-regulation enforcement, any more than you do with the advertising community or the funeral directors, two of the best self-regulation programs that I am aware of. But if you got up there in the 90 percent range, 90-plus percent, and if consumers were aware of what their rights are, and consumers who don't want to deal with the Internet Web site that doesn't post a privacy policy can do so in an informed way, I think we are pretty close to where we ought to be.

Mr. GORDON. I certainly agree that you are not going to get 100 percent compliance even with the most stringent of laws and police forces out all the time.

So you are saying then that there should be 90 percent compliance a year from now?

Mr. PITOFSKY. I hesitate to draw an arbitrary line, but certainly if you were there, you would have to say that great progress has been made, and we are probably at the point where consumers can protect their own interests.

Mr. GORDON. If you are at 90 percent?

Mr. PITOFSKY. Yes.

Mr. GORDON. So what happens if we are at 70 percent next year?

Mr. PITOFSKY. We will file another report.

Mr. GORDON. That would be a failing grade, though?

Mr. PITOFSKY. That would be very disappointing, since they are at 66 percent now. If they get to 70, you would think that not much has been accomplished. But now I want to go back to the point I made in my testimony. Simply counting the notices on Web sites is not enough. We want to give this committee more information than that; we want to get behind that number.

Now, for example, there are probably some Web sites that have notices that are so small and incomprehensible and impossible to read that the notice is not worth a thing. I want to get to that issue.

Mr. GORDON. I have one more question. What I would like to do quickly is ask you if you could send to the committee or send to me what the vehicle will be for whatever studies when you come back in a year, and what are those areas that should be studied, and what are those benchmarks. I am not looking for a specific number, but what should be the range of compliance there?

Mr. PITOFSKY. I think we should do that, Mr. Gordon, and we will.

Mr. GORDON. All right. Mr. Thompson, I have a—I guess it is a cliche that all of these answers, or most of these answers are wrong. You mentioned earlier in your testimony about technology where you are going to have a workshop where the consumer can protect himself. I mean how close are we and tell us about this technology. Everything is sort of moot if that is the case.

Mr. THOMPSON. I think that that is one of the things we want to find out. That is one of the reasons why we want to have a workshop, because we understand that there are some companies who are working on various technological ideas that will allow Web site users to capture their own information and decide under what circumstances they give it up to someone else. And I think that is going to be an important innovation. I want to see how far they are along. I want to see if that is something that is going to be effective.

I hope that you will let the committee know about that, and Mr. Chairman, I think that——

Mr. TAUZIN. Will the gentleman yield? We have a second panel——

Mr. THOMPSON. You may hear about that today.

Mr. TAUZIN. I think we will learn about it during the second panel. Stick around.

I thank the gentleman.

Mr. GORDON. In closing, Ms. Anthony, where do you think we should be a year from now—where will those benchmarks be, to avoid legislation.

Ms. ANTHONY. Last year, when we brought our report to this committee we set out a legislative framework we thought would be useful in crafting a balanced, protective piece of legislation. Some of the bills pending in the House and the Senate have many of those suggestions in them now. I don't propose to write legislation for the Congress, and sometimes it is difficult for you to do it yourselves, but I do think that the four fair information principles of notice, consent, access and security remain, still, the focus and the thrust.

Mr. GORDON. Thank you. Thank you, Mr. Chairman.

Mr. TAUZIN. I thank the gentleman.

The gentleman from Florida, Mr. Stearns, is recognized for a round of questions.

Mr. STEARNS. Thank you, Mr. Chairman. I thank you for holding this hearing, and I welcome the witnesses.

I am trying to understand, and this might be appropriate for the second panel, how much business—this is for Mr. Pitofsky, the chairman, how much business is corporate-to-corporate or business-to-business versus consumer to business?

Mr. PITOFSKY. Most commerce on the Internet is now business-to-business. The consumer segment is growing vastly, and I understand in the present year, 1 percent of all consumer purchases were on the Internet, and it is growing at an incredible pace.

Mr. STEARNS. So if the majority of the Internet business is business-to-business, do these companies set up privacy within their businesses?

Mr. PITOFSKY. I don't know the answer to that. I rather doubt that they do, but I don't know, and I could find out and submit something to you.

Mr. STEARNS. I think that is important, because these companies set up their own privacy policies. We have already in place what businesses are doing. We don't have to recreate the wheel here. And if the market is doing it itself, the private policy setup through business to business, it is most likely that probably, when we move on a bigger generation of revenues using the consumer to businesses, that same type of trade policy or private policy will also come together.

Mr. PITOFSKY. We are moving in that direction, but I am not sure we are going to get there. I think we have to keep our eye on this issue and make sure that progress continues.

Mr. STEARNS. If we offer consumers a choice for privacy on the Internet, do you think they would take that voluntarily? The companies, when they say you are coming to my Web site, if you click here you can have privacy, this kind of privacy, this type of encryption, do you think that is a voluntary way to circumvent the need for you folks or anyone else on my side of the aisle promulgating legislation, Federal legislation?

Mr. PITOFSKY. If there is a clear and conspicuous disclosure so that people don't have to search around for it from screen to screen, yes. I believe they would decide one way or the other that they

don't care that their information, their private information, is used; or that they do and would opt out.

Mr. STEARNS. Any others that would like to comment on the question?

Mr. TAUZIN. If the gentleman would yield, I think it is important that we keep our eye on how broad the problems are, however.

I don't want to embarrass anybody over this, but there was a story in the Boston Globe about a public television station sharing its list of subscribers with one of the national political parties. A young boy, Sam Black, is shown in the article as receiving a mailing from that national party because his name was given to them in exchange for other names by a public broadcast station. The station owner is quoted as saying, "It is standard industry practice for nonprofits like WGBH Boston to swap or rent lists of other groups in an effort to expand membership."

This is a problem even bigger than the Internet right now. We are going to have to keep an eye on it and see whether or not there are elements of it that at some point need addressing. I thank the gentleman for yielding.

Mr. STEARNS. Thank you, Mr. Chairman.

Just reclaiming my time, when I go to the restaurants and I give them my credit card, I don't know the waiter or waitress who takes my credit card. They go behind the back and they run it through the machine and come back. I was trying to say, in the private world there doesn't seem to be any outcry of this privacy from the government to institute on the restaurant level or on the Sears Roebuck level or even when I purchase something from Lands End.

So I was trying to say, if I don't see it there, do I see the need for this Federal legislation on the Internet? Because obviously this person who is working at the restaurant could make a copy of my credit card and make a facsimile or something of it and use it, yet I don't see that happening.

I guess in your opinion, the analogy between the private sector and the Internet, is it quite a bit different in your opinion, or is it something similar?

Mr. PITOFSKY. In my view, it is different and deserves more attention. Collection of information on the internet is more threatening to individual privacy. First of all, on the Internet you could accumulate information in a way that is not possible in a restaurant or a mall. You can marshal it, analyze it, or sell it to people in a way that is valuable to them, but is an intrusion to you.

Second, when you go into the restaurant and you think about ordering the salmon, but then you order the steak, the only reference that they have is what you actually bought. On the Internet, the technology allows people to accumulate information on what you thought about doing, your browsing activities. That includes books, that includes music, that includes all sorts of things that people are sensitive about.

So I do think that the Internet is different. I do think that privacy is important. The only question that I have is what is the best way to get there since it is a particularly sensitive area.

Mr. STEARNS. Mr. Chairman, I think my concluding comment would be what I think a recent report talked about, that most people in the Internet, the consumers, are not buying, they are just

browsing. But you point out that simply browsing offers an avenue to sell what they are browsing to other people. In fact, if you go on Hot Mail or Yahoo Mail, you can check off the things that you are interested in and you will get information sent to you every day. It just comes rolling in. So that whole process is revealing your market tastes. So the consumers have the right to decide, but they certainly don't want that information sold.

But I think this hearing is very important for all of us to understand. This is a first step. So I appreciate this time to question you.

Thank you, Mr. Chairman.

Mr. TAUZIN. I thank the gentleman.

The Chair now recognizes the gentleman from Virginia, Mr. Boucher.

Mr. BOUCHER. Thank you very much, Mr. Chairman. I want to commend you for organizing this discussion today on what is a very timely and important subject and also for inviting this distinguished panel of witnesses, the members of the Federal Trade Commission, whom I would like to welcome. I want to compliment each you for the excellent groundwork that you have done in the area of online privacy protection.

Having complimented you for that, however, I will have to express a measure of surprise at the conclusion that you have generally reached that no new Federal legislation is necessary at this time. In opposing the passage of legislation, Chairman Pitofsky, you have cited the progress that has been made by the industry in protecting online privacy due in significant part to the participation by the industry and third-party seal programs, the five or so programs in existence today. Yet it is my information that only some 1,000 or perhaps less of the Web sites currently are participating in third-party seal programs; and we also—that, by the way, is among Web sites that may number more than a million. I don't know how many there are—I doubt if you do either—but I am told there are at least a million, or perhaps 1.5 million or 2 million.

Then we also have the study from Georgetown that shows a broader survey of Web sites that was taken, that only 10 percent of the Web sites surveyed have a practice that complies with the four fair information practices that I think we all agree are important. So you have determined that or it has been determined that there are only about a thousand Web sites that are a part of third-party seal programs, and only 10 percent of all Web sites surveyed are complying with these four fair practices.

Now, given that fact, I am frankly appalled by the recommendation that we not act now. I believe that there are things that we can do that would even enjoy industry support. For example, I have introduced a bill, along with my Virginia colleague, Bob Goodlatte, with whom I have the privilege of chairing the House Internet Caucus, that would establish a disclosure and opt-out policy, so that everyone who visits a Web site would have the opportunity of knowing what information that Web site collects from the visitor. That visitor would also have the opportunity to know how the Web site uses that information. If the Web site disseminates that information to any third parties, the circumstances and the identity of the distributees would also be noted. And then the Web site visitor would have an opportunity to opt out, to not participate in a fur-

ther visitation of that Web site and to do so with the privilege of not having any personal information about him collected.

Our bill also, by the way, gives the FTC full authority to enforce those provisions under section 5 of the Federal Trade Act. I can tell you that in constructing this provision, we had extensive discussions with the industry and I think broadly the industry would support an approach such as this. And so why would it not be wise at this time to act before the situation gets beyond our control before the other 90 percent of Web sites that don't comply with these fair information practices collect so much information that there is nothing that we can do about it? Why don't we act now?

I know that I am asking you to support of repeat your positions, but perhaps with this new orientation, you will provide a different answer. I hope so.

Mr. Pitofsky.

Mr. PITOFSKY. Mr. Boucher, I know of your bill and I believe in many ways it is a constructive compromise between people who would very heavily regulate the industry and those, like us, who want to give self-regulation more of a chance.

Just two quick points: One, if the bill is limited to disclosure and opt-out, the chances are that we will have accomplished that in a year or so anyway. When we say that only 10 percent have all of the information, fair information practices, most of those people don't have the access and the security provisions that would not be covered by your bill.

Second, the seal profession. It is true that the seal programs have hardly scratched the surface. But the Better Business Bureau seal program only started about 6 months ago. It is a little tough to criticize them because they have only gotten a relatively few people to be members.

Then third, my concern is that if we settle for disclosure and opt out as your bill provides, and not ask for more, that is all that we are ever going to get. I think consumers are entitled to more than that, and by keeping the pressure on with respect to self-regulation, we may be able to get—we should be able to get more than disclosure and opt-out.

Mr. BOUCHER. I agree that we can get more than disclosure and opt-out. I would not propose that enacting our statutory offering be an alternative for a continued industry self-regulation.

I think there will be substantial pressure from Internet users for a better set of privacy protections that go beyond mere disclosure and opt-out, but enacting disclosure and opt-out at this point in time would at least make sure that every Internet user immediately would have the opportunity to know what information about him is collected and how that information is used. If he disagrees with that, he would have the opportunity to opt out without having anything collected.

It seems to me that that is a fundamental assurance that we ought to provide the American public. I agree, we ought to do more, but we ought to do at least that much. I think that we can do that much statutorily with industry support during the course of this conference.

Let me ask you one other question. I know that you are familiar with the discussions that are taking place between the European

Union and our U.S. Department of Commerce. The European Union has a very extensive directive that confers upon European citizens extensive privacy rights in the online environment, going essentially to the four industry practices that you would recommend here for self-regulation. But as a matter of law, that would be provided in Europe. The directive takes another step and says that data flows can be interrupted with respect to Europeans accessing Web sites in any nation that does not have a comparable level of privacy protection. We are very concerned that unless there is an agreement in the European Union that whatever we do offers that comparable level of privacy protection, that there would be an interruption of data flows when Europeans visit American Web sites.

Now, the discussions on creating the safe harbor and giving Europeans an opportunity of saying that we have an equivalent level of protection, aren't going very well. This very been under way for more than a year. They have been recessed. There is no conclusion in sight. I am wondering if we enacted at least a disclosure and opt-out policy if we might not be able then to give the Europeans a basis to say that a comparable level of protection exists here.

Do you have any thoughts about that and would that change your view of whether we ought to act now legislatively?

Mr. PITOFSKY. I am going to ask Commissioner Thompson, who has been our delegate to some of these meetings, to address that.

I agree with you that it is a matter of great concern. Negotiations have been conducted by the Department of Commerce in this matter. Whether they are going to—whether we are going to have a serious problem or not remains to be seen. From what I understand, the issues that are outstanding—and I am not close to the negotiations—would not be fully settled by a disclosure and opt-out provision. There are other complicated issues as well.

Let me turn to my colleague, Commissioner Thompson.

Mr. THOMPSON. I think the Chairman is right. There are a variety of issues that have to be resolved on the European side. But you are also right in noting that the concerns that the Europeans have about how we treat data in the United States is very important to us. It is not just notice and opt-out, but also the other elements. I think that they support the four elements that we have discussed and want to know what meaningful remedies their consumers will have in the United States.

Now, notwithstanding that, a legislative vehicle isn't always the most effective way to get at those protections if there is an effective framework for self-regulation. Now, there are certain parts of the industry that are leading in that charge and certain companies who we have talked about earlier who will satisfy that pretty clearly. The real question is, how can that be transferred into the broad base of companies that we and the Europeans want to see here in the United States have those protections. That has been the challenge and that is going to be the challenge that Ambassador Aaron is going to have to convince the Europeans of.

Mr. BOUCHER. Well, thank you very much. I appreciate that comment, Commissioner Thompson, and I want to thank each of these witnesses again for the work that you have done in this important

field and we all look forward to continuing our discussions with you.

Thank you, Mr. Chairman.

Mr. TAUZIN. I thank the gentleman. Before we dismiss this very esteemed panel, I would like to give any member who wants to make a final question or comment a chance to do so. We will first start with the ranking member, Mr. Markey, for a final thought or comment or question.

Mr. MARKEY. The point that I was—thank you, Mr. Chairman, very much.

In the securities marketplace, the so-called "crown jewel of capitalism," the engine of the capital formation process, we have self-regulatory organizations. They are called the New York Stock Exchange, the National Association of Securities Dealers, and the regional exchanges like the Boston Stock Exchange.

In the futures market, we also have SROs, self-regulatory organizations, the Chicago Mercantile Exchange, the Chicago Board of Trade, and the New York Mercantile Exchange.

The securities self-regulatory organizations are subject to supervision and oversight by the Securities and Exchange Commission. And the futures self-regulatory organizations are subject to the jurisdiction of the commodities futures trading commission. The SEC and the CFTC must approve all of the SRO's rules before they can take effect. They can direct them to adopt, modify or eliminate their rules, and they can inspect and examine their regulatory and enforcement programs to ascertain their adequacy and protect the public interest, assure the protection of investors and the maintenance of fair and orderly markets. And they do all of this without compromising the dynamism and the innovation in our Nation's financial markets which are technology driven, fast-paced, global and constantly changing.

So if we are talking about self-regulatory organizations like the securities and futures self-regulatory organizations, that is one thing. But if we are talking about SROs without Federal oversight and enforcement over them, then there is no accountability and no assurance that consumers will be protected. That is not self-regulation; that is self-delusion. We cannot operate in a world in which an industry which is so potentially invasive of every family's life can go completely on the honor system when there are so many powerful financial interests that could drive some of them in the opposite direction.

I might add I think at the end of the day that this whole notion that "dot com" means that you have huge debts, no real profits but maybe 5 or 10 years from now you might be able to show some profit was undermined if you saw it last week by an Internet site called C/Net. They were taking $800 million of their own money and were going to invest it in an advertising campaign. Their stock valuation dropped by about 15 percent because no one had ever seen a mode like this where an Internet company had actually made money, was investing it in a traditional business sense, and as a result, people were beginning to lose confidence. Maybe it is that people don't want to go online, that is, middle-class America, largely because they are not sure that their privacy is going to be protected, that their security is going to be protected. Maybe, at the

end of the day, in the same way that the Federal Trade Commission Act was originally put on the books says, the Industrial Age had been moving so fast that it was necessary to begin to catch up with it, that maybe the confidence that was necessary to be instilled in this marketplace that these companies can actually turn a profit would be related to their sense as ordinary middle-class families, that they should trust it, that they should believe in it. Right now, we see again from these polls that that is not the case.

So my request to you would be that you look at these issues again, you set a deadline in the near term for the industry and for yourselves. But understand that the information you have given us today heightens the likelihood that we need to legislate, not undermine it. I think it should leave you with the same result in terms of how you view your responsibilities at the Federal Trade Commission.

Thank you, Mr. Chairman.

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

Mr. Pitofsky, do you want to respond quickly?

Mr. PITOFSKY. Very briefly.

I could not agree more that the mix between law and self-regulation addresses complicated issues. We want to be sure as we proceed that we get it right. I know that that is what you are asking us to do, to investigate carefully.

On the other hand, this is not an area where internet sellers are completely unregulated, where there is no oversight. We recommended legislation with respect to privacy of kids and we bring cases under section 5 challenging invasions of privacy all of the time. So it is not totally unregulated. The question of where self-regulation is appropriate and where law is appropriate is exactly what we would like to try to address and we will continue to address and provide our thoughts to the committee.

Mr. TAUZIN. Does any other member wish to make—the gentlelady from California.

Ms. ESHOO. Thank you, Mr. Chairman.

You just mentioned, Mr. Chairman, you touched on the issue of children. You testified last year that legislative action was appropriate for protecting the privacy of children, and we passed the Children'S Online Privacy Protection Act. Your agency has written rules to implement it, though I understand they have yet to take effect.

Do you have any information on whether companies have improved their online protections for children in anticipation of these rules kicking in, and do you consider your actions in this area to be a success? Would you grade companies higher, give them a higher grade in the area of children's privacy than in the area of adult protections?

Mr. PITOFSKY. My reaction is an impression rather than a careful study. I do believe that there has been some improvement and some recognition on the part of companies, partly because some of the suits that the FTC has brought. Those suits that asked for the toughest remedies did involve invasion of privacy, using kids to disclose family finances. So we have cracked down there. There has been a lot of publicity. My impression is, things have improved, but I really don't have a statistical analysis available.

Ms. ESHOO. I think that what you could provide our committee with could be instructive in this area because it seems to me what has been interwoven in this hearing is, there is a nexus between setting the standard and then compliance with it. On the one hand, it is voluntary, and on the other, it has been legislatively directed. Perhaps we could be able to learn from the two. I don't know when you could bring something like that forward, but I would certainly be interested in it.

Mr. TAUZIN. I thank the gentlelady.

Mr. PITOFSKY. The best regulation combines the two: legislation in appropriate areas and self-regulation in appropriate areas.

Ms. ESHOO. Could I just follow up very quickly? Is it your sense overall, though, that the reason that you are saying that you don't believe it is appropriate for legislative action now is that it is too early or you just don't believe that there should be any legislative action in the adult privacy protection area?

Mr. PITOFSKY. It is not the latter. It is too early and the sector is too fast-moving. You want to measure the target accurately before you try for legislation. I think at least at this point things are moving in the right direction and it is premature.

Ms. ESHOO. Thank you.

Mr. TAUZIN. Anyone else?

Mr. Boucher.

Mr. BOUCHER. Mr. Pitofsky, I want to revisit with you briefly the question of how long we do have to wait. In answering that question, let me just point out with regard to TRUSTe we have now waited 2 years. And TRUSTe now certifies a total of 500 sites, 500 out of more than a million. With regard to the CPA WebTrust, we have now waited for 2 years and the WebTrust certifies 19 sites out of more than a million. And in Internet time, 2 years is not a short period of time. We all have waited substantially with regard to these two programs.

And then the Better Business Bureau, which admittedly is somewhat newer, 3 months old, only has 42 sites out of a million. Where are we going to be this time next year? When are we going to know that we have achieved success, and how long can we afford to wait?

Mr. PITOFSKY. I will just repeat what I said before. If there is as much progress this year as last year, then I think that we are on the right track and we are going to get to a place where all of us agree that we ought to be. If the progress falls off, if we find they put on a good show this year to head off legislation and nothing more happens, I will be up here, speaking for myself and I hope my colleagues would join me, in recommending that there be legislation, because the problem is not being solved.

Mr. BOUCHER. Well, Mr. Pitofsky, I thank you. I would only point out that I think there is some legislation that we can pass this year that the industry would not head off—in fact, would support—that would provide a certain set of guarantees that the public does not have today. Thank you.

Mr. TAUZIN. The Chair thanks the gentleman.

Let me wrap up by making a couple of comments. First of all, we have learned a good deal at this hearing. We thank you very much for your contributions. While this hearing was entitled The Current Status of Privacy Protections for Online Consumers, I

think my friend from Massachusetts and others on the committee will agree with me that privacy concerns are broader than even the online privacy concerns.

I made the point about the public broadcast station inappropriately trading or renting, selling something, its list, inappropriately to political parties. But in that regard it is clear from the testimony today that this thing is still very much in flux.

I read somewhere that only 15 percent of the Web sites are even identified on most search engines. There are a lot of Web sites out there. Many of them obviously are not even available to a lot of us through the search engines. I might mention to members that if you have a Web site and you haven't posted your own notice, today might be a good time to do it. I have instructed my staff to put together a notice and hopefully one that will be identified as an appropriate one with approach safeguards for people that visit our site.

In that regard, the other thing that we learned, as Mr. Stearns pointed out, is that most of the business today, most of the e-commerce is still business to business, but that a huge and growing sector is going to be direct consumer interaction with businesses in e-commerce. While that is only 1 percent of our commerce today, that is obviously going to grow very rapidly. So getting this right as we watch the industry make its attempts at self-regulation is going to be important.

Finally, let me point out to all of my friends on this side of the panel and the other side, that while it might be very inappropriate for us to try to put socks on this octopus, that it may be very appropriate at some point to make it very uncomfortable to go barefooted on the Internet. And at some point we may indeed wish to proceed with legislation to say to those who would not agree to proper self-enforcement, self-regulatory mechanisms that there is some fall-back, some safety net, to protect online consumers in that world.

I think that is sort what have we have been talking about today, at what point do we do that and at what time do we do that. In large measure, we are going to continue to rely upon the good work, Mr. Pitofsky, that you and your agency are doing in gathering information and reporting to us. I would encourage you to continue that good work and continue to report to us on the progress that is being made or the lack thereof. I finally would like to send a strong signal to the industry again that this hearing was designed not simply to catch up on progress, but also as a strong message to continue that progress in the hopes that whenever we do get to the stage where we have to decide whether to make it uncomfortable to go barefooted that that is a minimal government approach rather than a larger one. That is our hope and I think that is the purpose and intent of this hearing.

I would again encourage the industry to continue its efforts to try to find the mechanisms that work so that we have less concern here at this level and certainly at your level, Mr. Pitofsky. Thank you very much for your testimony today. Again, as always, we deeply appreciate your service to the country. Thank you very much.

Mr. PITOFSKY. Thank you, Mr. Chairman.

Mr. TAUZIN. We would now call up our second panel of witnesses. And they will include Mr. Robert Lewin, Executive Director of TRUSTe just mentioned a minute ago, of California. Ms. Deirdre Mulligan, Staff Counsel for the Center for Democracy and Technology; Ms. Solveig Singleton, Director of Telecommunications and Technology Studies for the CATO Institute; and Mr. Steve Lucas, Chief Information Officer and Senior Vice President, PrivaSeek, one of those efforts at software protections for consumers; and Mr. Jerry Cerasale, Senior Vice President, Government Affairs, Direct Marketing Association, Inc.

Ladies and gentlemen, if you would take your seats. What we might want to do—why don't you move to the center and we will get the staff to move the nameplates. If you move to the center, I think we probably would have a more productive session with you. I would ask staff to appropriately move the nameplates, and we can get started as soon as our committee settles down and we can ask our guests to take their seats.

Thank you very much. By unanimous consent, as you heard earlier, your written statements will be made a part of the record, so I would appreciate it if you did not read them to us. We have them in front of us. I would very much appreciate it if you would toss them aside right now and just kind of dialog with us. Give us the high points of your written testimony and any other comments that you want to make within a general 5-minute rule, which is the time allotted for witnesses and for members here at this hearing.

We will begin with Mr. Robert Lewin, Executive Director of TRUSTe. Mr. Lewin.

STATEMENTS OF ROBERT LEWIN, EXECUTIVE DIRECTOR, TRUSTe; DEIRDRE MULLIGAN, STAFF COUNSEL, CENTER FOR DEMOCRACY AND TECHNOLOGY; SOLVEIG SINGLETON, DIRECTOR OF TELECOMMUNICATIONS AND TECHNOLOGY STUDIES, CATO INSTITUTE; STEVEN LUCAS, CHIEF INFORMATION OFFICER AND SENIOR VICE PRESIDENT, INDUSTRY GOVERNMENT RELATIONS, PrivaSEEK; AND JERRY CERASALE, SENIOR VICE PRESIDENT, GOVERNMENT AFFAIRS, DIRECT MARKETING ASSOCIATION, INC.

Mr. LEWIN. Thank you, Mr. Chairman. My name is Bob Lewin, and I am the Executive Director of TRUSTe. I would like to start of again by thanking the chairman and the members of the committee for the opportunity to talk with you today.

As you know, TRUSTe is an Internet privacy seal program ,operating independent from government and industry. Our goal from the beginning was to develop a program that was understandable by consumers, but did have teeth to ensure compliance. I will talk more about this.

We feel that in the TRUSTe's seal that we have done this. When we developed the TRUSTe program in 1996, consumer privacy concern was barely a blip on the industry radar. But at that time several studies had pointed to the general distrust that the medium, primarily stemming from the fact that participation would compromise personal privacy, has raised the issue to the level that it is now. However, it is a complex problem as has already been pointed out.

How do you regulate business practices in a global medium that is constantly changing where you have rapid growth? What we tried to do with the TRUSTe privacy seal program is develop a solution that brings together government pressure with the discipline of self-regulation. That solution is what we call self-governance. Self-governance is a three-dimensional solution that applies and leverages various degrees of pressure from consumers, from government, and from the industry to implement the appropriate practices. Under that framework of self-governance, industry doesn't act alone; rather, it acts in concert with existing laws and mores.

With the TRUSTe program, if you draw the analogy with the Good Housekeeping Seal of Approval, which I understand is celebrating its 100th anniversary this year, just to keep it in prospective, perhaps that characterization is perhaps a little misleading. TRUSTe, we believe, is a more robust tool. There are few reasons to illustrate this. First, by displaying the seal, we go beyond just illustrating the commitment to the Web publisher to disclose privacy practices. But we provide consumers with an immediate and easy access to those policies with a click of the mouse.

Second, we have continually raised the minimum requirements for the program. When we started the program, all we had to do was ask a licensee to post a privacy policy. Today we require all new and renewing licensees to be in compliance with the FTC's fair information practices, all of the points that were talked about earlier.

Third, we work closely with respective licensees. We talk about Internet time, but the implementation of these times still involves people and the changes that are required within the organization. That time sometimes does not operate at the Internet speed that we all seem to have become accustomed to when we talk about technology. By providing consumers with more than a seal, by consistently raising the bar, and by being proactive in our advice to the Web sites, we have—we feel that we have become a leading facilitator of trusting relationships online.

We talked about the Georgetown Internet privacy survey. Suffice it to say that progress has been made. However, you look at that information depending on what side of the argument you are on, there has been some progress. Is it enough? Do we need to do more? Absolutely. Nobody disputes that. But progress has definitely been there.

Speaking for TRUSTe, in July 1997 we had 15 licensees. Today we are well past 100—800, sorry—well past 800. The acceleration in the number of licensees each month is tremendous. We will be by the end of this year well past 1,500 if the trends continue as they have been.

Now, while again we say there is significant progress, there is still a lot to do. First of all, since we have a solid foundation, now we want to spend more time and we will be focusing more time on consumer education. Last fall we did the Privacy Partnership, which was a grass-roots advertising program focused on educating online consumers on their privacy rights. It was led by an unprecedented bringing together of the large portal sites. That privacy partnership was the biggest online advertising campaign ever. It

had approximately 200 million banner ads that attracted 1 million people within a 3-week period of time.

Second, widespread consumer education and ubiquity is a priority, but our focus must be on guaranteeing the safety of the most vulnerable Web user, children. Last fall we launched the TRUSTe Children Privacy Seal Program in anticipation of the FTC's and Congress' move in this area. We have now—that has a higher level of privacy than is required for sites that are directed toward children. We enforce those through our program.

Last, our goal was to create a globally recognized privacy seal program. Now, with the rise of the European privacy directive and the implications of U.S. Business, it is critical to make our seal global, not just local, local being North America. To that end, we have recently expanded our program and appointed a European director, and we also have sites in Europe with the TRUSTe seal. By focusing our attention on consumer education, child protection and international expansion, we are making progress in not only getting ubiquity of the TRUSTe seal, but we are succeeding in creating a safer online environment.

I would like to conclude by thanking the chairman and members of the committee for giving us the opportunity to update you on where we are, but more importantly, where we are going. We are happy with the results from the FTC because it does demonstrate that progress has been made. But we also recognize that we have a lot more to do and we are committed to making it happen. Thank you.

[The prepared statement of Robert Lewin follows:]

PREPARED STATEMENT OF ROBERT LEWIN, EXECUTIVE DIRECTOR, TRUSTE

Thank you, Mr. Chairman. My name is Bob Lewin. I am the executive director of TRUSTe. I want to start off by thanking you, Mr. Chairman, and the members of the Committee for the invitation to speak today.

As many of you know, TRUSTe is an Internet privacy seal program operating independent from industry and government. For more than two years, we have been working to address consumer privacy concerns by providing Web businesses with the TRUSTe Privacy Seal, a symbol which effectively communicates a site's privacy practices and provides consumers with a powerful oversight mechanism. Our goal from the beginning was to establish a program easy enough for a consumer to understand, but with "teeth" to ensure compliance. With the TRUSTe seal, that is exactly what we accomplished.

I would like to spend a little time today talking to you about the TRUSTe program and where it is headed. I would also like to talk to you about how our program fits into the overall self-governance model and how that framework is proving to be the most effective way of ensuring the healthy growth of this new medium.

When we began development of the TRUSTe program in 1996, consumer privacy concern was barely a blip on the Industry's radar. But at the time several studies pointed to a general distrust in the medium, emanating largely from the fear that participation would compromise personal privacy. We understood, though, that this was only the tip of the iceberg and that the lack of trust would have staggering implications to the success of Internet commerce. Simply put, just as trust is critical to the healthy growth of communities, the absence of trust can cripple economic growth.

However, we were confounded by a complex problem: how do you regulate business practices on a global medium that is constantly changing and fast growing? It was clear to us that the answer was not in what many called self-regulation, defined by most as industry being given free-rein to act on its own accord. Similarly, we believed that government oversight in the form of laws and statutes wouldn't work within the global and evolving framework of the Internet.

What we created with the TRUSTe privacy seal program was a solution that melds the weight of government pressure with the discipline of self-regulation. That

solution is called self-governance. Self-governance is three-dimensional system that leverages a variety of pressure points (from consumers to government to industry) to implement appropriate practice. Under the framework of self-governance, industry doesn't act alone; rather, it acts in concert with existing laws and mores. [Some would say that this is the Internet's version of Checks and Balances].

Perhaps the brightest sign that the self-governance framework is working is the success of privacy seal programs, such as TRUSTe. I'd like to take a few minutes to describe our program, give you an overview of how the program is doing, and tell you where TRUSTe is headed.

In many ways, the TRUSTe program is the online privacy version of the Good Housekeeping Seal of Approval. Although even *that* characterization is a little misleading. TRUSTe is, in fact, a far more robust tool. There are a few reasons that best illustrate this.

First, displaying the TRUSTe seal goes beyond illustrating the commitment of the Web publisher to disclose privacy practices. TRUSTe provides consumers with immediate and easy access to the actual privacy policies by just the click of a mouse.

Second, the TRUSTe seal itself has raised its minimum standards of privacy practices disclosure. When we started the program we required only that TRUSTe licensee sites post privacy policies. Today, we require all of our new and renewing licensees to be in accordance with the Federal Trade Commission's standards for fair information practices.

Third, TRUSTe works closely with prospective licensees on the front end to ensure that their privacy practices are in-line with consumer demand. We invest a lot of our own resources to provide counsel to Web sites on how they can better develop trusted relationships online.

By providing consumers with more than just a seal, by consistently raising the bar of entry, and by pro-active counsel to prospective licensees, the TRUSTe privacy seal program has become a leading facilitator of trusted relationships online.

By every metric available, the self-governance model is working. According to the Georgetown Internet Privacy Policy survey, nearly two-thirds of all commercial Web sites are posting some kind of privacy disclosure. When you take that into context with previous benchmarks, the figure is staggering. While direct comparisons with the results of last year's FTC study cannot be made, the fact that 67 percent of sites now post privacy disclosures suggests significant progress has been made. And while we recognize that not all of these disclosures are as comprehensive as they could be, the TRUSTe program gives businesses the tools and the help they need to develop their privacy policies so that they are in line with fair information practices.

Progress can most clearly be seen in the success of the TRUSTe program.

To give you an idea of TRUSTe's growth, in July 1997 we had a total of 15 licensees. Today, that number has risen to more than 800. In fact, more than 90 percent of Web users are on TRUSTe approved sites each month. Looking to the future, our internal projections show that we will have more than 1500 licensees by the end of the year.

Privacy seal programs illustrate a self-governance model that allows an industry to impose rules on itself while, at the same time, exposing itself to outside scrutiny. If a TRUSTe licensee is found to have violated its agreement with us, not only can we sue them for contract violation, but the Federal Trade Commission can take action as well. Beyond that, sites found in violation of the licensing agreement are likely to suffer reputation stains that can jeopardize their market position.

But while a significant amount of progress has been made, there are still (to quote the poet) miles to go before we sleep.

First, now that we have built a solid foundation, our efforts moving forward will be focused on consumer education. In fact, we are already off to a good start. Last Fall TRUSTe formed the Privacy Partnership, a grassroots advertising campaign aimed at educating online consumers about their privacy rights. Led by an unprecedented union of all of the Internet portal sites, the Privacy Partnership has become the biggest online advertising campaign, *ever*.

Second, while widespread consumer education and ubiquity is a priority, our focus must be on guaranteeing the safety of the most vulnerable Web users: children. Last fall we launched the TRUSTe children's privacy seal, a special symbol that holds higher privacy standards for Web sites that target kids. In the next year, we will be placing emphasis on promoting this new seal to child-oriented sites.

Lastly, our goal from the outset was to create a globally recognized privacy seal that was suitable for the global Internet medium. With the rise of the European Privacy Directive and its implications to U.S. business, it is critical to make the TRUSTe seal applicable globally, not just locally. To that end, TRUSTe recently expanded its program by appointing an interim European director. We will continue to build that program out, as well as look to other regions for growth.

By focusing our efforts on consumer education, children's privacy and international expansion, we are making progress in not only gaining ubiquity for the TRUSTe privacy seal, but we are succeeding in creating a safer online environment for everyone.

I want to conclude by thanking you, Mr. Chairman, for inviting me here today. Online self-governance has become a distinct characteristic of the Internet. Privacy seal programs and the quick mobilization by the online community to address consumer privacy concerns indicate that the self-governance model is working. But we need to realize that self-governance, like the medium itself, is in its nascent stages.

The vision of self-governance is a result of the democratic quality of the Internet, where the law is defined largely by the engagement and participation of each community member. That requires the participation of all members of the Web community, from the media to businesses to advocacy groups, in educating consumers about their privacy rights online and what road signs to for on the Web. It also requires the engagement of public policy decision-makers in scrutinizing the activity of the online world. But, at the same time, it is critical now more than ever to not pass unnecessary regulations that will stand in the way of the healthy growth of this medium.

Based on the initial success of the TRUSTe program, the rise in popularity of e.commerce and the validating benchmarks of specific Web studies, we are well on our way to creating a safer and consumer empowering environment on the Web.

I would now be happy to answer any of your questions. Thank you.

Mr. TAUZIN. Thank you very much, Mr. Lewin.

Now, Ms. Deirdre Mulligan, Staff Counsel for the Center for Democracy and Technology.

STATEMENT OF DEIRDRE MULLIGAN

Ms. MULLIGAN. Thank you again for the opportunity to be here there. There is a little bit of a Groundhog Day feeling, having been here last year at this time, and I hope that my comments are substantially different, although I think that we are looking in many ways at a similar dilemma as in "Are we there yet?" and how best do we get there.

I would just like to emphasize three points before diverging from my written remarks. One, the Internet is incredibly unique and offers us unique opportunities. Literally, as you pointed out, as Mr. Cox pointed out, it offers some unique challenges to protecting privacy. Nowhere can individuals be traced and monitored like this anywhere in the off-line world. And I think that is probably the most important thing that the FTC has continued to bring to this discussion.

In their efforts, which I think have focused really on fairness when we talk about privacy, what do companies do with information, how much control do individuals have over information and now they are starting, having read through some of their reports, to diverge into some of the more tricky issues in the online arena. Unique identifiers, the issues posed by something like the Pentium III PSN; are we all going to have a digital dog tag as we wander around the Internet—online profiling, how much information is out there, what is being used, how it is being used. Is law enforcement, for example, gaining access to this data?

A report that the FTC delivered to you last year, 2 years ago now, in the individual reference services group identified that, in fact, private sector data is in fact very often used by law enforcement agencies. So talking about the flow of data back and forth between the public and private sectors is an important place that we need to look at.

The second is that privacy is a very complex value, and what the FTC has focused on over the past 4 years now has been the fairness component. There are other issues as the committee has pointed out earlier today. Individual expectations of privacy don't exist just vis-a-vis the private sector. They also are very alive and well, as we know, from things like the rejection of the know-your-customer rules, reactions to unique health identifiers vis-a-vis the government. In fact, we have been looking at what the government is doing about privacy protections and privacy protections on the World Wide Web. Two months ago, we actually did a survey of government privacy policies, what are they saying at Web sites, and found that about a third of them were not posting policies. There has since been some direction from OMB to actually step up.

I think the appointment by the White House of someone to look at privacy issues is another very positive step. We see privacy emerging as a much more important piece of both the administration and of the FTC's agenda as a consumer protection issue.

However, I want to step back and say, imagine if tomorrow when you woke up and you got out of bed and you walked down the street that you found out that cash had disappeared. When you went to buy your cup of coffee and your newspaper, when you went to buy your half-smoked or grilled cheese or whatever it might be at lunch, and perhaps the antacid and the Rogaine, everything that you purchased you were buying with your credit card. And that you also found out that every business that you went into, that 90 percent of them, perhaps more, before you even made a purchase, they were actually asking you for information before you actually made a purchase.

And in addition, a large majority of them when you walked into the store asked you, as a condition of shopping, to place this teeny-tiny newfangled camera called a "cookie" on your shoulder, because they want to get a sense of what you are doing. For good purposes, they want to improve how they are stocking their shelves, et cetera, but basically they want to monitor what it is that you are doing. Perhaps they don't know who you are, but they certainly care a lot about your preferences. Do you want the salmon or the filet mignon? How long did it take you to make up your mind?

In addition, you found out that later on in those practices, that information that was being stored in the private sector did become fodder for a Kenneth Starr, who is interested in what books you purchased; or the Drug Enforcement Agency, recently interested in what people are buying at the grocery store, how many little plastic bags are you purchasing, that this private information that is being collected within the private sector is bleeding back into our government actions.

I think that many of us would feel like the American public has said they do. The figures of 87 percent of the people being concerned in the online environment is exactly because this is the kind of environment that I think people feel like they face.

Now, I think the Internet is a wonderful place. I think technology has an enormous opportunity to help consumers protect their privacy, strong encryption, which this committee has been very powerful in working toward, their basic practices—TRUSTe, the Better Business Bureau OnLine, all of them are moving in the

right direction. There is certainly a candle that is burning and some of the bugs are flocking to the candle and some of them run away.

I think the question is always, how do we get to the bad actors? Unfortunately, I think that I feel as though we are in a similar position as we were last year. There has been much more progress. There are many more companies that are beginning to say things about privacy, and the leaders have taken some very bold steps, saying that we are not going to spend advertising dollars at Web sites that don't put in privacy policies; that is a very clear market incentive and it's the kind of thing that we need from leaders. However, when I look at a figure of 10 percent, and I look at 66 percent and I say, how do we get that 10 percent to be 100 percent, I have to say that I think we need the government also to play a role.

I think that working together through a combination of technology, self-regulation, and legislation that we can provide the comprehensive privacy protections that we need. But I think there is a lot of discussion that needs to happen, as the rulemaking going on in the Children's Online Protection Act right now highlights. Very difficult issues: When is data identifiable; access to information, how do we do it; when is information identifiable; when do people need to get access to it.

So this is not—I am very pleased that the FTC is going to continue to work on these hard issues. I certainly would welcome your future efforts to look at these hard issues, but I certainly think that the government has a role to play in this area.

[The prepared statement of Deirdre Mulligan follows:]

PREPARED STATEMENT OF DEIRDRE MULLIGAN, STAFF COUNSEL, CENTER FOR DEMOCRACY AND TECHNOLOGY

I. OVERVIEW

The Center for Democracy and Technology (CDT) is pleased to have this opportunity to testify about privacy in the online environment. CDT is a non-profit, public interest organization dedicated to developing and implementing public policies to protect and advance civil liberties and democratic values on the Internet. One of our core goals is to enhance privacy protections for individuals in the development and use of new communications technologies. We thank the chairman and Representatives Markey and Boucher for holding this hearing and for their commitment to seeking policies that support both civil liberties and a vibrant Internet.

CDT wishes to emphasize three points this morning:

- The Internet presents new challenges and opportunities for the protection of privacy. Our policies must be grounded in an understanding of the medium's unique attributes and its unique potential to promote democratic values.
- Privacy is a complex value. In the context of this discussion, we believe Congress should focus on ensuring that individuals' long-held expectations of autonomy, fairness, and confidentiality are respected as daily activities move online. These expectations exist vis-à-vis both the public and the private sectors.

  By autonomy, we mean the individual's ability to browse, seek out information, and engage in a range of activities without being monitored and identified.

  Fairness requires policies that provide individuals with control over information that they provide to the government and the private sector. The concept of fairness is embodied in the Code of Fair Information Practices[1]—long-

[1] The Code of Fair Information Practices as stated in the Secretary's Advisory Comm. on Automated Personal Data Systems, *Records, Computers, and the Rights of Citizens*, U.S. Dept. of Health, Education and Welfare, July 1973:

Continued

accepted principles specifying that individuals should be able to "determine for themselves when, how, and to what extent information about them is shared."[2] The Code also requires that those who collect and use personal information do so in a manner that respects individuals' privacy interests. Self-regulatory efforts designed for the online environment are gradually moving closer to the standards for privacy protection set out in the Code of Fair Information Practices. However, legislation, as well as robust self-regulation, is both inevitable and necessary to ensure privacy protection is the rule rather than the exception on the Internet.

In terms of confidentiality, we need a strong Fourth Amendment in cyberspace. But confidentiality protections—both technical and legal—are growing increasingly porous as technology changes and more information resides outside of the home on networks. It is time to update and strengthen the Electronic Communications Privacy Act. Further, our laws protecting privacy will have limited impact in the global environment. For that reason, to ensure that citizens and businesses have the ability to protect their sensitive information and communications, the government must change its policy course on encryption.

- Preserving these core elements of privacy on the Internet requires a thoughtful, multi-faceted approach combining self-regulatory, technological, and legislative components.

II. WHAT MAKES THE INTERNET DIFFERENT?

CDT focuses much of its work on the Internet because we believe that it, more than any other medium, has characteristics—architectural, economic, and social—that are uniquely supportive of democratic values. Because of its decentralized, open, and interactive nature, the Internet is the first electronic medium to allow every user to "publish" and engage in commerce. Users can reach and create com-

---

There must be no personal data record-keeping systems whose very existence is secret.

There must be a way for an individual to find out what information about him is in a record and how it is used.

There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent.

There must be a way for the individual to correct or amend a record of identifiable information about him.

Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data. Id. at xx

The Code of Fair Information Practices as stated in the *OECD guidelines on the Protection of Privacy and Transborder Flows of Personal Data* http://www.oecd.org/dsti/sti/ii/secur/prod/PRIV—EN.HTM

1. Collection Limitation Principle: There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

2. Data quality: Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

3. Purpose specification: The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

4. Use limitation: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the "purpose specification" except: (a) with the consent of the data subject; or (b) by the authority of law.

5. Security safeguards: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

6. Openness: There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

7. Individual participation: An individual should have the right: (a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; (b) to have communicated to him, data relating to him: within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and, in a form that is readily intelligible to him; (c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and, (d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified completed or amended.

8. Accountability: A data controller should be accountable for complying with measures which give effect to the principles stated above.

[2] Alan Westin. *Privacy and Freedom* (New York: Atheneum, 1967), 7.

munities of interest despite geographic, social, and political barriers. As the World Wide Web grows to fully support voice, data, and video, it will become in many respects a virtual "face-to-face" social and political milieu.

But while the First Amendment potential of the Internet is clear, and recognized by the Supreme Court, the impact of the Internet on individual privacy is less certain. Will the online environment erode individual privacy—building in national identifiers, tracking devices, and limits on autonomy? Or will it breathe new life into privacy—providing protections for individuals' long held expectations of privacy?

The Internet poses both challenges and opportunities to protecting privacy. The Internet accelerates the trend toward increased information collection that is already evident in our offline world. The trail of transactional data left behind as individuals use the Internet is a rich source of information about their habits of association, speech, and commerce. When aggregated, these digital fingerprints reveal a great deal about an individual's life. The global flow of personal communications and information coupled with the Internet's distributed architecture presents challenges for the protection of privacy. However, Anonymizers, anonymous remailers, and other privacy-enhancing tools allow individuals to create zones of privacy—limiting who knows what about them and protecting their sensitive communications from prying eyes. Computer code and products are becoming increasingly critical to the protection of privacy in this distributed environment. With privacy-enhancing tools users will be empowered to control their personal information in new ways.

As we move swiftly toward a world of electronic democracy, electronic commerce and indeed electronic living, it is critical to construct a framework of privacy protection that fits with the unique opportunities and risks posed by the Internet. But as Congress has discovered in its attempts to regulate speech, this medium deserves its own analysis. Laws developed to protect interests in other media should not be blindly imported. To create rules that map onto the Internet, we must fully understand the characteristics of the Internet and their implications for privacy protection. We must also have a shared understanding of what we mean by privacy. Finally we must assess how to best use the various tools we have for implementing policy—law, computer code, industry practices, and public education—to achieve the protections we seek.

III. THE EROSION OF PRIVACY AND THE PATH TOWARDS ITS RESTORATION

There are several core "privacy expectations" that individuals have long held vis-à-vis both the government and the private sector, the protection of which should carry over to interactions on the Internet. Surveys of Internet users, and would-be Internet users, reveal a high level of concern with threats to privacy online. Surveys suggest that concern over privacy is keeping individuals off the Internet[3], retarding the growth of e-commerce[4], and leading individuals to engage in privacy-protective behaviors such as providing false information.[5] A recent survey of Internet users found that 87% are concerned about threats to their personal privacy.[6]

The remainder of our testimony will discuss the three critical privacy expectations of autonomy, fairness, and confidentiality, explore the changes in technology and policies that threaten them, and finally outline a plan for their restoration.

A. The Expectation of Autonomy

1. Why is it at risk? Imagine walking through a mall where every store, unbeknownst to you, placed a sign on your back. The signs tell every other store you visit exactly where you have been, what you looked at, and what you purchased. Something very close to this is possible on the Internet.

When individuals surf the World Wide Web, they have a general expectation of anonymity, more so than in the physical world where an individual may be observed by others. As documented in several surveys, individuals value their anonymity and will take steps, such as providing false information and refusing to register, to protect it.[7] Online, individuals often believe that if they have not affirmatively disclosed

---

[3] A 1998 Business Week Survey found that privacy was the number one reason individuals are choosing to stay off the Internet, coming in well ahead of cost, concerns with complicated technology, and concerns with unsolicited commercial email. Business Week, March 16, 1998.

[4] A TRUSTe and Boston Consulting Group survey conducted in 1997 found that privacy concerns were leading users to limit their engagement in electronic commerce.

[5] Id. and see footnote 6.

[6] *Beyond Concern: Understanding Net Users Attitudes About Online Privacy*, AT&T, 1999.

[7] The 8th *annual poll of the Grahpics, Visualization, and Usability Center at the Georgia Institue of Technology* found that in order to protect their privacy, significant numbers of people

Continued

information about themselves, then no one knows who they are or what they are doing. But, contrary to this belief, the Internet generates an elaborate trail of data detailing every stop a person makes. The individual's employer may capture this data trail if she logs on at work, and it is captured by the Web sites the individual visits. This transactional or click stream data can provide a "profile" of an individual's online life.

Two recent examples highlight the manner in which individuals' expectation of autonomy is increasingly challenged in the online environment. (1) The introduction of the Pentium III processor equipped with a unique identifier (Processor Serial Number) threatens to greatly expand the ability of Web sites to surreptitiously track and monitor online behavior. The PSN could become something akin to the Social Security Number of the online world—a number tied inextricably to the individual and used to validate one's identity throughout a range of interactions with the government and the private sector. (2) The Child Online Protection Act (COPA), passed in October, requires Web sites to prohibit minors' access to material considered "harmful to minors." Today, when an individual walks into a convenience store to purchase an adult magazine, they may be asked to show some identification to prove their age. Under the COPA, an individual will be asked not only to show their identification, but also to leave a record of it and their purchase with the online store. Such systems will create records of individuals' First Amendment activities, thereby conditioning adult access to constitutionally protected speech on a disclosure of identity. This poses a Faustian choice to individuals seeking access to information—protect privacy and lose access or exercise First Amendment freedoms and forego privacy.

2. The Path to Individual Autonomy Online

While the global, distributed environment of the Internet raises challenges to our traditional methods of implementing policy, the specifications, standards, and technical protocols that support the operation of the Internet offer a new way to implement policy decisions. In the area of autonomy, focusing on standards and applications is crucial. By building systems that respect individuals varied needs for identification, pseudonymity, and anonymity—building a digital wallet with cash, credit cards, a metro fare card, and a driver's license—will help build an online environment that promotes autonomy. By building privacy into the architecture of the Internet, we have the opportunity to advance public policies in a manner that scales with the global and decentralized character of the network. As Larry Lessig repeatedly reminds us, "(computer) code is law."

Accordingly, we must promote specifications, standards and products that protect privacy. A privacy-enhancing architecture must incorporate, in its design and function, individuals' expectations of privacy. For example, a privacy-friendly architecture would provide individuals the ability to "walk" through the digital world, browse, and even purchase without disclosing information about their identity, thereby preserving their autonomy. Of course, it would also provide individuals the opportunity to create relationships that are identifiable—or at least authenticated—for engaging in activities such as banking. This would be coupled with policies that allow individuals to control when, how, and to whom personal data collected during interactions is used or disclosed.

While there is much work to be done in designing a privacy-enhancing architecture, some substantial steps toward privacy protection have occurred. Positive steps to leverage the power of technology to protect privacy can be witnessed in tools like the Anonymizer, Crowds, and Onion Routing, which shield individuals' identity during online interactions, and encryption tools such as Pretty Good Privacy that allow individuals to protect their private communications during transit. Coupled with rules such as those found in the Government Paperwork Elimination Act of 1998, which established privacy protections governing personal information collected when the public uses electronic signature systems,[8] technology may evolve in ways that support individuals' interest in autonomy.

The law prohibits companies that collect such information from using or disclosing it without the permission of the person involved. Authored by Senators Leahy and

---

falsify information online. Particularly, users report regularly falsifying registration information. The most common reason for not registering is the lack of a statement about how the information will be used. In addition, the GVU study showed that users would rather not access a site than reveal information. (1998)

The survey *Beyond Concern: Understanding Net Users Attitudes About Online Privacy* found that individuals were reluctant to provide identifying information such as credit card numbers but were more willing to provide information that did not identify them. AT&T (1999)

[8] Many such systems gather sensitive information in the course of providing and guaranteeing an electronic signature.

Abraham, this marks the first attempt to craft a legislative approach to dealing with the potential erosion of privacy created by electronic signature use.

B. The Expectation of Fairness and Control Over Personal Information

1. Who controls the data? When individuals provide information to a doctor, a merchant, or a bank, they expect that those professionals/companies will collect only information necessary to perform the service and use it only for that purpose. The doctor will use it to tend to their health, the merchant will use it to process the bill and ship the product, and the bank will use it to manage their account—end of story. Unfortunately, current practices, both offline and online, foil this expectation of privacy. Much of the concern with privacy in electronic commerce stems from a lack of privacy rules in various sectors of the economy, such as financial and health, that handle a treasure trove of sensitive information on individuals.

Whether it is medical information, or a record of a book purchased at the bookstore, or information left behind during a Web site visit, information is routinely collected without the individual's knowledge and used for a variety of other purposes without the individual's knowledge—let alone consent.

Focusing on the online environment, we now have information from two studies assessing the state of privacy notices on the World Wide Web. Last June, the Federal Trade Commission's "Privacy Online: A Report to Congress" found that despite increased pressure, businesses operating online continued to collect personal information without providing even a minimum of consumer protection. The report looked only at whether Web sites provided users with notice about how their data was to be used; there was no discussion of whether the stated privacy policies provided adequate protection. The survey found that, while 92% of the sites surveyed were collecting personally identifiable information, only 14% had some kind of disclosure of what they were doing with personal data.

The newly released Georgetown Internet Privacy Policy Survey provides new data. The Survey was designed to provide an update on the state of privacy policies on the World Wide Web. The study shows that definite progress has been made in making many more Web sites privacy-sensitive, but substantive privacy protections are still far from ubiquitous on the World Wide Web. While more Web sites are mentioning privacy, only 9.5% provide the types of notices *required* by the Online Privacy Alliance, the Better Business Bureau and TRUSTe. Indeed, fair information practices on the Web appear to remain the exception, not the rule.

The Georgetown Survey shows that, spurred by surveys documenting consumer concern and anxiety, and the work of individual companies[9] and industry self-regulatory entities such as TrustE, the Online Privacy Alliance, and the Better Business Bureau, an increased number of Web sites are providing consumers with *some* information about what personal information is collected (44%), and how that information will be used (52%). Companies posting fuller information about their data handling[10] are more likely to make them accessible to consumers. Many have a link to such statements from the home page (79.7%).[11]

However, on important issues such as access to personal information and the ability to correct inaccurate information, the Georgetown Survey shows that only 22% and 18% respectively of these highly trafficked Web sites provide consumers with notice. On the important issue of providing individuals with the capacity to control the use and disclosure of personal information, the survey finds that 39.5% of these busy Web sites say that consumers can make some decision about whether they are re-contacted for marketing purposes—most likely an "opt-out"—and fewer still, 25%, say they provide consumers with some control over the disclosure of data to third parties.[12]

---

[9] For example, IBM recently stated that it would limit its advertising to Web sites that post privacy notices.

[10] The report calls these "privacy policies" as compared to "information practice statements." "Privacy policies" are a more comprehensive description of a site's practices that are located in a single place and accessible through an icon or hyperlink. A site may have a "privacy policy" by this definition but still not have a privacy policy that meets the elements set out by the FTC or various industry self-regulatory initiatives for an adequate privacy policy.

[11] In response to the question, "Is a Privacy Policy Notice easy to find?" surfers in the 1998 survey answered yes for approximately 1.2% of Web sites. FTC Report, Appendix C Q19.

[12] This number is generated using the data from Q32 (number of sites that say they give consumers choice about having collected information disclosed to outside third parties)—64—and dividing it by 256 (the total survey sample (364) minus the number of sites that affirmatively state they do not disclose data to third-parties (Q29A) (69) and the number of sites that affirmatively state that data is only disclosed in the aggregate (Q30) (39)).

Overall, the Georgetown survey reveals that, at over 90% of the most frequently trafficked Web sites,[13] consumers are not being adequately informed about how their personal information is handled.[14] At the same time the survey found that over 90% of these same busy consumer-oriented Web sites are collecting personal information.[15] In fact, the survey revealed an increase in the number of Web sites collecting sensitive information such as credit card numbers (up 20%), names (up 13.3%), and even Social Security Numbers (up 1.7%).

Thus, while many companies appear to be making an effort to address some privacy concerns, the results from the consumer perspective appear to be a quilt of complex and inconsistent statements. The number of sites that provide consumers with the types of notices required by the Online Privacy Alliance, the Better Business Bureau and TrustE, and called for by the Federal Trade Commission and the Administration, is still relatively small (9.5%).

The posting of privacy notices is not just a private sector issue. In a recent CDT study of federal agency Web sites, we found that just over one-third of federal agencies had a "privacy notice" link from the agency's home page. Eight other sites had privacy policies that could be found after following a link or two and on 22 of the sites surveyed we could not find a privacy policy at all.

The lack of widespread adherence to Fair Information Practices is undermining consumer confidence. A recent survey by the National Consumers League found that the majority of online users are not comfortable providing credit card (73%), financial (73%), or personal information (70%) to businesses online.[16] Due to privacy concerns 42% of those who use the Internet are using it solely to gather information, while a smaller 24% actually venture to purchase goods online.[17] A second study found that 58% of consumers do not consider financial transactions online to be safe, and 77% do not believe it is safe to provide a credit card number through a computer.[18] Privacy has been rightly identified by the Federal Trade Commission, Congress, the business community, and advocacy organizations as a critical consumer protection issue in e-commerce.

2. Establish Rules That Give Individuals Control Over Personal Information During Commercial Interactions. We must adopt enforceable standards, both self-regulatory and legislative, to ensure that information provided for one purpose is not used or redisclosed for other purposes without the individual's consent. All such efforts should focus on the Code of Fair Information Practices developed by the Department of Health, Education and Welfare in 1973. The challenge of implementing privacy practices on the Internet is ensuring that they build upon the medium's real-time and interactive nature to foster privacy and that they do not unintentionally impede other beneficial aspects of the medium. Implementing privacy protections on the global and decentralized Internet is a complex task that will require new thinking and innovative approaches.

The Georgetown Survey supports our belief hat a combination of means—self-regulation, technology, and legislation—are required to provide privacy protections on the Internet. The study, as discussed above, shows that some progress has been made in making many more Web sites privacy sensitive, but substantive privacy protections are still far from ubiquitous on the World Wide Web. Because many Web sites need baseline policy guidance and because self-enforcement mechanisms, while emerging, may not always provide a viable remedy, we believe that legislation is both inevitable and necessary to ensure consumers' privacy on the Internet.

To achieve real privacy on the Internet, we will need more than better numbers, redoubled efforts by industry, or a legislative mantra. We will need a good-faith concerted effort by industry, consumer and privacy advocates, and policymakers to develop real and substantive answers to a number of difficult policy issues involving the scope of identifiable information, the workings of consent and access mechanisms, and the structure of effective remedies that protect privacy without adversely affecting the openness and vitality of the Internet.

As the Federal Trade Commission's rulemaking under the Children's Online Privacy Protection Act and industry's various efforts at self-regulation show, these issues are not easy. But armed with the findings of the Georgetown Internet Privacy

---

[13] Only 9.5% of the most frequently visited Web sites and 14.7% of those that collect information had privacy policies containing critical information called for by the FTC, the Adminiatration, and required by the Online Privacy Alliance, TrutstE and the BBB Online, about notice; choice; access; aecurity; and contact information.

[14] Last years survey found approximately 2% or Web sites that collected data, and less than 1% of all Web sites, had adequate noticea.

[15] 92.9% are collecting some type of personal information.

[16] *Consumers and the 21st Century*, National Consumers League (1999).

[17] Id.

[18] *National Technology Readiness Survey*, conducted by Rockridge Associates (1999).

Policy Survey, we believe interested parties are in a position to move forward on a three pronged approach—expanded self-regulation, work to develop and deploy privacy-enhancing technologies such as P3P, and legislation—all require a serious dialogue on policy and practice options for resolving difficult issues in this promising medium.

In its testimony last July, the Federal Trade Commission stated that, "...unless industry can demonstrate that it has developed and implemented broad-based and effective self-regulatory programs by the end of this year, additional governmental authority in this area would be appropriate and necessary."[19] Despite the considerable effort of Congress, the Federal Trade Commission, the Administration and industry to encourage and facilitate an effective self-regulatory system to protect consumer privacy, based on the survey results we do not believe that one has yet emerged. Like Commissioner Anthony, we believe that industry leadership and self-regulatory programs are a critical component of a privacy framework for the Internet but that legislation is also necessary to establish a baseline and ensure consumers are protected from bad actors.

Last year, the Federal Trade Commission offered a legislative outline that embodied a framework, similar to the one we suggest, building upon the strengths of both the self-regulatory and regulatory processes. This year several bills have been introduced on a wide range of privacy issues. Senators Burns and Wyden,[20] and Leahy[21] have introduced proposals as have Representatives Goodlatte and Boucher,[22] and Vento.[23] We anticipate additional proposals from Senators Kohl, Torricelli, Dewine, and Hatch, and Representative Markey. Historically, for privacy legislation to be successful, it must garner the support of at least a section of the industry. To do so, it generally must build upon the work of some industry members—typically binding bad actors to the rules being followed by industry leaders—or be critically tied to the viability of a business service or product as with the Video Privacy Protection Act and the Electronic Communications Privacy Act.

Several companies have staked out leadership positions on the issue of online privacy and several self-regulatory programs have formed to drive industry best practices online. Numerous surveys have documented that consumers are concerned about their privacy in e-commerce. In addition, work is underway to develop the tools necessary to implement fair information practices on the World Wide Web. The World Wide Web Consortium's Platform for Privacy Preferences ("P3P") is a promising development. The P3P specification will allow individuals to query Web sites for their policies on handling personal information and to allow Web sites to easily respond. While P3P does not drive the specific practices, it is a standard designed to promote openness about information practices, to encourage Web sites to post privacy policies and to provide individuals with a simple, automated method to make informed decisions. Through settings on their Web browsers, or through other software programs, users will be able to exercise greater control over the use of their personal information. Regardless of how policies are established, an Internet-centric method of communicating about privacy is part of the solution.

As Congress moves forward this year, we look forward to working with you and all interested parties to ensure that fair information practices are incorporated into business practices on the World Wide Web. Both legislation and self-regulation are only as good as the substantive policies they embody. As we said at the start, crafting meaningful privacy protections that map onto the Internet requires us to resolve several critical issues. While consensus exists around at least four general principles (a subset of the Code of Fair Information Practices)—notice of data practices; individual control over the secondary use of data; access to personal information; and, security for data—the specifics of their implementation and the remedies for their violation must be explored. We must wrestle with difficult questions: When is information identifiable? How is it accessed? How do we create meaningful and proportionate remedies that address the disclosure of sensitive medical information as well as the disclosure of inaccurate marketing data? For the policy process to successfully move forward these hard issues must be more fully resolved. We look for-

---

[19] Last years survey found approximately 2% or Web sites that collected data, and less than 1% of all Web sites, had adequate notices. *Privacy Online: A Report to Congress*, Federal Trade Commission, June 1998.

[20] The Online Privacy Protection Act of 1999 (S. 809), introduced on April 15, 1999, by Senators Burns (R-MT) and Wyden (D-OR).

[21] Electronic Rights for the Twenty-First Century Act of 1999 (E-RIGHTS) (S. 854), introduced on April 21, 1999 by Senator Leahy (D-VT).

[22] Internet Growth and Development Act of 1999 (H.R. 1685), introduced on May 5, 1999 by Representatives Boucher (D-VA) and Goodlatte (R-VA).

[23] Consumer Internet Privacy Protection Act of 1999 (H.R. 313), introduced on January 6, 1999, by Representative Vento (DFL-MN).

ward to working with the Committee to explore these issues and develop a framework for privacy protection in the online environment. The leadership of Internet-savvy members of this Committee and others will be critical aa we seek to provide workable and effective privacy protections for the Internet.

C. The Expectation of Confidentiality

1. Who has access to records in cyberspace? When individuals send email they expect that only the intended recipient will read it. In passing the Electronic Communications Privacy Act in 1986, Congress reaffirmed this expectation. Unfortunately, it ia once again in danger.

While United States law provides email the same legal protection as a first class letter, the technology leaves unencrypted email as vulnerable as a postcard. Compared to a letter, an email message is handled by many independent entities and travels in a relatively unpredictable and unregulated environment. To further complicate matters, the email message may be routed, depending upon traffic patterns, overseas and back, even if it is a purely domestic communication. While the message may effortlessly flow from nation to nation, the privacy protections are likely to stop at the border.

Email is just one example. Today our diaries, medical records, and confidential documents are more likely to be out in the network than stored in our homes. As our wallets become "e-wallets" housed somewhere out on the Internet rather than in our back-pockets, the confidentiality of our personal information is at risk. The advent of online datebooks, and producta such as Novell's "Digital Me", and sites such as Wellmed.com[24] which invite individuals to take advantage of the convenience of the Internet to manage their lives, financial information, and even medical records raise increasingly complex privacy questions. While the real "me" has Fourth and Fifth Amendment protections from the government, the "Digital Me" is increasingly naked in cyberspace.

2. Protecting the Privacy of Communications and Information. Increasingly, our most important records are not "papers" in our "houses" but "bytes" stored electronically at distant "virtual" locations for indefinite periods of time and held by third parties. The Internet, and digital technology generally, accelerate the collection of information about individuals' actions and communications. Our communications, rather than disappearing, are captured and stored on servers controlled by third parties. Daily interactions such as our choice of articles at a news Web site, our search and purchase of an airline ticket, and our use of an online date book, such as Yahoo's calendar, leave detailed information in the hands of third-parties. With the rise of networking and the reduction of physical boundaries for privacy, we must ensure that privacy protections apply regardless of where information is stored.

Under our existing law, there are now essentially four legal regimes for access to electronic data: 1) the traditional Fourth Amendment standard for records stored on an individual's hard drive or floppy disks; 2) the Title III-Electronic Communications Privacy Act standard for records in transmission; 3) the standard for business records held by third parties, available on a mere subpoena to the third party with no notice to the individual subject of the record; and 4) a statutory standard allowing subpoena access and delayed notice for records stored on a remote server, such as the diary of a student stored on a university server, or personal correspondence stored on a corporate server.

As the third and fourth categories of records expand because the wealth of transactional data collected in the private sector grows and people find it more convenient to store records remotely, the legal ambiguity and lack of strong protection grows more significant and poses grave threats to privacy in the digital environment.

Congress took the first small step towards recognizing the changing nature of transactional data with amendments to the Electronic Communications Privacy Act enacted as part of the Communications Assistance for Law Enforcement Act of 1994 ("CALEA"). But the ongoing and accelerating increase in transactional data and the detail it reveals about individuals' lives suggests that these changes are insufficient to protect privacy.

Moreover, the Electronic Communications Privacy Act must be updated to provide a consistent level of protection to communications and information regardless of

[24] WellMed.com is a proprietary Online Health Management System which works by collecting personal health information from individuals, analyzing that information to develop unique health profiles which are used for a variety of purposes. One service is HealthNow!—"an online personal health record enabling secure, confidential, and private storage, management, and maintenance of health information by individuals and their families. HealthNow affords easy access of medical records from one central location anytime and anywhere the need arises."

where they are stored and how long they have been kept. Senator Leahy's recently introduced legislation is an effort to restore 4th Amendment protections to our personal papers. Technologies that invite us to live online will quickly create a pool of personal data with the capacity to reveal an individual's travels, thoughts, purchases, associations, and communications. We must raise the legal protections afforded to this growing body of detailed data regardless of where it resides on the network.

IV. CONCLUSION

No doubt, privacy on the Internet is in a fragile state. It is clear that our policy framework did not envision the Internet as we know it today, nor did it foresee the pervasive role information technology would play in our daily lives. Our legal framework for protecting individual privacy in electronic communications, while built upon constitutional principles buttressed by statutory protections, reflects the technical and social "givens" of specific moments in history. Crafting privacy protections in the electronic realm has always been a complex endeavor. Reestablishing protections for individuals' privacy in this new environment requires us to focus on both the technical aspects of the Internet and on the practices and policies of those who operate in the online environment.

However, there is new hope for its restoration. Providing a web of privacy protection to data and communications as they flow along networks requires a unique combination of tools—legal, policy, technical, and self-regulatory. We believe that legislation is an essential element of the online privacy framework. Whether it is setting limits on government access to personal information, ensuring that a new technology protects privacy, or developing legislation—none will happen without discussion, debate, and deliberation. Providing protections for individual privacy is essential for a flourishing and vibrant online community and marketplace. We thank the Committee for the opportunity to share our views and look forward to working with the members and staff and other interested parties to foster privacy protections for the Digital Age.

Mr. TAUZIN. Thank you, Ms. Mulligan.

Next will be Ms. Solveig Singleton, Director of Telecommunications and Technology Studies for CATO.

Ms. Singleton.

STATEMENT OF SOLVEIG SINGLETON

Ms. SINGLETON. Thank you, Mr. Chairman. My name is Solveig Singleton. I am a lawyer at the CATO Institute.

What I would like to do today is raise some key questions about the interest in Federal standards for privacy. And essentially, as some of you may know, my answers to those questions are very controversial, but I hope that we can all agree that the questions themselves are important and that the sheer number of these questions should give Federal regulators pause before they move toward Federal privacy standards.

The first point that I would like to make is that essentially there has never been a serious philosophical debate about whether privacy in this sense that we are talking about today is a right or whether it is a complex mix of preferences and questions of business ethics. That is to say, it is pretty clear that Americans have a right of privacy against the government; that is guaranteed by the fourth amendment to the United States Constitution. But the default rule in the private sector has generally been that people and businesses feel free to communicate information about real people and real events to other businesses. There are exceptions to that rule, but I think that even in the case of a new technology like the Internet, it is very important to have this philosophical debate about the free flow of information versus controls on that information before we move ahead.

Another point is that I think one of the unarticulated assumptions behind the interest in Federal standards for privacy has been that targeted marketing, which consumers tend to be very suspicious of is, in fact, an activity that they should be suspicious of and there is harm that they need to be protected from, so if it is a casualty of Federal privacy standards, we don't need to worry very much.

But I think there is actually a lot of empirical research that has been done on the role that advertising plays in enhancing competition, in giving consumers more choices and essentially in getting them information that they wouldn't get otherwise. While that information may seem to be biased, it is better to get biased information from 12 different companies than to get no information at all or just a trickle of information.

Let me think. What is another one?

I would also like to underscore that based on survey data, the approach to the privacy problem has started at the FTC with the strong view that something needs to be done about this in order for consumers to have trust in electronic commerce and, in addition, that there is reason to believe that businesses will not respond to this consumer demand on their own.

But I think that there has been very little discussion sort of at an economics level of exactly why it is that there would be consumer demand that somehow businesses would not respond to. If you look at the high-tech marketplace, you see an awful lot of businesses offering and catering to very many strange and diverse consumer tastes. It is possible that they are going to be stubborn about privacy if consumers really demand it, but it seems unlikely.

So I guess looking at the electronic privacy marketplace, if you see not everyone is coming on board with a privacy standard right away, maybe that is just they are being perverse and stubborn in some way; but maybe also it is because, in fact, that in their real-world experience, the consumer demand for privacy, while it might be something that they strongly express in surveys, simply does not materialize in their real-world experience. So it is important to question the assumptions that we are making as we go forward with this debate, just in case those assumptions were not in fact very accurate.

In following up with this point, I will make the quick point that if we were talking about a question like cable rate deregulation, the committee wouldn't sort of even begin to consider going forward if what the FTC had to offer them was a survey of consumers saying that consumers wanted lower cable rates, which I am sure they do. But clearly the question is a lot more complicated than that. So I think that surveys can only be a very small part of this picture. There are a lot of holes in our understanding of what is going on with electronic commerce. I have laid out some alternative studies in my written testimony, including evidence about the cost savings to consumers, the impact on competition and so on.

I can see that I should wrap up pretty quickly. I will just say finally that another important question relates to bad actors. I think it is very important that when you look at the enormous experimentation that is going on out there in the business world, you

don't automatically put somebody in the category of a bad actor simply because he has not posted a privacy policy.

I will now conclude. Thank you.

[The prepared statement of Solveig Singleton follows:]

PREPARED STATEMENT OF SOLVEIG SINGLETON, DIRECTOR OF INFORMATION STUDIES, THE CATO INSTITUTE

Mr. Chairman, my name is Solveig Singleton and I am a lawyer at the Cato Institute. In keeping with the truth in testimony rules, I note that the Cato Institute does not receive any money at all from the federal government, nor has it in the past.

Today I will raise some key questions about the push for more federal standards on privacy, and propose some answers. In a sense, the most valuable thing I have to offer will be the questions—it's hard to do the answers justice in a short period of time. But I hope we can all agree that the questions I raise are serious ones. The persistence and nature of these questions in itself should give Congress pause before it regulates.

Essentially, I'll make these points:

- Strange assumptions about business ethics and markets underlie the push for federal atandards.
- Huge holes remain in our understanding of the economics of e-commerce and of the economic benefits of the free flow of information.
- The standards by which self-regulation has been judged have often been quite unreasonable.

PRIVACY PREMISES ABOUT MORALITY

One key assumption behind the privacy movement is that we know that customers ought to have notice and consent about how information about them arising from a transaction should be used, as a matter of right.

But does this really make sense? Ordinarily, we are free to make all kinds of observations about other people without their consent (this is how journalists make their living). If two people interact in a transaction, why should one party have a right to exclude the other from using the information arising from it? If I buy a lawnmower from Sears, there's two entities involved in the transaction—me, and Sears. Why should I have a sole claim on the information relating to that event? In a country that takes the free flow of information seriously, why should I have the right to veto Sear's decision if it's managers choose to tell another business about that transaction—communicating information about real people and real events?

In the context of e-commerce, especially with sensitive information, some businesses will give notice or experiment with more sophisticated privacy options to retain customer loyalty—just as it has been vital for doctors to respect their patients' confidentiality. But this is a complex matter of business ethics—the one-size-fits-all approach won't work. Privacy is a preference that will vary from person to person, place to place, and over time. In some contexts it will matter to consumers and business. In others, it will not.

In this country, with its long tradition of respect for business and for the free flow of information, the assumption that the secondary use of information collected from web sites ought to be sending us into a frenzy of moral outrage is very peculiar. To illustrate this point, a story ran in the *New York Times* about Vice President Al Gore'a "Write to the Vice President" web site. Somebody noticed that this site collected the names, addresses, grades, schools, and ages of children without requiring parental consent. Since then, its been changed. My point is about Al Gore's web master. I'm sure when his web master was designing that web page it did not even occur to him that asking for this information without getting consent was anything other than a normal, natural thing to do. This illustrates just how new this is, how odd the tone of moral outrage that marks the movement towards federal standards on privacy. It is removed from centuries of normal human experience.

The debate about privacy is not just a debate of right versus economics. It is a debate about the free flow of information versus controls on that information. Furthermore, the default rules for how human beings exchange information about one another favor the freedom of information—with privacy being by special arrangement. Generally, human beings are free to make observations about other human beings, and record and report these—so long as they do not violate a confidentiality agreement, hack into someone's web site, or break into their house. Usually our pri-

vacy rights have been bounded by property right and contract obligations, with a handful of narrow privacy torts available at common law.

PRIVACY PREMISES ABOUT MARKETS

A key unarticulated assumption behind the push for federal privacy standards is that is that marketing exploits consumers and is not useful to them—so we don't need to worry much if our regulation strangles targeted marketing. This is the old-fashioned view. But empirical research has established that marketing play a crucial role in getting information into the hands of consumers. Some of the information conveyed through advertising is biased (that's the point, and everyone knows it), but biased information from a variety of sources is far better than none. Advertising plays a key role in heightening competition, lowering prices, and improving choice and quality; more targeting simply means it can play that role at a lower cost. Consumers do not need to be protected from these things.

There's another peculiar assumption here, and that is the idea that somehow broad privacy protections (as opposed to just good security practices) are vital to the growth of electronic commerce, *but somehow e-commerce companies are so silly that they won't move forward and give consumers what they want on their own.* Now if you start with that assumption and look at the world—yes, you see a lot of movement towards privacy seal programs—but not everyone is there yet. And a lot of people then think, oh, there must be some kind of market failure. But what if the initial assumption isn't true? What if the data we have on what consumers want, which we get from prompting them in a survey, is not that reliable?

These are the questions we should be asking, especially when we look out at the world and see electronic commerce taking off. Especially when there seems to be no reason in principle, looking at the economics of the matter, for entrepreneurs to perversely ignore any aspect of consumer demand. Given the benefits that consumers have gotten from high-tech businesses in the last decade, the vast diversification of markets in response to a million variations on customer tastes, the view that business would not respond to privacy preferences is an extraordinarily bizarre view. If they are not responding across the board, maybe its because demand isn't strong across the board.

PRIVACY: REVIEWING EMPIRICAL EVIDENCE ON PRIVACY

We ought to look more closely at the type of evidence being collected and considered in the privacy debate. Frankly, the empirical work done so far has been dazzlingly shallow.

A good bit of that information comes from self-reported data on surveys, from asking consumers "do you care about privacy?" Now, who would say "no" in answer to this question? Is the respondent distinguishing privacy from security issues? From spam? Even if they are, talk is cheap. Real preferences are revealed by consumer's actions, when they must consider the time and cost of actually obtaining what the survey offers them for free. Self-reporting is simply not that reliable—try wandering around among some of the tourists assembled in the mall for the Fourth of July and ask them if their kids are smarter or dumber than average. As Chet Thompson of Prodigy once noted, "Market surveys told Prodigy that people wanted to do their grocery shopping by computer. They didn't."

Here are some other studies that ought to be performed in order to better judge the impact on consumers of federal privacy standards:

- A study of whether businesses that have not posted privacy policies have experienced similar rates of growth to those who have.
- A study of the impact on small business and startups of top-down privacy regulation.
- A study of how businesses, especially startups, use information to enter new markets & to develop new products.
- A study of the cost saving obtained by doing targeted rather than direct marketing.
- A study, not of the number of sites that post privacy policies in absolute terms—but of the number of sites that post such polices as compared to the number that posted such policies a year ago, a year and a half ago, 2 years ago. What is the rate of increase?

What all these studies have in common is that they all reflect actual behaviors and costs, not hypothetical preferences. (One caveat; in emphasizing these holes in our understanding I do not mean to imply that an empirical finding, for example, that consumers really do want privacy, would justify regulation—the conflict in principle between privacy and the free flow of information is still inescapable, as is the need for evidence of market failure).

Imagine if Congress to address the question of cable rate deregulation simply by directing the FCC to ask consumers if they would prefer lower cable prices. Clearly, that would be disastrous. Yet we see some policymakers cheerfully considering privacy regulation for electronic commerce largely on the basis of survey data, as if regulating the Internet is a casual thing, like tossing off a Christmas mailing.

JUDGING SELF-REGULATION

I will leave it to other presenters to present figures about how the use of privacy seal programs has grown, and to describe those programs. I am going to talk about how to assess these programs. It's important to start with realistic expectations.

What should the goals of self-regulation be?

The goals of a system of self-regulation should be evolve over time in the marketplace. One characteristic of demands made on e-commerce merchants respecting privacy "self-regulation" has been that the goals of the regulation are assumed to be known. Regulators have insisted that a system of self-regulation must ensure that customers have notice of how their data is being used, that they have a choice about whether it is not be collected or not, and so on.

In the real world, however, no one really knows what state of affairs "ought" to obtain with respect to privacy. *The question of when human beings will need to reveal information to gain trust, will be willing to offer trust without information, and will need to respect confidentiality to gain trust is a bafflingly complex question.*

The goals of systems of self-regulation will evolve and change over time, and will vary widely across the e-commerce marketplace. Entrepreneurs will make informed guesses about privacy policies to allay their customer's fears (if any) of doing business online. Some entrepreneurs will get it wrong, and lose ground; others will get it right, succeed, and be imitated by late-comers. But entrepreneurs must be permitted to take their cues from the results of engaging in the marketplace, not from top-down commands.

How long should self-regulation take?

What is a market? A market is a device for processing information. The economist Bastiat once commented that it is a miracle that Paris got fed every morning. For that to happen, Parisians' diverse tastes in breakfast foods must somehow become known to myriad bakers, café's, butchers, and grocers. Parisian consumers must obtain the knowledge that bread is available at the bakery, not at the tailors. The local needs of bakers and grocers must somehow become known to farmers and middlemen scattered around the countryside. *Through the price system and other mechanisms, markets harness local knowledge and subjective tastes, setting in motion a process that results in the populace of Paris' being fed—all without any central planning or direction.* This is extraordinary. Indeed, as we learn from our experience with communist economies (as economists Ludwig Von Mises and F.A. Hayek predicted decades ago), central planning cannot begin to coordinate the distribution of resources as effectively as the chaotic, decentralized market.

Understanding that a market is a bottom-up learning process helps us to expect that establishing systems of self-regulation will longer than a year, two years, or three years. The embryonic privacy seals programs we see now will ultimately be supplemented by gated "safe" communities online (such as AOL and E-bay), and intelligent "bots" and infomediaries to guide consumers through, and other technological and business innovations. The process will never really end.

What if not everyone participates?

FTC Commissioner Orson Swindle pointed out recently that the goalposts for privacy regulation are moving. A year ago, the concern was we would not have thriving e-commerce if we don't solve the privacy problem. Well, electronic commerce took off, and there's a lot of progress with the privacy problem. So the wording has changed. Now, we can hear that e-commerce will never rise to it's *full* potential, because the market hasn't moved fast enough. Maybe the idea is that if the trained seal balances the ball on his nose the first time, we'll just keep adding balls and sooner or later they'll fall off and then we'll call that a market failure.

Given the vast numbers of start-ups, wild experiments, and small businesses that will be the next generation of pioneers in e-commerce, it would be unlikely that all of them will automatically concede the importance of having a privacy seal on their sites, unless and until they see significant indication of customer demand for it. Perhaps some sites that participate will have some sinister purpose in mind, but most of them will simply be ordinary businesses who simply don't share the vision of a privacy imperative. A lot of them will be noncommercial, amateur sites, or sites that are borderline commercial or noncommercial.

It would be a grave mistake to assume that because a business doesn't have a seal or post a notice, it ought to become a target of regulation. Lacking a privacy policy simply isn't even close to being evidence that that site poses a danger to consumers, in any real sense. Treating these sites as legitimate enforcement targets would be wrong, and deeply insulting to hundreds of honest entrepreneurs. And it creates some serious practical problems, too. Enforcement efforts will be far, far more effective if they can be targeted against actual perpetrators of identity theft, fraud, and so on. Requiring enforcers to disperse their focus to hundreds of sites simply because those sites don't have a seal would be an incredible waste of time.

What about bad actors? Sites that actually do perpetrate fraud or scams of some sort? There are many laws already against fraud and deceptive practices.

Self-regulation that arises as a natural outgrowth of consumer demand is truly voluntary and decentralized. Kosher food labels are a good example, offering consumers a choice of many different standards—*or none at all.* But for many quality and customer service issues, no third party standards or oversight at all are necessary for "self-regulation." That is, *true market-based self-regulation blurs into no regulation at all, with each company "regulating" itself according to internal standards of customer or client service and no third party oversight.* Bad service is checked by competition.

Ultimately, we might see nearly as many different privacy policies as there are e-commerce companies. A system of privacy "self-regulation" imposed uniformly on the market might well tend to collapse over time (rather as the Comics Code has) in any sector where there is little consumer demand for confidentiality. In some cases, no third-party rating systems would be able to capture the extraordinary variety of patterns of customer preferences that emerge.

CONCLUSION: WHAT IS MINIMAL REGULATION?

Given the flurry of concern about privacy, even legislators and businesses worried about the impact on electronic commerce are almost ready to concede the need for "minimal regulation"—just requiring sites to post their policies, that's all. But from my standpoint that's too radical a step, both unnecessary and not well informed. What kind of enforcement mechanism would we create? Do we really want to penalize the honest owner of a 50 year-old hardware store in Peoria because he put up his web site without a privacy notice? Why should enforcement resources be devoted to this? For once, the Cato Institute's position isn't the radical one. Things are working fine as they are; leave the Internet alone.

Mr. TAUZIN. Thank you, Ms. Singleton.

Next will be Mr. Steve Lucas, Chief Information Officer for PrivaSeek.

Steve.

STATEMENT OF STEVEN LUCAS

Mr. LUCAS. Thank you, Chairman Tauzin and members of the subcommittee. I would like to thank you for inviting me here today to share my views on the issue of online privacy. Again, my name is Dr. Steven Lucas. I am the Senior Vice President of PrivaSeek. We are a Colorado-based Internet company that was founded in late 1998. As you know, the issues of consumer privacy both online and off-line have received a tremendous amount of attention. We commend Congress, and the subcommittee in particular, for directing attention to this issue.

In the 1890's, Supreme Court Justice Louis Brandeis defined privacy as the right to be left alone. A century later and a new millennium upon us has brought us fully into a new digital economy that is driven by information as one of the principal means of the creation of wealth. What now seriously addresses the concept of privacy is the right to control personal information as an inherent property right of the person. This argument and the resulting actions to recognize this right are critical to individual prosperity in a democratic society.

About a year ago, I think that no one would deny that the state of online privacy practices was, at best, marginal. I think that few would deny that since that time industry has made substantial progress in terms of its efforts to improve the state of consumer privacy protection. Privacy organizations like TRUSTe have successfully recruited online companies. They have participated in seal programs. They have launched Web-based consumer education programs aimed at providing consumer education about privacy rights and also the data collection practices of the sites that they visit. So trade associations, as mentioned, have also announced codes of fair information practices.

Recent survey results also bear out the fact that a growing proportion of the online industry are posting privacy practices. We were proud to be a sponsor of the Georgetown Privacy Policy Survey. This survey did demonstrate, although the results were not what we would hope, that there has been some improvement in this area. I think the proliferation of Web site privacy statements over the past year signifies that online companies are realizing the need for, as well as the initial benefits derived from ensuring that consumer privacy information is protected in the online environment.

While this is all great progress, I think what we really need to do is ask ourselves the question of where do we go from here. I think it is critical that further action be taken by industry to ensure that privacy policies are comprehensive, that they meet all of the fair information requirements. The focus of my testimony today is going to be on a nonregulatory solution to promoting privacy protection for online consumers.

Currently, many companies, including PrivaSeek, are developing new technologies that are capable of ensuring privacy protection for online information. Like PrivaSeek, these companies believe that technological solutions provide the most effective, efficient, and safest means of protecting intensive online data without unnecessarily hindering the growth of the electronic marketplace or the ability of consumers to control and gain value from their privacy practices.

PrivaSeek is the first "consumer infomediary" dedicated to establishing a new global consumer-centric marketplace that is based on principles that consumers establish the rules for the collection and use of their information. As PrivaSeek's first major initiative in March of this year, we announced our "Persona" technology. After several months of testing, I am pleased to announce that yesterday we released the first commercial version of our Persona product called Persona Valet.

Persona acts as a negotiator of information between the consumer and the marketplace. It is based on the fundamental notion that individuals own their personal information and should be in control of it online. This includes the ability to track the use of their information and to control under what circumstances information is shared with sites that request it.

When consumers visit PrivaSeek's site, no information is collected from them. If they choose to be a PrivaSeek member, they can then create an online Persona which includes information like

their name, their address and a preferred way that PrivaSeek can contact them.

They can then decide to provide additional information such as e-mail address, phone numbers, interests and hobbies, electronic commerce information such as credit card information and shipping addresses.

Then consumers are asked to define their personal use preferences for all of the information that they provide us. By setting their own preferences, they control the information that is provided and under what circumstances the information can be shared with PrivaSeek-approved partners. Consumer information is never disclosed to anyone without prior consent. Additionally, consumers can change their personalized set of privacy preferences at any time by accessing their account and changing the conditions that govern how PrivaSeek will manage their data. At the end of the day, though, it is the consumer who chooses how personal information is utilized.

We also provide consumers with a tool that allows them to automatically complete forms that may be necessary to complete e-commerce transactions or to complete forms that may be required for services and registration on the Web.

Since we were also created to assist consumers in keeping their personal information secure, security is naturally one of the company's primary concerns. We rely on state-of-the-art technology at all points of information collection, transmission, and storage to ensure that the security and the integrity of the consumer's data is never compromised. Additionally, the information is stored in what we call the "Persona WebVault" which is maintained in a facility with a long history of being able to manage sensitive information with audited data and physical security practices available.

Privacy partners go through a very rigorous approval process that includes a comprehensive privacy policy assessment. If an organization is approved, it has to sign a contract with PrivaSeek requiring the organization to abide by the information controls established by the consumer in their Persona. Under this contract, the company agrees to follow the consumer's specific instructions with regard to the information. For example, if the consumer doesn't want the information to be used for internal marketing purposes, that information is never transferred nor can the site use it.

In the event that the organization violates that contract in any way, we will immediately remove them as a PrivaSeek certified partner and we will immediately take legal action against the company.

The Persona technology enables the consumer to automatically safeguard their personal information and their identity on the Web. It also allows them to gain value from it. It allows consumers to access their data and privacy preferences from any device that is connect to the Web.

In light of the emergence of viable and innovative technological solutions, as well as the increasing adherence of Web sites to self-regulatory programs, we believe that a legislative mandate governing privacy protection would be premature at this time. Considerable time and effort and resources have been devoted to the development of new technologies designed to safeguard consumer data

in terms of privacy and products, as well as tools like the certificates and certification technology.

Just as Congress and the FTC have provided a grace period for online companies to demonstrate their commitment to widely accepted information practices, so too should these technologies be provided with an opportunity for the deployment, recognition and trust of both consumers and the online marketplace, the technologies that go a long way to building an environment conducive to the recognition of the right to privacy.

We believe that the work by PrivaSeek and organizations like the World Wide Web consortium and their P3P effort are also important. However, it is also our view that a new system of laws and governance may be needed to help the transition by building a legal framework that recognizes these rights.

We consider ourselves a new intermediary, but at the same time we also have to consider that the government may have to assume the role as the ultimate consumer intermediary through its use of regulatory authority and by working with industry to create an environment that is based on the critical vision of our future society.

Again, we thank you for the opportunity to appear today and we look forward to working with you and members of the committee in the future.

[The prepared statement of Steven Lucas follows:]

PREPARED STATEMENT OF DR. STEVEN LUCAS, SENIOR VICE PRESIDENT, INDUSTRY GOVERNMENT RELATIONS & CHIEF INFORMATION OFFICER, PRIVASEEK, INC.

Chairman Tauzin and Members of the Subcommittee, I would like to thank you for inviting me here today to share my views on the issue of online privacy. My name is Steve Lucas, and I am the Chief Information Officer and Senior Vice President of Industry Government Relations at PrivaSeek. Headquartered just outside of Denver, Colorado, PrivaSeek is an Internet start-up founded in late 1998.

As you know, the issue of consumer privacy—both online and offline—has received a tremendous amount of attention over the past year. PrivaSeek commends Congress, and this Subcommittee in particular, for directing its attention to this increasingly important issue.

One year ago, the state of online privacy practices was by most accounts marginal. The Federal Trade Commission's ("FTC") 1998 "March Sweeps" of 1,400 Web sites revealed that only 14% of sites had privacy policies posted on the site that contained information concerning what information was collected and how it was used. Proponents of government regulation of online privacy practices saw the results as clear evidence of the need for comprehensive legislation, while critics argued that the survey results were inaccurate and/or inconclusive at best. Regardless of the particular pundit's perspective, the net effect was an overwhelming impression that industry was doing a less than acceptable job of protecting online consumer data.

I think that few would deny that, since that time, industry has made significant strides in terms of its efforts to improve the state of consumer privacy protection online. Privacy organizations such as TRUSTe have not only successfully recruited online companies to participate in their rigorous and resource-intensive online "seal" programs, but also have launched Web-based consumer education programs aimed at heightening Internet users' awareness of their own privacy rights, as well as appropriate data collection practices of Web sites that they visit. Also, several trade associations have instituted codes of conduct governing fair information practices, and, at the same time, many individual Web sites are voluntarily posting privacy statements.

Recent survey results also bear out the fact that a growing portion of the online industry recognizes the importance of embracing responsible privacy practices. Privaseek was proud to be one of the sponsors of the Georgetown University Internet Privacy Policy Survey that was conducted at the request of the FTC. This survey was released in June of this year and revealed a dramatic rise in the number of Web sites posting comprehensive privacy statements. Specifically, of the sample drawn from the 7,500 most popular sites, more than 65% had posted privacy poli-

cies. Additionally, of the 100 most popular sites surveyed, 94% contained privacy disclosures. The proliferation of Web site privacy statements over the past year signifies that online companies are realizing both the need for, as well as the mutual benefits derived from, ensuring that consumer privacy information is protected in the online environment.

While all of this is in fact great progress, the question before us today is where do we go from here? It is critical that further action be taken by industry to ensure that privacy policies are comprehensive, meeting all of the tenets of fair information practices. There are six key elements to this action. First, sites should provide notice of their information practices, including what information they collect from consumers and how they use it. Second, they should also offer consumers choices as to how the information is used, and seek consent for the intended uses. Third, sites should not disclose personally identifiable information about consumers to third parties without consumers' consent. Fourth, sites should offer consumers access to the information collected about them and an opportunity to correct inaccuracies. Fifth and sixth, sites should contain information about their security measures and consumer recourse options. All of this information should be easy to find and easy for the consumer to understand.

As was demonstrated last summer in the *GeoCities* case,[1] as well as more recently in the *Liberty Financial* matter,[2] the FTC currently has the tools necessary to take action against companies that may violate consumers' online privacy. Thus, widely adopted self-regulatory programs, operating in conjunction with the FTC's existing Section 5 enforcement authority, provide effective mechanisms to ensure the protection of personal data online. And, they ultimately deliver benefits for both businesses and consumers in the evolving digital economy.

The focus of my testimony today is on another non-regulatory option for promoting privacy protection for online consumers. Currently, many companies, including PrivaSeek, are developing new technologies that are capable of ensuring privacy protection for online information. Like PrivaSeek, these companies believe that technological solutions provide the most effective, efficient, and safest means of protecting sensitive online data without unnecessarily hindering either the growth of the electronic marketplace or the ability of consumers to control and gain value from their privacy preferences.

PrivaSeek is the first "consumer infomediary" dedicated to establishing a new global consumer-centric marketplace based on principles where consumers establish the rules for the collection and use of their information. As PrivaSeek's first major initiative, in March of this year, we announced our "Persona" technology. After several months of testing, we are pleased to announce that yesterday, we released the first commercial version of the Persona product, called Persona Valet.

Persona acts as a negotiator of information between the individual consumer and the marketer's Web site. Persona is premised on the fundamental notion that individual consumers own their personal information and should be in control of it online. This includes the ability to track the use of their information and to control under what circumstances information is shared with sites that request it.

When consumers visit the PrivaSeek Web site, no information is collected from them. If they choose to become a PrivaSeek member, they then create an online "Persona" which includes information such as their name, address, and the preferred method for PrivaSeek to contact them. This limited information is used to create the user's Persona Account.

The consumer may decide to provide additional information such as email address, phone numbers, interests and hobbies, and electronic commerce information such as credit card numbers and shipping addresses.

Consumers are also asked to establish their personalized set of usages for their information. By setting their own preferences, they control what information is provided and under what circumstances the information may be shared with PrivaSeek-approved partners. A consumer's information is never disclosed to anyone without prior consent. Additionally, consumers can change their personalized set of privacy preferences at any time by accessing their account and making changes to the conditions that govern how PrivaSeek will manage their data. At the end of the day, it is the consumer who chooses how personal information is utilized.

Persona Valet provides consumers with a useful tool for accomplishing routine tasks like shopping online and managing personal information on the Internet. When consumers surf or shop the Web, Valet automatically saves them time and effort by automatically completing forms that may be required to register for a service or make a purchase.

---

[1] *In the Matter of Geocities*, FTC. File No. 9823015.
[2] *In the Matter of Liberty Financial Companies*, FTC File No. 9823522.

Since PrivaSeek was created to assist consumers in keeping their personal information private, security is naturally one of the company's primary concerns. PrivaSeek relies on state-of-the-art technology at all points of information collection, transmission, and storage to ensure that the security and integrity of consumers' information is not compromised. By virtue of a digitally encrypted secret password and network firewalls that prevent unauthorized access to a consumer's individual profile, the consumer has exclusive access to information in their Persona. Additionally, the information is stored in the "Persona WebVault," which is maintained at a facility with a long history of safeguarding sensitive information with audited data and physical security practices.

PrivaSeek partners, including online merchants and content vendors, go through a rigorous approval process that includes a comprehensive privacy assessment by a team of third party privacy experts. If an organization is approved, it must sign a contract with PrivaSeek requiring the organization to abide by the information controls specified in the consumer's Persona. Under this contract, the company agrees to follow the consumer's specific instructions with regard to this information. If a consumer does not wish to have the information used for internal marketing purposes, the merchant may not use that information without violating the contract. If the organization in any way violates its contract with PrivaSeek, it will be dropped immediately as a PrivaSeek-approved partner, and PrivaSeek will take legal action against the company.

Thus, the Persona technology not only enables consumers to automatically safeguard their personal information and identity on the Web, but to actually gain value from it. It also saves consumers precious time and effort by keeping track of passwords and purchases and by automatically entering a consumer's personal information in online forms. The Persona technology provides a secure method of storing data that can easily be audited by a third party. It also allows consumers to access their data and privacy preferences from any device that is connected to the Web.

In light of the emergence of viable and innovative technological solutions, as well as the increasing adherence by Web sites to self-regulatory programs, PrivaSeek believes that a legislative mandate governing online privacy protection would be premature at this time. Considerable time, effort, and resources have been devoted to the development of new technologies designed to safeguard consumer data, both in terms of privacy enhancing products, as well as certification tools such as digital authentication technology. Just as Congress and the FTC have provided a grace period for online companies to demonstrate their commitment to widely accepted fair information practices, so, too, should these promising technologies be afforded an adequate opportunity for deployment, recognition, trust, and use both by consumers and the online marketplace.

Again, thank you for the opportunity to appear before you today. We look forward to working with you in the future and serving as a resource to Members and staff of this Subcommittee, as well as to all members of the House of Representatives.

Mr. TAUZIN. Thank you, Mr. Lucas.

Finally, Mr. Jerry Cerasale, Senior VP for Government Affairs, Direct marketing association here in Washington, DC.

Jerry.

STATEMENT OF JERRY CERASALE

Mr. CERASALE. Thank you, Mr. Chairman. It is a pleasure to be back here again.

Specifically, I would like to direct you and your staff to page 8 of my testimony and you can find the Web address of the DMA's privacy policy generator, you can answer a few questions, and you can get a privacy policy all printed out for you and put it on your Web site.

Mr. TAUZIN. I may just call upon you.

Mr. CERASALE. As you know, the DMA represents over 4,500 companies in the United States and in 54 foreign countries. So these companies have a vital interest in commerce over the Internet both in the United States and globally.

I would like to just quote one thing from my testimony. It is the DMA's privacy principles and guidance for marketing online. "All

marketers operating online sites, whether or not they collect personal information from individuals, should make available their information practices to consumers in a prominent place. Marketers sharing personal information that is collected online should furnish individuals with an opportunity to prohibit the disclosure of such information."

I think that is where the DMA is right at the moment in moving forward. We are pleased with the results of the Georgetown study. We are not ecstatic, but it is a lot better than it was a year ago. I can have a little bit bigger smile on my face this year than last year.

We still have a long way to go, but in response to Mr. Boucher's statements about his idea of notice and opt-out, and how pervasive it is and where it hits, the Georgetown study of the top 100 sites showed that 94 percent had notice and 83 percent had notice and personal choice. Those 400 sites represent 94 percent of all the hits on the Internet. So if you—if you multiply 94 percent times 83 percent you get 80 percent of their hits on the Internet were at sites that gave notice of what they do with information and some personal choice to the individual. That is not 100 percent, but it is a long ways toward going there from the 14 percent that we had a year ago.

We think at the DMA that the keys are notice and choice for the individuals. Security, one of the major items in the principles that the FTC has stated, is an important factor for all businesses that are working online. As we see from these viruses that come floating through, it is important for businesses to have significant security in their systems to try to protect their own business systems. So that is an important factor. It is true that any business site that is doing any sales on the Internet must collect personal information. You either have to—if you are selling information that you can distribute online, you have to have an e-mail address. There has to be some means for getting payment or you have to have some physical address from which to send the product.

So it is important for all marketers to have a policy up and give some personal choice. That is what we are working toward, which is why at the beginning of this month we started a Privacy Promise in which all members of the DMA must give notice of what they do and the opportunity to opt out no matter what medium that is used for marketing or else they will be losing their membership in the DMA. Staff is now working to examine that and preparing cases for a board meeting in October of this year as we move forward, and we will make that public.

I again appreciate the opportunity to be here. I will answer any questions. Thank you very much.

[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 online privacy. I am Jerry Cerasale, Senior Vice President of Government Affairs for The Direct Marketing Association, Inc. ("The DMA"). The DMA's vast membership includes the leaders of the current economic explosion of the Internet and electronic commerce. For this reason, The DMA has

been working diligently to encourage development of a global medium that continues to flourish and provides our customers with the best possible experience in their Internet transactions.

Last year I testified before this subcommittee and urged that Congress continue to create space to allow time for self-regulation develop. I am pleased to report that this self-regulatory framework has developed significantly since that hearing. Mr. Chairman, based on our extensive experience in this area, The DMA is convinced that self-regulation and technological innovations are the most effective methods for establishing privacy protection in the borderless world of the Internet, and must continue to be the cornerstone of any domestic or global approach for ensuring privacy online.

As demonstrated by the May Georgetown Internet Privacy Policy Survey ("Georgetown study"), significant progress has been made since the survey the Federal Trade Commission conducted on online privacy last year. This progress is particularly encouraging given the multitude of new self-regulatory programs that continue to be developed and implemented. Industry self-regulatory principles, consumer choice technologies, and an extensive educational campaign are creating a privacy regime that is both flexible and effective—requirements for the Information Age.

There are three main topics I wish to focus on in my testimony today that I believe will put into perspective the state of online privacy today. First, I will discuss in more detail the results of the Georgetown study. Second, I will briefly describe the principles that The DMA believes are essential to protecting privacy online. Finally, I will describe several of the ongoing efforts that the DMA is engaged in to empower consumers.

II. PROGRESS FROM INDUSTRY SELF-REGULATORY EFFORTS IS SIGNIFICANT AND CONTRIBUTES TO THE GROWTH OF ELECTRONIC COMMERCE

A. The Growth of Electronic Commerce is Extraordinary

One of the reasons often cited for the importance of protecting privacy on the Internet is that unless individuals are protected on the Internet, they will be hesitant to embrace electronic commerce. All evidence continues to indicate that consumers are comfortable engaging in transactions on the Internet, as electronic commerce continues to grow at an unprecedented rate. The personalization and interactivity unique to the Internet provide an attractive forum for individuals to engage in commercial transactions.

For DMA members, the main use of information collected over the Internet is for marketing purposes. For example, a site may remember that I purchased a particular product there previously and direct me to the same section of its online store. This type of personalization is one of the unique attributes of the Internet. Any "harm" associated with the collection and use of information in such contexts is minimal, and outweighed by the beneficial uses of the information, such as improving the visitor's experience at the site through personalization. The DMA believes that the Congress should be particularly hesitant to enact laws that may disrupt the exponential growth of the Internet.

The Department of Commerce's The Emerging Digital Economy II released in June states that from 1998 to 1999 the number of web users world-wide increased by 55 percent. In early 1998 it was estimated that Internet retailing might reach $7 billion by 2000. Actual estimates for 1998 alone range from $7 billion and $15 billion, far exceeding all expectations, with forecasts now projected to be $40 billion to $80 billion by 2002. We anticipate that these numbers will continue to grow.

B. The Georgetown Internet Privacy Policy Survey indicates that vast improvement in the privacy practices of Internet companies is occurring.

The Georgetown study indicates that privacy self-regulation on the Internet is working. No longer are the discussions surrounding Internet privacy focused on whether self-regulation provides an appropriate framework for protecting privacy online, rather the discussions are now focusing on the details of the policies, such as the breadth and content of the notices.

The significant improvement shown in the Georgetown study is a result of the hard work of The DMA, the Online Privacy Alliance (of which The DMA is a member), BBBOnLine, TRUSTe and others. The study shows that 94 percent of the top 100 web sites have posted a privacy policy notice or an information practices statement. When considered in light of the fact that 98 percent of all Internet users visit the more popular sites, it is clear that meaningful and effective privacy practices do already exist online for consumers. Moreover, there has been a significant increase in the number of policies posted in the past year. In fact, close to 66 percent

of all sites now post privacy policies, up from 14 percent in last year's Federal Trade Commission survey.

To be certain, this is just the beginning. Although the Georgetown study indicates significant progress in the number of privacy policies on web sites, there is still room for improvement. The study showed that most of the sites surveyed do not yet include all of the elements set out in the Online Privacy Alliance principles. This is understandable because some of the seal programs are just recently, after much development, beginning to accept applicants to their programs. We expect that as companies participate in and implement these seal programs, the quality and content of the notices will improve.

III. THE DMA'S PRIVACY PRINCIPLES AND GUIDANCE FOR MARKETING ONLINE

A. Privacy Principles and Guidance for Marketing Online

While The DMA recognizes that that there is still work to be done to educate companies as to the principles that should be included in privacy policies, we are very encouraged by the result in the Georgetown study indicating that 93.5 percent of the top 100 sites that collect information and post a privacy disclosure provide notice, with 83 percent of these sites providing privacy choices for consumers. The DMA believes that notice and choice are the most significant principles for online privacy protection as together they empower consumers to determine the uses of their information.

The DMA has developed *Privacy Principles and Guidance for Marketing Online* in order to explain and highlight the issues unique to online and Internet marketing. The primary feature of these guidelines is notice and opt-out.

> *"All marketers operating online sites, whether or not they collect personal information from individuals, should make available their information practices to consumers in a prominent place. Marketers sharing personal information that is collected online should furnish individuals with an opportunity to prohibit the disclosure of such information."*

On July 1, The DMA's Privacy Promise went into effect. It requires all members, as a condition of membership, to provide their customers with notice and the ability to opt out of the use of customer information for marketing purposes. The Privacy Promise includes the provision of notice and opt-out on the Internet set out in the Marketing Online Principles to which I just referred.

I also would like to mention that last fall The DMA supported the passage of the Children's Online Privacy Protection Act. The DMA supported this legislation because we believe that young children present a special case. Unlike adults, children may not fully understand choices regarding privacy. Based in part on existing guidelines developed and followed by The DMA, this legislation contains strong protections for children, prohibiting the collection or distribution of personally identifiable information from children under 13 without prior parental consent or direct parental notification. The DMA is currently working with the Federal Trade Commission as it develops regulations to implement this Act.

B. Enforcement of Online Privacy Protections

The DMA has been at the forefront of enforcing effective, responsible self-regulatory codes governing the uses and transfer of information by the direct marketing industry for many years, long before the growth of the Internet. As a result of its extensive membership, The DMA has enjoyed great success obtaining broad compliance with its various codes and guidelines. The cornerstone of the industry's self-regulatory codes is The DMA's *Guidelines for Ethical Business Practice.* These guidelines apply to marketing in all media including the Internet.

Through its Committee on Ethical Business Practice, a peer-review program, The DMA responds to cases of alleged Guideline violations brought to its attention by an array of sources—business, consumers, public officials, and the media. This peer-review process is effective. Most cases are resolved through cooperation with the Committee and its recommendations. Members that do not resolve complaints cooperatively are also subject to review by The DMA Ethics Policy Committee with the potential for suspension, expulsion, or censure.

The DMA has initiated a process which reveals all cases and their resolution. Furthermore, where the subject company has not committed to follow guidelines after review, its name is publicly disclosed. In instances where violations of law are also found, the Committee refers matters to the appropriate law enforcement agencies.

Moreover, privacy principles adopted by individual companies and held out to the public also are subject to enforcement by the FTC and state attorneys general. By publicly posting policies as required by the Privacy Promise and consistent with criteria set out in the OPA guidelines, companies become subject to deceptive practices

enforcement actions under existing federal and state consumer protection law if they do not comply with their stated policies. Thus, this self-regulatory framework is far more than a system of voluntary compliance.

IV. THE DMA AND OTHERS CONTINUE TO DEVELOP AND IMPLEMENT SELF-REGULATORY REGIMES THAT EMPOWER CONSUMERS REGARDING ONLINE PRIVACY

A. The E-mail Preference Service

The DMA will soon launch an e-mail preference service that will allow individuals to remove their e-mail addresses from marketing lists in a manner similar to The DMA's long standing telephone and mail preference services. This ambitious undertaking is aimed at empowering consumers to control unsolicited commercial e-mail, while creating room for the many societal benefits of legitimate marketing in the interactive economy. Once this e-mail preference service is up and running, participation in it also will be a requirement of DMA membership.

B. Public Education

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 educating consumers about the process. Through education, individuals will better understand the potential benefits of interactivity, as well as the choices they have to control information that they submit. Therefore, The DMA has developed a Web page devoted to privacy and launched its Privacy Action Now initiative.

The DMA has 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.

C. Technology Solutions

In light of the unique characteristics of the Internet, technology will play an 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, indeed helping to develop and promote, such software. Under this approach, it will be the individual users, rather than industry or the government, who will determine the uses of their personal information.

Over the past two years, The DMA has been involved in an initiative that supports this concept, the Platform for Privacy Principles or P3P. This initiative, undertaken by the World Wide Web Consortium, is developing 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 are working 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.

The DMA also has created and made available from its Web site a technical tool that allows companies to create and post effective privacy policies. This Privacy Policy Generator (http://www.the-dma.org/policy.html) enables companies 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 have sent policies to The DMA for review.

V. CONCLUSION

The DMA believes that self-regulation is the most effective means of protecting privacy on the Internet. The Georgetown study indicates that significant progress has been made and the self-regulatory framework is working. The DMA realizes that this is only the beginning. We continue to explore and develop innovative approaches to protecting privacy on this extraordinary medium. The approach that we are taking is allowing electronic commerce to flourish, while at the same time enabling the development of a privacy regime that is flexible for the information age.

We congratulate the Chairman for his continued interest in the exploration of these issues, and look forward to working with the Subcommittee.

Mr. TAUZIN. Thank you very much. The Chair recognizes himself for a round of questions.

First, let me point out that the issues that are raised in the Information Age on the one hand have some parallel in the Brick and Mortar Age. You sort of made the case, Ms. Mulligan. Today when we go to grocery stores and banks, the camera is monitoring us. Those cameras can watch us browsing through the store. And I assume someone sitting back in the back room with a monitor can keep records, if they want to, on what shelves we stop at and what activities we engage in in those stores. There are no notices on the bank doors or the store doors saying, you will be monitored while you are inside. There is no notice on the walls of these halls in the Rayburn Building that there are cameras all over the place. I assume somewhere in the Capitol Police offices there are monitors where Capitol Police can monitor your movements in this building and perhaps even microphones that can pick up conversations. I am not sure. It would be interesting to find out.

When you fill out a mail order form you are sending all kinds of information into the mail order world. When you fill out—how many questionnaires have you filled out this year? I have filled out a bunch already. I will fill out a lot more before the year is over.

How many reports do we file every year, Mr. Markey, detailing personal information? One of the witnesses on the last panel is married to a former Member of the Congress. I assume a lot of that information she is concerned about being in the public domain was obtained from public records because her husband had to file it as a Member of Congress.

In the real world, there is a lot of information going out, a lot of monitoring and a lot of things happening without notice to consumers, without the right to opt out. So the questions that are posed online have a parallel in the real world.

What is interesting is the difference here. The difference is the enormous power of the Internet to gather that information. I think Chairman Pitofsky put his finger on it when he said that the Internet has the power now to detail what we are thinking about doing, not just what we are doing, in much larger ways and to create a profile of behavior, our thoughts, even now. Not just our preference, but what we might consider preferring. Quite a different ball game for consumers to have to walk into. You put your finger on it again, Ms. Mulligan. If you and I had to, every time we used cash, to fill out a questionnaire about our preferences, talk about what we looked at buying or thought about buying before we paid cash, and somebody had a big information portfolio on our family and our purchasing history, we would be less likely to go shopping at a store that required all of that.

Do any of you know what percentage of transactions, financial transactions, in America are done with cash today?

Ms. MULLIGAN. There are some statistics. I think Alan Greenspan——

Mr. TAUZIN. The number I had was 2 percent.

Ms. MULLIGAN. It is 2 percent of the value, but actually many of the actual transactions—meaning large purchases, of course,

tend to be made with credit cards. But the actual number of transactions, a quarter into the telephone, the 35 cents into the telephone, the quarter into the newspaper vending machine——

Mr. TAUZIN. The number of transactions is a lot higher. But in value, I think it is about 2 percent when you consider all of the mortgages, the checks, the credit cards, all of the forms of secured transactions we engage in. Two percent is cash. That is a lot that is being done in a recorded way somewhere, some kind of transaction. The point I am making is there are parallels and yet there are big differences in the Information Age.

The second point a number of you made—Ms. Singleton, you pointed it out and, Mr. Cerasale, you made it, too—this is an Information Age. The basis of the argument is the capacity of the Information Age to function. Be careful how we balance the so-called private rights to information and the private property right and the capacity of an Information Age to function with our information. We all jealously guard our private information, so it is a delicate cut. How can we set it up in a commercial world where it works to the consumer's satisfaction and yet still works? It is a good one.

Ms. Singleton, you raised the question. Do we look at actual experience and learn from it or just assume? And there are some good things here.

I wanted to ask you—before I do that, Mr. Lucas, you gave us a good example of a technology your company is developing that I can use, as a consumer going online, to protect my personal information. You are not the only one. There are other company doing that, right?

Mr. LUCAS. That is correct.

Mr. TAUZIN. Doesn't Novell have a similar software product? And I assume other companies do, too, that I can't think of right now.

Mr. LUCAS. There are other companies that have started——

Mr. TAUZIN. Your point is, lots of companies are building software products that I can eventually purchase and use in connection with seals and partnerships to know that I am in control of my information online; is that correct?

Mr. LUCAS. There are several companies——

Mr. TAUZIN. And your point is, they ought to be given a chance to see whether consumers like them or want them; or in a real world, Ms. Singleton, I believe they are important enough to invest in and to use on the Internet, right?

Mr. LUCAS. That is correct.

Mr. TAUZIN. Mr. Lewin, you testified that your numbers are growing in TRUSTe in terms of companies signing up. You said about 1,500. What percent of transactions, how much traffic is involved in the companies that you are engaged in?

Mr. LEWIN. Right. By using a survey conducted by Media Metrics, which is a recognized industry to "keep track of the number of hits," if you will, at each of the sites, it is estimated that during the course of a month that the sites that carry the TRUSTe seal, about 90 percent of the users hit a TRUSTe-sealed site each month.

Mr. TAUZIN. So it is significant. You have got your seal program going, you have got your marketing enforcement. Are you going to be part of our direct marketing group? You have got to obey these

rules; if you don't, I will kick you out. I assume that you kick people out or sue them in court on your contracts if they violate, right?

Mr. LEWIN. We have those options. Fortunately, to date, everybody has recognized the value and we have not had to do that.

Mr. TAUZIN. The Better Business Bureau has its own seal. I saw a whole list of other seals in the commission's report.

Here is my question. How do I know which one of these seals and which one of these operations I can trust? TRUSTe sounds like I can trust it, but how do I know? The Better Business Bureau has a reputation; I assume I can rely on that to some degree. But how do I know which one of these is going to be not only a good seal organization, but one that is monitoring the operations of its members to ensure that they are following the policy they agreed to, and two, they are taking the trouble of bringing suits or investigating and kicking them out of the organization if they fail to follow the policy?

How will I know that as a consumer, Mr. Lewin?

Mr. LEWIN. I will speak from our point of view.

The best way we have of demonstrating that is to do just as we demonstrate it. We have a watchdog process whereby any consumer that has a complaint against one of our licensed sites conveys that complaint to us. The first thing that we do is to ensure that the site itself has had an opportunity to respond to that. If they have not, we investigate it.

If indeed we find that there is a violation of the privacy policy, we contact that Web site and make sure it is remedied. If they do not remedy that situation, which again has not occurred, we will throw them out of the program and if necessary, based on the contract that we have with that site, we will take legal action or turn them over to the State, local agencies, whatever is appropriate.

Mr. TAUZIN. How do consumers know that you are going to do all of that?

Mr. LEWIN. Again, that is a good question. With the Privacy Partnership program, we had some very great success in increasing awareness. We need to continue doing that. That is one the key points that I mentioned in my prepared article, my statement.

Mr. TAUZIN. Mr. Cerasale, let me wrap it up with you.

How do I know that the Direct Marketing Association is going to properly monitor its members and make sure they are following the new policy that you just put out on privacy? How do I feel comfortable in dealing with one of your member firms that you are watching them and you are going to kick them out if they misbehave or misuse my information?

Mr. CERASALE. Two things. One, of course, is to actually do something, get the information out, public.

The second thing is the DMA's privacy policy says you have to give them notice and you have to give them an opportunity to opt out. Those are two things that have to appear on the Web site. As we said before, once you are on the Web site and you say, here is what I do and here is what I promise to do and you don't do it; we also have FTC jurisdiction through section 5 violation coming so that it is not just a seal on a DMA member and I follow the Privacy Promise, but you also have to have a notice and give choice

to the consumer and then once you do that, you have to follow it in that means.

Mr. TAUZIN. Which is at least more than you got in the hallways of the Rayburn Building.

The gentleman from Massachusetts, Mr. Markey.

Mr. MARKEY. Thank you, Mr. Chairman.

Mr. Lewin, when a Web site has violated your privacy policy and you say you boot them out, you then say that—and then we notify the State or other jurisdictions that could take action against them.

Mr. LEWIN. If applicable, yes.

Mr. MARKEY. What if I was in a State that had no laws?

Mr. LEWIN. Again, if the violation was to our license agreement that we had with the site, then we would pursue that. My comment was——

Mr. MARKEY. What does the consumer get? You could sue them because they violated your trust, but what about the consumer? What right do they have to any restitution because their privacy was violated under your program?

Mr. LEWIN. That is a good point. During this entire watchdog process, as we call it, we keep the consumer informed of what is going on, what the problem was, et cetera, et cetera, et cetera. If there is something that caused enough harm to the consumer that it required some type of legal action, justified by that individual, then obviously they can accomplish that.

Mr. MARKEY. What if the State had no laws on the books, Mr. Lewin, and the consumer is out $100,000, they believed that their privacy has been compromised and their reputation is ruined? Where do they go if the State has no laws? What can you do for this individual?

Mr. MARKEY. What can you do for this individual?

Mr. LEWIN. In your hypothetical situation, we just bring the, No. 1, the remedy, so that it does not occur again. If it is against a——

Mr. MARKEY. But that is corporate. I am talking about the individual. Where does a—where does an ordinary person go? Do they go to you, Mr. Lewin, do you help them get their privacy process back?

Mr. LEWIN. No.

Mr. MARKEY. Do they go to you to get money back, will you bring the suit?

Mr. LEWIN. No.

Mr. MARKEY. You say go to the States, if applicable. Should there be laws at the State level for people to go to gain remedies because their privacy, their families' secrets have been compromised in a way that harmed the family?

Mr. LEWIN. From what I have observed in the press so on and so forth, there seem to be enough or sufficient and local and State laws dealing with the kinds of situations that may create what you are kind of postulating.

Mr. MARKEY. Do you think every State in the union has sufficient laws on the books so that the people can gain——

Mr. LEWIN. I don't know that for a certain.

Mr. MARKEY. They do not, Mr. Lewin, let me tell you they do—that is why we are here at the Federal level because they do not. So notwithstanding with your good efforts, and they are good ef-

forts, I want to congratulate you and companies like yours for your programs. But at the end of the day, you can't get them back their reputation, you can't get them back what the family lost. And the States can't get them back what they lost because they don't have laws either.

And the question is, where do you go, which office do you go to. Who do you—what rights do you rely upon, Mr. Lewin? And what we are hearing today is that we don't have any place to go. Although your program is a very good step, and I think people should avail themselves of it. But at the end of the day, there is a certain kind of—to me the way I view this whole revolution is that it empowers individuals, it gives every one of us the ability to be able to act, that is to greatness of the system.

And here at the end of the day, while all of this power, theoretically comes to me, I don't have any privacy rights. I don't have any security rights. I don't have any place to go to enforce them. I am told that it is a one-way street, you know, that there are no laws which are passed or which are going be to passed. And that is what really—what troubles me, Mr. Lewin, although you are the best that is in—that has been inserted to substitute for that, but even with that, as you say, there would be no place for anyone to go to get the relief their family needs.

Thank you, Mr. Chairman.

Mr. TAUZIN. Thank you very much. With the gentleman's indulgence, I was looking for this while I was doing my round, but I wanted to point it out to you. The Discover magazine awards new technology winners each year, one of their awards winners this year is called Video in a Chip. Look at these cameras out here, you can tell when they are watching you, they are pretty big devices.

You guys have got to lug them in and out of here. New developments, today's video cameras generate pictures from charge couple devices from CCDs which provide greater picture but require a pile of support circuitry, they cannot sit on the same chip. But guess what, the one-chip camera has been developed, Lucent Technologies, using the same CMOS materials in the personal computer, Mark Leonities and his colleagues at Lucent agree that every secret agent's dream contraption, a video camera the size of a cigarette lighter, a lot easier to carry guys, but also a lot more intrusive in the lives of Americans.It is not just online privacy. It is some big issues here.

The gentleman from Illinois, Mr. Shimkus.

Mr. SHIMKUS. Thank you, Mr. Chairman. Mr. Lewin, I just want to follow-up on some of my colleagues questions from the Commonwealth of Massachusetts. Do you have any—I mean these were postulated as hypotheticals. Do you have any real world stories of—based upon people who are involved in your entity with the business relationship with you that have had problems and have had to go through some of the hurdles that the gentleman mentioned.

Mr. LEWIN. Not as they relate to the issues of privacy that we are talking about here. We have been made aware because people visiting a Web site that have had some difficulties and see our trustmark has sent us some complaints outside of the preview of the area that we are talking about in privacy, but that is the only——

Mr. SHIMKUS. That has only been external requests, you don't have anybody that is dealing with your product who have complained about loss of information?

Mr. LEWIN. No. If there had been a complaint, cases that were valid, and approximately 80 percent of the cases that we get—come to watchdog process deal with some misunderstanding that the particular consumer with the Web site, something wasn't clear, so on and so forth. In those cases that were valid, of which there were—when you boil it down, there are only about four cases, it was in two of those cases, there was just simply a bug in what the Web site thought was happening, but indeed something else was happening, and once it was called to their attention, they fixed it, recognized their problem and proceeded.

In one case, it was known, but it was a misunderstanding and it was fixed. And in the last case, that was also a similar situation.

Mr. SHIMKUS. Let me just throw out a question for the panel as a whole. As I hear this, and I heard the information on cash transaction, is it impossible in this day and age to be anonymous?

Ms. MULLIGAN. I will take a first stab at that. I think many of us enjoy a whole lot of "anonymity," that we don't really appreciate. When you walk down the street, you may pass a lot of people and they may observe you, but very few of them are taking a picture, recording, following. And so the experience of the individual is a whole lot of—I actually think probably a more powerful term and something I think many Americans really resonate is autonomy, a lot of us experience a lot of autonomy in freedom to do a lot of things without the fear that everything we are doing is recorded and monitored.

And if you think about the Privacy Act which governs what information the government can collect about us, one of the things that puts limits on was their collection of their information about our First Amendment activities because there was this notion that in order for us to, as a society, debate, explore issues, have a robust participatory dialog about what appropriate policies were, we needed to have some protection from government surveillance, and so that there is a—you know, there is a real recognition of the importance of autonomy, anonymity, and I think many of us experience it in lots of different ways during the day, but there is a growing sense, and I think things like the piece that was pointed to in the Washington Post about the government has your number, the kind of growing lookup services industry that provides a wealth of data about individuals, not for marketing purposes but many other purposes, there is a sense that many of the footprints that we leave both in the online and offline world don't become permanent; they don't disappear.

Mr. SHIMKUS. Mr. Lucas, would you like to comment?

Mr. LUCAS. I would like to comment about the technology that is available for anonymity. I would just like to caution the committee when people present the fact that they are anonymous to be careful. There is a different between anonymity and what is called factual anonymity.

Anonymity for example when someone—when a technology claims that they have an application on a PC that talks to a Web site, but things like IP addresses are transferred, that is not anony-

mous. I would also remind that there is a recent project at MIT where they took the personal identifiable information from the students and the faculty there and just kept people's date of birth and zip code. Having that information alone and combining that with offline data sources, they were able to identify—remember you were talking about medical information—they were able to successfully correlate back over 80 percent of the people to a personal identifiable record.

When you talk about anonymity, I think consumers nowadays—40 percent of the data that is submitted to the Web is falsified. And I think that the reason that consumers do that is they feel that this presents a layer of anonymity between them and the site and it truly isn't anonymous. So from a technology perspective, there are technologies out there that provide what you would consider to be factual anonymity, but not all that claim they are anonymous do that.

Mr. SHIMKUS. Did you want to add?

Mr. CERASALE. Well, I never sought a Social Security number for my children until I couldn't claim them as an exemption on my taxes without doing it. So my children received Social Security numbers then. It is very difficult in this world today to survive without health insurance and you can't really be anonymous in health insurance. So I think that the thing of what you think of total anonymity is virtually impossible in the United States today, but that doesn't mean that there are things that what—parts of your life that you do think you can be anonymous.

Mr. SHIMKUS. I agree. Because when I was hearing the debate on cash transactions we just went through the hurdles earlier of this Congress on know your customer law that was being portrayed in the banking industry. And even if you want to operate under full cash transaction type basis, the desire to have access to that information by the government on cash transactions also hurts your ability to be somewhat anonymous. And that is—I think that is the reason why we are struggling with this issue, this technology is just amazing.

And I think more than just information, it is the easy access of the information that makes it much more of concern to both spectrums, from those who are the most liberal to those who are most conservative, there seems to be a tremendous consensus of trying to protect our freedom of our own information.

With that, I yield back the balance of my time.

Mr. TAUZIN. I thank the gentleman. I point out that there is great conflict though, the fact that only 2 percent of the total volume of financial activity is in cash also is important to know that inside that 2 percent is most of the illegal activity. People don't go around using credit cards to do illegal sorts of things. And, you know, so you have got that conflict between government's ability to deal with the illegal activities and your right to keep information private, trying to be anonymous sometimes. Pretty tough balancing act we are going to have to do here.

The gentlelady from California, Ms. Eshoo.

Ms. ESHOO. Thank you, Mr. Chairman. I guess the illegal cash activities are still not attracted by the mileage that is offered by using a credit card. I often think that is one of the main attractions

for using it for everything. My mother is still appalled that I would use a credit card to buy groceries; she just can't believe that.

Mr. TAUZIN. Do you remember the story about Jerry Springer?

Ms. ESHOO. The cash transaction.

Mr. TAUZIN. If the gentlelady remembers the story about Jerry Springer. What did he did, used a check, I think, in a house of illegal prostitution. This kind of thing is rare, but it happens.

Ms. ESHOO. I am glad it was you that brought up Jerry Springer, I am talking about my mother, you are talking about Jerry Springer. At any rate, this has really been an instructive panel. And I once again want to welcome my constituent, Mr. Lewin, and each one of you that has contributed to this.

I have a thousand questions really swimming around in my mind on this. One of the things that comes to mind is that without good consumer education, I think that the seal on a Web site is really going to get lost in the increasing barrage of banter ads and logos and all the advertising. I mean you look at these sites and, you know, your eye is just drawn—or it is a challenge to your eyes, because you are drawn to so many things that are blinking and waving and trying to get your attention.

So I really don't know what kind of further efforts are being made and maybe Mr. Lewin can tell us something about that.

And I am also curious, has anyone ever ripped off your seal; and if they have, how do you find out, and once you find out what do you do?

And what do people pay for these services? Is it the same nationally or is there competition between you and the Better Business Bureau. And how do you advertise; how do you get the word out?

Mr. LEWIN. Okay.

Ms. ESHOO. Does the FTC get anything out of it?

Mr. LEWIN. Wait a minute.

Ms. ESHOO. I told you I have a thousand questions.

Mr. LEWIN. It was an overload to my mind there. Let me try to address my questions. If I miss one, please remind me. First of all, regarding how the site pays TRUSTe for the use of the seal, that is based solely on the company's revenue. In the—it starts at $299 for the year, and then it goes up to $4,999.

Ms. ESHOO. And others do approximately the same?

Mr. LEWIN. Yes, they are approximately the same, that is correct. I should point out that 85 percent of our sites are $10 million or less. So the word is getting out to the small sites, okay, it is not just a big site phenomena. People that are getting into the activity of establishing their servers and so forth want to do the right thing, and I want to emphasize that, they want to do the right thing. And when people do something wrong. I am talking about the Web site now, on the Web site, it is typically out of ignorance, they just don't know, or they didn't have the information and so they come to us and seek advice.

To address your question about have people tried to rip our seal off, yes. We know of now 7 cases and 4 of the cases happened prior to last month and 3 just recently happened.

Ms. ESHOO. How did you know?

Mr. LEWIN. How we find out is through a couple of mechanisms. We are beta testing some technology that goes out and searches the

Web looking for graphics. And it comes back with the identification of the Web site, what is called the URL, we match that against our authorizing licensee list and if we don't have a match, a-ha, our attorneys have an opportunity to write a letter, which indicates that——

Ms. ESHOO. You don't need an attorney to do that.

Mr. LEWIN. It looks more impressive if you have all the names on the top of the paper.

Ms. ESHOO. I know; I am just teasing.

Mr. LEWIN. In all four cases, it stopped. They took the seal off. To be fair, in three of those cases because they sent us a signed agreement, they thought that they can put the seal up. That is not the case, that is the beginning of the process, because they have to talk to one of our account executives, as they are called, that guides them through the actual creation of the privacy statement, and only after they bless it are they authorized to put the seal on, if it says everything that should be said.

And the one case was just somebody who they thought they could get away with it. The other three cases, the letters have already been written, and we anticipate that they will be resolved. But if somebody—if somebody ignored our letters or didn't take action, we would pursue it to the fullest extent, because what we offer is credibility. If we lose credibility, we lose everything. And so we pursue that vigorously.

And as to your other question.

Mr. TAUZIN. She asked what the FTC have to do with your——

Mr. LEWIN. Oh, thank you. We stay involved with what goes on with the FTC, and I guess the model I would like to use is with the Children's Privacy Seal that we put together, once we—in our discussions with the FTC saw what was going on and we attend their workshops and so on and so forth, we try to anticipate what is going to happen, so we alert our licensees that are—that have Web sites that are focused on children 13 years or under to start making these changes, to start looking at this, to give them the lead time necessary and to make them ready when indeed that is enacted.

The other thing that we do is we respond to their requests for information. In cases that have been drawn to their attention if there is any information that we have that they feel might be appropriate, then we will work with the appropriate parties at the FTC.

Ms. ESHOO. I think in so many of the things that have been expressed by the panelists, and including the previous panel is that we have made some progress, we have made some progress and the progress that has been made, the innards of it have some weight to them. But it seems to be that overall in this area of online privacy protection, et cetera, et cetera, that right now it is really more the exception than it is the rule.

And it is startling to me, because everything else is in direct contrast to that on the Internet. I mean it is the speed of lightening; it is incredible. If you just keep layering on the statistics of the usage and its importance, I mean one can just go on and on.

And I am so struck with the fact that this remains a premature baby that doesn't—is not gaining weight the way it should. I mean

this is really in the incubator. So I don't know if it would be prudent for the Congress to say by such and such a date, this is the progress that needs to be made.

I mean we are dealing with that in terms of medical privacy; if we don't act by a certain date, then the Secretary of HHS will then write the regulation or the language for it. But it seems to me that it is an area that either the private sector is going to make grow and grow rapidly or we need a Federal nudge here.

I don't know. Does anyone want to add anything to that?

Ms. SINGLETON. Let me add something quickly. I think actually the contrast between sort of what has been called for in privacy and what is actually developed. On the one hand, if you continue to operate from the same assumptions that you started with, then it looks like okay the Federal Government has to start doing something.

Ms. ESHOO. And what I really didn't understand in your opening testimony though what your assumptions were. I think you were questioning the assumptions on which——

Ms. SINGLETON. Yes, exactly. I mean it is very difficult for me to lay out my thinking about privacy in a concise manner, but I do think that it is really important to go back when things are not working the way you expected them to work and say maybe this isn't quite as simple a question as we thought. Maybe there are costs to consumers as well as benefits.

Ms. ESHOO. This is not just a philosophic debate and discussion about assumptions. We know that there are areas that are already protected, and we are trying to be delicate and prudent and maybe even bring some wisdom as to how we shift that architecture that is already in place to this new medium.

Ms. Mulligan, did you want to add something?

Ms. SINGLETON. I am sorry I hadn't quite finished.

Ms. ESHOO. But you are on my time though.

Ms. SINGLETON. I am sorry.

Ms. MULLIGAN. I think it is an important question and, you know, the analysis that the FTC provided is okay we have some progress here access, much less progress; security, less progress; the whole pie, do you want the whole thing? We are talking still 10 percent, how do we get from here to there. I have to tell you the TRUSTe program, the DMA line, the standards in those programs are becoming much more like the fair information practices that are embodied in the Privacy Act or the OECD guidelines which are kind of the international discussion, and I think there is an enormous amount of buy-in on what the principles are, and the real question is, how do you get ubiquity.

And I believe that ubiquity is going to come through increased focus by the FTC, increased self-regulatory efforts, but also a focus on how to get the people who aren't paying the attention in the room, and I think that Congress has traditionally played that role of how do you get the bad actors, how do you get the free riders, the people who are making a dollar off of information and really aren't interested in putting themselves under the FTC's, you know, spotlight by saying anything, because if they don't say anything, chances are nobody is going to come after them.

Ms. ESHOO. Thank you very much. Thank you, Mr. Chairman.

Mr. TAUZIN. Thank the gentlelady.

The gentleman from Ohio, Mr. Sawyer, is recognized.

Mr. SAWYER. Thank you, Mr. Chairman. I was just struck by the notion of the Federal nudge. I was wondering whether that may be filed in technical terms between a resolution and an unfunded mandate.

Mr. TAUZIN. Does it get an H.R. Or an HS? I am not sure.

Mr. SAWYER. I assume that many moons ago you passed the point at which we were offered the opportunity to submit our statements for the record.

Mr. TAUZIN. Yes. That has been by unanimous consent.

Mr. SAWYER. I welcome the opportunity to undertake that.

Mr. Lewin, you have talked a lot about the kinds of things that the people whose sites you provide certification to their obligations and responsibility, do you face a particular liability having certified a site and then having found it to be not in compliance with the standards which you certify?

Mr. LEWIN. The—well, in our agreements we indemnify in terms of, you know, our trustmark and what we do and so on and so forth. If I understand your question correctly, and please tell me if I don't, are we liable if the Web site does something dastardly to a consumer and we should have caught it; is that the question?

Mr. SAWYER. That is essentially it, yes.

Mr. LEWIN. No.

Mr. SAWYER. I assume you prefer not to be?

Mr. LEWIN. Right, right. And I think that the issues are pretty clear. There could be changes that occur on a daily basis. What have you. Although we do monitor sites on a quarterly basis. And we do what we call seeding, which we track information as if we were a consumer of that Web site. And, therefore, if we get information from a—to one of our seeding addresses, we know where it came from and then we, you know, should that have happened, yes or no. And it is a very iterative process.

Mr. SAWYER. You have talked about looking for failures. Do you monitor Web sites——

Mr. LEWIN. Yes.

Mr. SAWYER. [continuing] that are actively in play? How do you go about that?

Mr. LEWIN. Yes. Currently that is done on—by our account executives and it is actually looking at the Web site in, No. 1 ensuring that there are no changes or if there were changes, are they similar to their business operating practices and so forth. We are also exploring technology now, as Dr. Lucas has already pointed out, that we are exploring to do some of that in a more automated fashion so we can do it on a more regular basis, and that is something that I am confident between now and the end of the year that you will see substantial progress in.

We also, by the way, provide what we call wizards which are—privacy wizards which allow an organization to quickly set up a privacy seal if they take certain defaults so on and so forth. And if they want—the more tailoring they do, the longer it takes. But we try to automate as much as possible the knowledge that we have gained by doing these licensees over and over again in various industries.

Mr. SAWYER. You had mentioned that most of the failures to comply were inadvertent; were they errors?

Mr. LEWIN. Yes.

Mr. SAWYER. Have you encountered those that were willful?

Mr. LEWIN. There was one case where the organization thought it was okay to do what they were doing. We disagreed, and as part of our escalation process, we called an outside auditor and in our program, Price Waterhouse, Coopers and KPMG to conduct the survey to verify our findings, and that was done at the licensee's expense which is part of our agreement, which was not a trivial expense. Once it was verified that indeed that was a problem the licensee recognized that they were at fault, and they changed their practice.

Mr. SAWYER. Mr. Cerasale, will you soon be offering an opportunity for consumers to remove their names from E-mail lists?

Mr. CERASALE. Yes, we will, similar to our telephone and mail or physical mail preference.

Mr. SAWYER. I assume that that is far from being a more onerous task, considering it is actually probably made easier by the medium that you are dealing in——

Mr. CERASALE. Well——

Mr. SAWYER. [continuing] by comparison to paper?

Mr. CERASALE. Actually trying to get it done electronically very quickly has proved to be some problem with making everything mesh computer to computer which is what has been slower. It will—it should be easier for a consumer to be able to mesh and get through to get on that E-mail preference list.

Mr. SAWYER. Do other organizations similar to yours undertake the same kind of thing?

Mr. CERASALE. I don't believe so. I think from our review, our history with the telephone preference service and the mail preference service, we look like we are the only ones working on that E-mail preference service.

Mr. SAWYER. Do you see that as a comparative advantage to the DMA or should, in terms of the gentlelady from California, others be given a Federal nudge to follow your example?

Mr. CERASALE. Well, they can actually—you would not have to be a DMA member to get that—to get that list, to use the list. We have a fee that we charge companies to use it to help cover our costs, but you don't have to be a DMA member to do it.

Mr. SAWYER. Thank you very much. Mr. Chairman, Ms. Singleton, did you want to finish up a thought that you were unable to complete on the gentlelady's California time?

Ms. SINGLETON. I think I would just like to reiterate that there are still an enormous number of open questions in this debate. A lot of information that has not been collected about the way information is used in the economy and how that benefits consumers in particular. And I think that particularly when things aren't going as expected, it is really important to question whether there is really a simple issue at all.

Mr. SAWYER. I think that is precisely the point that the chairman was making. Thank you, Mr. Chairman.

Mr. TAUZIN. Thank the gentleman. The gentleman from California, Mr. Cox, is recognized.

Mr. COX. Thank you. I have essentially two questions. One is the degree to which we can have agreement on the kinds of information that would be especially harmful to restrict the collection of, and when we are talking about people's medical information, for example, we get to sort of the core what we think we ought to have a privacy interest in protecting.

But there are other things about what we do that presumably the marketplace as a whole and we as individual consumers have an interest in making sure there is commerce in so that stores have what we want when we go visit them and so on.

So my first question really is what is it that we would be very well advised not to put on a list of things along with personal medical information that would we sort of presume we ought to keep private?

And the second thing is the extent to which, and I particularly want to address this question to Ms. Singleton, to which we ought to look to sort of 19th century legal traditions of private property rights to help us. To what extent can property rights take care of this debate as against move overarching government regulation which I think has sort of going after people one at a time on a case-by-case basis with ever more detailed regulations to try and fix problems specifically rather than generally.

And I leave it to any member of the panel to address the first question. Is there some information that we really should not think about restricting because it will subvert the marketplace?

Ms. MULLIGAN. I would like to actually link the two of them together. Generally when we talk about privacy, it is not necessarily about restricting specific pieces of informations, it is about giving the individuals to make decisions when they disclose information how it is used beyond the use of they disclosed it for. So, of course, medical information, most individuals are going to want that to flow freely between them and their doctor. And they are going to want it to kind of stay in that confined environment.

So the question is how do you ensure that? You can certainly ensure it through a property right. But I think what generally has been put in place since the 1970's in a variety of sectors of the economy whether it is government information, video rental records, the Fair Credit Reporting Act, is the notion of the way in which we protect a piece of property that I have willingly given to you for a specific purpose is to say that you have some obligations now about how you handle that data, and if you want to disclose it to the chairman, you get my permission or you allow me to opt out depending on how sensitive the data is, you take on some obligations to protect it, to make sure it doesn't get corrupted.

Mr. COX. So a license basically——

Ms. MULLIGAN. Yeah, the notion of a property right is really, it is the core that underlies what we call the code of fair information practices, they are not intentioned at all, and it is just kind of a bundle of rights and how do we best preserve those. And I think you can certainly do it through a case-by-case litigation giving individuals property interests.

I think there hasn't been a very thorough review of different statutes on the books and different common law models to figure out which actually best drive practices in the marketplace. We

don't know that, and which actually provide the most suitable remedies to consumers and which actually provide the best enforcement mechanisms. So the FTC must be an excellent place for ensuring general compliance; but as Representative Markey said, when an individual is harmed, am I going to get a specific redress from the FTC? Well, no, I might get that under a private right of action, but as far as ensuring compliance, if it is my name that has been resold, there may not be a whole lot of, you know, interests in my going to court.

There is a lot of barriers to nationally pursuing that action. So in thinking about how you structure a means——

Mr. COX. Although if we gave people access to even small claims court, anybody that was trafficking in that kind of information would be hit by a thousand bee stings, they would probably want to correct the behavior.

Ms. MULLIGAN. Absolutely, I think there is a whole host of ways you can go about looking at this. And I think one of the things that people call for legislation, we are not calling—there is a need to think about, which—I certainly listened to what Ms. Singleton is saying. There are questions you need to answer.

Mr. COX. Ms. Singleton, do you want to address that?

Ms. SINGLETON. Yes, I will take each question sort of point by point. I guess my first question is that there certainly is going to be areas where people are a lot more sensitive about the information than others. In some of those areas might be, for example, including religious preferences, sexual preferences and so on.

On the other hand, even in those areas, I think we have to act very carefully, because if you were to decide, for example, that religious information was something that would be sensitive, does that necessarily mean that we need regulation? And I think there it would be not necessarily and, in particular, it would be really important to look at if you got a new kosher foods company starting up and you want to enter that marketplace, and you are looking to identify your first customers; if that information is not available to you, you may never get off the ground.

So even once we have identified a sensitive sector, that is not necessarily going to sort of help decide whether or not there should be a Federal standard. I think on the property rights context, there is two parts to my answer, one is to say that if you look at the common law often, and back at the 19th century cases, often you will find a right to privacy tied in very close to a violation of physical property rights.

And, for example, in the 19th century, invasion of privacy was often sort of bundled into a nuisance suit if somebody had built a building too close together.

Mr. COX. Referring to the 19th century, what I really mean is 19th century property rights what we consider to be property in the 19th century, intellectual property wasn't a big deal back then, if you take those notions even physical property as they were bequeathed to us in the 19th and 18th centuries, and you use that as the model in the 21st century, my question is, is that promising?

Ms. SINGLETON. Okay, got it. I think there the closest analogies we can look to would be what other property rights and information exist, and these would include copyright, patent, and, to some

extent, defamation. And I think that those suggest that there can be property rights of information, but even in those areas the Internet has raised some really important new issues. And traditionally also those property rights and information have been relatively narrow, I mean, that is to say, particularly in patent law, for example, you know, it is time limited, it is limited to certain relatively technical information that is not generally in the public domain. So I think that sort of having a default rule that suddenly a large category of information that relates to people is a property right that wasn't before is potentially going to cause some problems.

Mr. COX. Well, Mr. Chairman, I thank you. I would just also mention that I got a chance to meet with the bankers from GOSS bank, which was a big Soviet bank, I probably talked to some of them, probably 1990, before the collapse of the Soviet empire, and we were having a conversation through an interpreter, and I speak some Russian, and I got involved with the interpreter and we have quickly figured out they it didn't have a word for mortgage, you know, the big bankers in the Soviet Union, and what I was trying to say was the No. 1 sort of startup capital for small business in America was the mortgage, and they needed to have land title registry and all the things we never think about in this country in order to get small business started up there, and what was then the Soviet Union, what quickly became Russia.

I think we need to remember that without a basis in law that free market actors cannot contract privately with one another properly, so we need to pay some attention whether or not we are importing these concepts from our forebearers in the 21st century. And I thank you for being generous with the time.

Mr. TAUZIN. Interesting. My visit to St. Petersburg confirmed that, a wonderful free market and little booths on the streets where they are selling products, right behind them are all the buildings owned by the public which are empty. I wondered what had gone on there, that is the people's building. Nobody can conduct commerce in there. It is really strange. No word for mortgage.

Mr. COX. I am sure they have one now.

Mr. TAUZIN. I am sure they have got one now.

Final comments. Mr. Markey.

Mr. MARKEY. Thank you, Mr. Chairman, very much. I am very intrigued by this whole notion of private right of action. And I think we need a lot of discussion about it, not just in this context, but also in the financial service industry context. I think if an individual had the ability to go to court in order to vindicate their privacy rights with no class action possible, the limitation on damages which could be received, I think that would go a long way toward helping to make sure that there was a cleansing of the industry.

And I hope that in the financial services industry context perhaps we can talk about that, it was part of my underlying amendment a couple of weeks ago that I finally paired down to its essential elements, but I think a private right of action is something that we might be able to agree with on a bipartisan basis.

Can I ask, Ms. Mulligan, in conclusion, if I could, are we asking the wrong question, when we focus so much of our discussion on mere disclosure requiring consumers to find, to click on, and then read a privacy notice on each Web site when they surf? It is a very

cumbersome thing. In the era of the World Wide Web, you can just keep moving. And just define privacy policy and read it could be a half a day.

It seems like an analog answer to a digital question, you know, how do we—how do we deal with these issues in this new era? You know, are we thinking in terms that reflect the new technology on the speed with which people can move from site to site; and as a result, we have to think outside of the old traditional boxes?

Ms. MULLIGAN. I think both yes and no. I think we have to import the old principles, and I think, as you said, no notice isn't enough and very clearly if you look at industry standards, BBBOnLine, TRUSTe, the Federal Trade Commission's proposals, your proposals and the financial services——

Mr. MARKEY. How can P3P help?

Ms. MULLIGAN. Absolutely. I think there is a role for technology to automate the disclosure. You know, we don't have a Schumer box for the information age, the hope is.

Mr. MARKEY. A what box?

Ms. MULLIGAN. We don't need a disclosure box for the information age, what we need is a technology that helps individuals, a Markey box.

Mr. MARKEY. I am afraid to pursue it. This is live in the Senate as well.

Ms. MULLIGAN. I am sorry. What we need is a technology piece that is going to enable consumers to talk about privacy, whether it is self-regulation or it is legislation, it is a wild Web, there is many Web sites. We have jurisdiction issues left and right, and the technology is going to be a critical piece, whether it is providing individuals with anonymity or factual anonymity or giving them the ability through something like the platform for privacy preferences being developed at the World Wide Web consortium to figure out what a privacy statement says and whether or not it abides by what they think they want their information to be handled.

Mr. MARKEY. Without a minimal standard, Ms. Mulligan, how can we expect the marketplace to ever know what it is that is expected of it? How do we reach that point absent any legislation passing that can then be pointed to as the expectation that each industry, each company would have to reach?

Ms. MULLIGAN. Well, I think, like you, I believe that there is the need for some baseline legislation, and so I am not saying that we don't need that, I think we clearly do. But in the absence of that, I think that consumers can be empowered through technology to do some self-policing about where they disclose information, how they disclose information to avail themselves of technology, and to look for businesses who have put themselves out in front to say that we are doing the right thing.

But I do think that self-regulatory efforts and technology that are grounded upon a shared baseline of policy is going to be the most successful in the end.

Mr. MARKEY. I want to thank you, Ms. Mulligan, and all of you. This was an excellent panel. I want to thank you, Mr. Chairman, I really enjoyed today's hearing, and I think you really helped put a spotlight on a lot of the nuances of this issue which we are going to need to understand if we are going to move forward.

I, of course, hope that we do move forward. But this hearing is indispensable in our understanding, and I hope that we can begin to work together toward crafting some bipartisan legislation that can deal with these issues.

Thank you, Mr. Chairman.

Mr. TAUZIN. Thank my friend. Any other further comments.

Mr. SAWYER. Thank you, Mr. Chairman. Let me just go back to a point Ms. Mulligan made and it has nothing to do with the Schumer box. Ms. Mulligan in your testimony, you made a compelling analogy to walking through a mall, and the notion that either a mall or each of the shops within it could stick an identifier on your back as you walk through.

How does personal discipline with regard to giving out information apply to that capacity to profile based simply on places that you have perhaps not even walked into, but simply looked in the window as you can in traversing global communication systems that exist today?

Ms. MULLIGAN. I think as Chairman Pitofsky said earlier, there are really unique ways in which digital technology can collect and analyze information. We don't have a lot of real world analogies, while the camera, you know, in the Rayburn halls may get glimpses of us as we walk by, it is not actually monitoring everything that we do, it is not our own personal camera.

And I think that, you know, consumer education is certainly part of it, because some of the information that is collected is collected through very useful purposes, when you go to a Web site where you have been, can be very helpful.

Mr. SAWYER. Helping to whom?

Ms. MULLIGAN. It can be useful to you as a consumer at times.

Mr. SAWYER. It might be. But I can make great use out of advertising, advertising that comes in and is available to everyone and comes from one direction and is one way. But when, in fact, I am providing the information that allows me to be targeted in ways that I am unaware of, even ways that may not particularly identify me but make me vulnerable to a diminishment of my autonomy and anonymity, that does affect me in ways that I can't possibly effect or affect by virtue of personal discipline.

Ms. MULLIGAN. Yeah, I think that is part of the reason that it is important that the FTC is going to continue to look at issues like profiling and identifiers. There are areas that may not specifically hit on individual privacy as in information that is identifiable, but that still give Representative Eshoo and you this uneasy feeling that someone is monitoring my activities and making decisions about me, even though they don't know it is me, and that is another component of privacy. And I think it is one that we have just begun to touch on.

Mr. SAWYER. And the cross-referencing of information may, in fact, make it possible to identify you or a very small fraction of a universe out of perhaps a worldwide population. It is virtually the way that law enforcement has worked for the last 200 years by cross-referencing information until specific individual or small number of individuals can be identified in ways that are inescapably demonstrable, that holds up in court, it will certainly hold up in commerce.

Thank you, Mr. Chairman.

Mr. TAUZIN. Thank you. We were just musing that we got a cross-referencing you can almost figure out who voted for you and who didn't vote for you.

Let me ask finally, is there anything wrong legally, morally with my posting a Web site that says upfront, come visit with me here, share information with me, I will not protect your privacy? Anything legally, morally wrong with me, if people want to come and visit with me and use my Web site share my Web site with me?

Mr. CERASALE. As long as you don't hide it. You don't have to make sure you can display it, and know it is fair.

Mr. TAUZIN. Ms. Singleton, you raised the issue, it is the right of privacy in the private sector as opposed to other personals in our society as sacred as it was constitutionally against government? Is it such that I can surrender it by agreeing you to take any information you want about me as long as I am told up front that you are going to do that; is that okay? Mr. Lewin?

Mr. LEWIN. Well, you have given notice, you have given them the choice, you have stated it very explicitly, the issue may become how clear is it. I mean how clear in your language are you making it to that individual, to that average consumer coming to your site, this is indeed what you are going to do and that is where the key issue is.

Mr. TAUZIN. In other words, is it a right we need to define and is it waiverable and under what circumstances? It is kind of what it boils down to; is that right?

Mr. COX. I want you to yield on that, because it is technologically impossible now, and there is a race in software to see who is ahead of whom in terms of getting there first. But is it possible right now for somebody to collect information on you before you even get around to reading their privacy notice?

Mr. TAUZIN. Yes.

Mr. COX. What we want to make sure of is that we don't hang a lot on this issue of opt-in or opt-out, that it is basically the opting that matters, we don't want silence to be consent. We want people to know what they are doing and there has got to be some evidence that there is an agreement.

Mr. TAUZIN. Mr. Lucas, would your technology do that?

Mr. LUCAS. The technology—we believe that it is kind of ironic on the Web page that we talk a lot about relationships that we are trying to establish, relationships with consumers. I may be a little old fashioned, but I believe you have to ask permission from a person in order to have a relationship with them. I think the laws that prohibit it any other way.

I think it is also ironic that we can spend millions and millions of dollars as an industry to determine information about a consumer, but when companies are asked to step up to providing access to information that they have about a consumer that becomes either too expensive or too complicated or there is some excuse. I think that one of the biggest issues that we need to provide to the consumers is the issue of access and the issue of being able to control whether a site can do profiling on them. You are absolutely right.

Mr. TAUZIN. The right to correct bad information; we have got to get to that sooner or later.

Mr. LUCAS. Absolutely. If we are talking about the European Union directive that was mentioned earlier, one of the basic problems that we had in the negotiations is over the issue of access, and it has never been over the real issue of access, and that is it is really a technology issue it is authentication. I can't think of a worst privacy violation than someone coming to a site and saying they are an individual and not being able to authenticate. But that really hasn't been the strongest issue. It has been a reluctance, it has been a liability, it has been all different kinds of issues. So I think, yes, we have to provide access, we have to provide consumers to opt-out of profiling.

Mr. TAUZIN. Last night, I got into a marvelous book, The Rising Tide, which I have been meaning to read, I finally got into it last night. It details a marvelous conflict between two enormously powerful people, one, the head of Bureau of Engineers and the other a great engineer himself, over whether to—how—or how, rather, to open up the mouth of the Mississippi River for the whole country to commerce.

The fight was over whether to dredge one of the passes, the southwest pass, a little at a time with dredges that kept breaking down, or the incredible idea, the other gentleman had I think his name was Eades, the other guy was Humphreys, I think, his idea was to put jetties out to channel the flow of the river out—off the continental shelf so that rush of the river itself would open up and clean up the river itself to commerce.

This was right after the great war of northern aggression against the south, the river was all blocked up at that time. They built the jetties, immediately commerce, the port of New Orleans, it just skyrocketed second only to the port of New York, eventually it eclipsed New York in tonnage.

The question is sort of parallel here. We don't know the answer yet, is the rush of consumers to electronic commerce being inhibited because we haven't addressed all of these questions? Do we need to address them in front of that rush, in order to open it up? Or, as in the case of those jetties, to get it all flowing, set some policy down that everybody knows and feels comfortable with, or is it as the Commission seems to believe, or some of the Commission at least, that indeed consumers are rushing to electronic commerce options and making their own decisions about how much commerce they want to do on it?

In short, can we know how much electronic commerce would be occurring if we had adopted policies upfront on privacy and security as opposed to letting the marketplace work themselves, can we know and how do we know? Mr. Lucas.

Mr. LUCAS. I don't think we can—I don't think there has been a number that is been assigned to it, but I can tell you if you refer to some of the surveys that have been by people like Dr. Alan Westin, it is clear that over 80 percent of the consumers who are asked what is the No. 1 reason they don't participate in electronic commerce is the lack of control over—and if you talk to consumers, my experience has been it is not the initial collection of information, because as was mentioned before, there are millions of con-

sumers that went to a site and gave out the most detailed information for the chance of winning a PC valued under $500. What consumers have told us over and over again, it is the secondary use of information.

If they go to an e-commerce site and buy a widget, they don't want that information sold or transferred to anyone else without their permission.

Mr. TAUZIN. Ms. Singleton raises the issue, and I will give everybody a chance to come back if you like to, but raises a question as to whether or not those statistics, those surveys are really replicated in the real world, and the virtual world in this case, in effect, consumers knowing now that they have—can go to a seal organization, knowing that they can use the technology very simply, knowing that there are in place more and more notice of privacy rights, more and more protections for them.

Are they in fact still not choosing to engage in electronic commerce? What are they waiting for, if they now know all of these things are coming into place so rapidly as the Commission seem to imply to us today, any one of you? Mr. Cerasale.

Mr. CERASALE. I think there are some parallels we can go back to look at. Today, outside of electronic commerce, looking at remote sales, that means you don't go in a face-to-face purchase, 40 percent of Americans do not—have never purchased remotely before the Internet. So you have a situation where only 60 percent of Americans feel that they either want to or have a credit card to be able to do it or a checking account to be able to purchase remotely and not deal with cash.

So that is—we are not certain exactly why and we are trying to look out, trying to find out why is it that 40 percent don't participate, so that you are never going to get all of the consumers even on the Net as you get online.

The second item is, that 15 years ago, even though they had telephone payment of credit cards to L.L. Bean, 15 years ago, 95 percent of all of their sales were through the mail, a check coming into the mail, the people were not confident to give L.L. Bean their credit card number. Now, it is 97, 98 percent credit cards, and that is not looking at what is happening with their significant growth in their online commerce.

So that it took time, even with a trusted name, for the Americans to feel comfortable to give out a credit card number. So I think that part of what is happening today in the slowness in the Internet is that people haven't used it, people are a little bit worried, they are going to wait to hear that their friend used it, had no problem with it, and so forth.

I can tell you the first time that I ever used the Internet, to press the button to send the Boston Red Sox my Discover card number, I sat there for 10 minutes before I hit the enter button. I got the tickets, it was a great game they actually won, and——

Mr. TAUZIN. Was it doubts about the security or the Red Sox?

Mr. CERASALE. It was the doubt—it was before August, so it was okay. So those things, I think those things are in place. I do—that doesn't diminish what Professor Westin has found and so forth, but I think there is a reluctance in something new for Americans to sit back and wait and listen to the grapevine and see what it is.

Mr. TAUZIN. Let's wrap it up, Mr. Lewin.

Mr. LEWIN. Just a quick note, and to emphasize the points already made, one of the key issues facing a lot of organizations that are now Web enabling some of their activities, their commerce activity, is the issue that we are going—there has been some progress made in the online world that is taking this date and blending it with information that they have collected through other mechanisms, registration cards and what have you, and what is the offline world. And now dealing with the issue of how do I take the rules that I established here and the decisions made by people and apply them to all of the legacy information that they have lying around is really a key issue for a lot of these organizations. And how to reconcile those, and what to do with it is something that is very much on their minds right now. And it is something that has to be paid attention to.

Mr. TAUZIN. Interesting. Anyone left with a question? Do we build the policy jetties now and open up the river, or do we let the industry dredge it out one dredge at a time?

Ms. MULLIGAN. Just on statistics of the causal effect, how do we know is it because people are anxious because of privacy, and the National Consumers League Survey, which is actually mentioned in my testimony, found that 42 percent of individuals who are using the Internet were only using it to surf for information, were not making purchases, with a much smaller 24 percent actually making purchases and citing privacy concerns.

And I think, you know, you can't completely extrapolate there, but that is 50 percent of the people who could potentially be engaged in online commerce are picking up the phone or perhaps sending in a check.

Mr. TAUZIN. So there is some evidence out there of reluctance still.

Ms. Singleton.

Ms. SINGLETON. I think one thing, I noted this in my written testimony also, there is a couple holes in the empirical information here. One would be what the rate of growth are of companies who have posted a privacy policy as compared to the rate of growth of similarly situated companies that have not. Now, it is important to compare similarly situated companies so you are not comparing AT&T to Joe's Hardware Store in Peoria, but I think that is one area.

Another thing to do is to look at the rate of growth of in commerce through—say, communities like America Online that has got sort of the whole regulatory fabric in there as a private community and to look at that and to compare it to rates of growth to e-commerce generally.

Mr. TAUZIN. Thank you very much. Any final, final thoughts?

Mr. MARKEY. To Mr. Cerasale, Red Sox tickets, $24; Popcorn, $2; parking, $10; e-commerce, $1 trillion; privacy protections, priceless. That is where we are, Mr. Cerasale, trying to put a price on it.

Mr. TAUZIN. I thought you said Red Sox tickets——

Mr. MARKEY. Half an hour before the game, outside of Fenway, they will all be priceless. There are some very wealthy people paying a lot of money.

Mr. TAUZIN. Did you see McGwuire last night? Wasn't that amazing?

Mr. COX. We have one little baseball thread hanging here and that is the distinction between the privacy policies of the Boston Red Sox on the one hand and the notion, fanciful or otherwise, of consumers that something might go on in cyberspace between their computer and the Boston Red Sox terminal.

The development of secure connections is very important. I think that everybody is willing to trust the Boston Red Sox, not everybody, but most——

Mr. MARKEY. Our fondest and deepest——

Mr. COX. [continuing] right at the window if you are there picking up your ticket at will-call, but it is this sort of cyberspace issue that maybe as I send my credit card number to the Red Sox over the telephone lines it is being routed somewhere that I don't know about and pirates are going to take that information.

Mr. MARKEY. More likely the Yankees.

Mr. COX. It is impossible to avoid these metaphors. Before we switch back from baseball to the Mississippi Delta, I think I had better yield back.

Mr. TAUZIN. I thank you all. This has been very enlightening, and we appreciate your testimony and your contributions. The hearing stands adjourned.

[Whereupon, at 2:14 p.m., the subcommittee was adjourned.]

[Additional material submitted for the record follows:]

PREPARED STATEMENT OF PETER J. GRAY, CHAIRMAN, INTERNET CONSUMERS ORGANIZATION

The Internet Consumers Organization (ICO) is pleased to submit this statement on privacy for the hearing record. ICO provides policymakers and other interested parties with fair and balanced policy positions on issues of importance to both Internet consumers and providers of online products and services. Our objective is to help ahape a progressive environment for the Internet, and to conduct research and education programs to enhance consumer confidence in using the Internet for e-commerce and other purposes. ICO is incorporated in the District of Columbia as a nonprofit organization.

In the privacy arena, the rationale for public policy appears to be based on a series of assumptions that rely heavily on public attitude polls, media exposure of abuses, potential threats to personal privacy, laws and regulations of other countries, and misinterpretation of statistical data and anecdotal information. To get a better reading on privacy issues, and to help make informed decisions about privacy protection, it is useful to examine the following key assumptions and compare them to the reality of the consumer marketplace:

Assumption: Consumers are universally concerned about the privacy of their personal information.

Reality: Some people are more privacy-sensitive than others; some care most about protecting sensitive information, like medical records; others don't seem to care, and are willing to trade-off their privacy for free or lower-cost products or services, or other benefits.

Assumption: Consumers who say they are concerned about their privacy will refrain from using the Internet.

Reality: People often behave or act differently from what they say or believe. This is a form of cognitive dissonance that may explain the discrepancy between the Louis Harris polls, where 81% of Net consumers expressed concerns about privacy, and the explosive growth in Internet usage. What's really happening? The Pew Research Center found that Americans' daily Internet usage rose from 4% in 1995 to 25% in 1998. Media Metrix reported a 15% increase in monthly Internet users, from about 54 million in May 1997 to 62 million in May 1998. Forrester Research found that over ¾ of online households now surf the Web.

Assumption: Privacy concerns are keeping consumers who use the Internet away from using e-commerce to purchase goods and services.

Reality: The facts don't bear this out. The Department of Commerce reports that online sales grew from about $3 billion in 1997 to $9 billion in 1998. Forrester Research estimates that 26% of online users made regular purchases on the Web in 1998. Jupiter Communications found that the number of people buying something on the Net grew from 10 million in 1997 to 17 million last year, and it projects U.S. online sales to be about $12 billion in 1999. The Institute for the Future forecasts e-commerce sales to consumers will exceed $1 trillion by 2010. Polls show that women are more concerned about privacy than men, yet they buy more online than men do, according to a recent survey by CommerceNet and Nielsen.

Assumption: Most consumers are worried about unauthorized access to their e-mail messages.

Reality: Forrester Research shows that over 80% of online users regularly send e-mail messages, still the most frequent use of the Internet. Most of these users are not worried about the privacy of their e-mails, since they don't attempt to encrypt their messages or use anonymous identities.

Assumption: Consumers consider Internet privacy as more important to them than convenience, security, reliability, cost, value, choices, customer service, speed of access and other benefits.

Reality: Some may value privacy more highly than other factors, but others may not. Individuals have a hierarchy of needs and preferences, which may change over time. Someone shopping for the lowest cost airfare available may be willing to divulge a degree of personal information in order to get the ticket. Someone else who pays bills online may value security and reliability of the service more highly than privacy. Researchers surfing the Web may be primarily interested in speed of access to resource information. System intrusions, computer viruses and worms, unauthorized access to personal files and fraud, may lower consumer confidence and become more important deterrents to e-commerce than privacy.

Assumption: Consumers will not do business with companies that don't have privacy policies or privacy seals posted on their websites.

Reality: Most people want to deal with companies that they trust and have confidence in. Good privacy policies and practices are an important element of trust. But, good customer service, fair and prompt dispute resolution, excellent product quality and other factors are also important elements of trust. BizRate.com found that the level and quality of customer service, on-time delivery, product representation, and shipping and handling were rated higher than privacy in determining consumers' likelihood of repeat purchases from an online merchant.

Assumption: Consumers trust governments over businesses to protect their privacy.

Reality: There have been notable privacy lapses by both federal and state government organizations, such as the IRS, Social Security Administration, state motor vehicle bureaus, health care and other agencies that created public distrust and outrage. Federal, state and local governments should be required to disclose and enforce their privacy policies to protect the confidentiality of citizens' information.

Assumption: Self-regulation by industry will prevent enactment of online privacy legislation.

Reality: Industry self-regulation demonstrates the willingness and ability of responsible companies to earn the public's trust. But, self-regulatory initiatives tend to postpone or dampen, rather than prevent the enactment of privacy laws, because some companies fail to self-regulate. Still, new laws are not the panacea for assuring general online privacy protection. Targeted legislation may be desirable in some specific instances (e.g. to protect sensitive medical records from unauthorized access without the consumer's knowledge or consent).

Assumption: People have no control over their personal privacy in cyberspace, and they are powerless to protect themselves from privacy intrusions.

Reality: Informed consumers have the ability to control their online privacy by using technological means to protect their personal information. They can seek out companies that have good privacy policies, disable cookies and refuse to provide certain information about themselves. A partnership between the private sector, government agencies, and non-profit consumer organizations should be formed to educate and inform consumers on how best to protect their privacy.

Assumption: People object to company practices that involve the collection and use of personal information about them.

Reality: A recent Vanderbilt University study found that over 72% of Web users would provide personal information to companies that disclose how the information would be used. If a company with a good privacy policy discloses it to the public, and uses information it collects to provide consumers with benefits, consumers are more likely to allow such information to be used to suggest products or services

based on their personal preferences. A good example of a responsible privacy policy that engenders consumer trust is that of Amazon.com.

In conclusion, there is a need to critically examine the assumptions that drive and shape privacy policy in the U.S. Legislation and regulations are not the panacea for comprehensive online privacy protection. Instead, a combination of legislation targeted to address specific abuses, enforcement of existing laws and regulations, industry self-regulation with oversight, consumer education, application of technological solutions and consumer actions to protect themselves, will help to protect online privacy.